DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) CON BASE AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION SEGUN LINEAMENTOS DEL MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES EN EL MARCO DE LA ESTRATEGIA GEL (GOBIERNO EN LINEA) Y EN CUMPLIMIENTO DEL DECRETO 1078 DE 2015 Y 2573 DE 2014.

RONALD MAURICIO CELY ESPITIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
PROGRAMA ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTÁ D.C.
2018

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) CON BASE AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION SEGUN LINEAMENTOS DEL MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES EN EL MARCO DE LA ESTRATEGIA GEL (GOBIERNO EN LINEA) Y EN CUMPLIMIENTO DEL DECRETO 1078 DE 2015 Y 2573 DE 2014.

RONALD MAURICIO CELY ESPITIA

PROYECTO APLICADO PARA OPTAR POR EL TITULO DE ESPECIALISTA EN SEGURIDAD INFORMATICA.

DIRECTOR DEL PROYECTO DE GRADO
ING. YOLIMA ESTHER MERCADO PALENCIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
PROGRAMA ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTÁ D.C.
2018

Nota de Aceptación

_____

_____

_____

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

Bogotá D.C., Febrero del 2018

DEDICATORIA

Este proyecto de seguridad informática lo dedico a mi familia, porque me han dedicado la ayuda, paciencia y la fuerza que día a día me han brindado para continuar con mis sueños de lograr los objetivos propuestos en mi proyecto de vida, gracias a Dios todo fue posible.

AGRADECIMIENTOS

Agradezco a la Universidad Nacional Abierta y a Distancia por brindarme la oportunidad en cursar el programa de especialización en seguridad Informática, mediante el cual expreso que el desarrollo del proyecto sustenta un ejercicio realizado con mucho esfuerzo y dedicación del equipo del proyecto que la Federacion Colombiana de Municipios asigno para cumplir con los objetivos planeados y propuestos.

A los Directores del Proyecto Ing. Yolima Mercado Palencia y Salomon Gonzalez, por su tiempo y dedicación en transferir sus valiosos conocimientos, por su paciencia, por el esmero e intachable y determinada rigurosidad para lograr el desarrollo de un proyecto de grado con altos niveles de profesionalismo y en la aplicabilidad de las mejores practicas y normatividad para la presentación de proyectos de grado.

CONTENIDO

Pag.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

TÍTULO

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) CON BASE AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION SEGUN LINEAMENTOS DEL MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACION Y LAS COMUNICACIONES EN EL MARCO DE LA ESTRATEGIA GEL (GOBIERNO EN LINEA) Y EN CUMPLIMIENTO DEL DECRETO 1078 DE 2015 Y 2573 DE 2014.

INTRODUCCION

El Diseño del Sistema de Gestión de Seguridad de la Informacion con base al Modelo de Seguridad y Privacidad de la Informacion del Ministerio de las Tecnologias de la Informacion y las Comunicaciones, se desarrollara con la recopilación de las guías de seguridad y privacidad de la información del programa de la Estrategia de Gobierno en Línea, mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL.

La Estrategia de Gobierno en Línea, liderada por la Dirección de Tecnologías de la Información y las Comunicaciones de la Federación Colombiana de Municipios – Dirección Nacional Simit, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de ofrecer servicios de tecnología con altos estándares de seguridad y privacidad de la información, de tal manera que contribuye con la construcción de un Estado más participativo, más eficiente y más transparente, hacia las autoridades de tránsito y municipios del País.

La planificación e implementación del SGSI con base al Modelo de Seguridad y Privacidad de la Información – MSPI, en la Federación Colombiana de Municipios – Dirección Nacional Simit, está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos: Estratégicos, misionales, apoyo, control y evaluación; y el tamaño y estructura de la Entidad.

El Modelo de Seguridad y Privacidad de la Información – MSPI, debe ser concebido en la Federación Colombiana de Municipios – Dirección Nacional Simit, para conducir a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

En la Federación Colombiana de Municipios – Dirección Nacional Simit, debe proyectarse en establecer una alineación del MSPI con el Marco de Referencia de Arquitectura TI y orientar transversalmente los procesos de la entidad, contemplando los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

El Modelo de Seguridad y Privacidad de la Información en la Federacion Colombiana de Municipios, debe pretender facilitar la comprensión del proceso de

construcción de una política de privacidad por parte de la alta dirección de la entidad, que permita fijar los criterios que seguirán para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con dicha información.

1. PROBLEMA

1.1 DEFINICIÓN DEL PROBLEMA

La Federación Colombiana de Municipios es una persona jurídica de carácter privado, sin ánimo de lucro, creada mediante el concurso y consenso de los entes territoriales en ejercicio del derecho constitucional de asociación. A ella pertenecen por derecho propio todos los municipios, distritos y asociaciones de municipios del país y tiene como finalidad la defensa de sus intereses. En este sentido, la Federación Colombiana de Municipios se rige por el derecho privado, salvo en lo que concierne a la función pública asignada según los artículos 10 y 11 de la Ley 769 de 2002, cuyo fundamento constitucional se esgrime en el artículo 209 de la Constitución Política.

Luego, si bien es cierto que la Federación Colombiana de Municipios se rige por las normas del derecho privado, en lo concerniente a la función pública delegada por disposición legal, se encuentra sometida a las normas propias del derecho público, siendo aplicable entonces para el presente proceso de contratación, los procedimientos contemplados en la Ley 80 de 1993, modificada por la Ley 1150 de 2007, Ley 1474 de 2011 y el Decreto Reglamentario 1082 de 2015.

La Federación Colombiana de Municipios por expreso mandato legal, ha requerido desde sus inicios, contar con una infraestructura tecnológica suficiente que garantice un adecuado y permanente funcionamiento, y que sea susceptible de perfeccionamiento a través de la implementación de nuevas tecnologías aplicadas siempre al logro del fin perseguido, con métodos de control y calidad de la información.

1.2 DESCRIPCION DEL PROBLEMA

En el marco del cumplimiento de dicha función pública delegada y teniendo en cuenta que la Direccion Nacional Simit, administra un sistema de información que está disponible en internet y a pesar de las implementaciones en seguridad puede llegar a ser objeto de intentos de sabotaje o ataques cibernéticos, se hace necesario para la entidad prepararse en la protección del sistema y de sus activos de informacion contra posibles ataques y amenazas, la proteccion debe estar alineada al MSPI (Modelo de Seguridad y Privacidad de la Informacion) que dispuso el Ministerio de las Tecnologias de la Informacion y las Comunicaciones en el marco de la estrategia GEL y en cumplimiento de lo señalado en el articulo 5 del decreto 2573 del 2014.

Así mismo la Federación Colombiana de Municipios dentro de la administración y actualización del sistema Integrado de Información sobre Multas y Sanciones por Infracciones de Tránsito debe garantizar la integridad de la información almacenada en el Sistema y blindar la infraestructura asegurando su disponibilidad para la consulta del estado de cuenta, cargue de información de las autoridades de tránsito

a nivel nacional y por supuesto, la generación de paz y salvos que permitan, a los ciudadanos, realizar los trámites de tránsito.

Dado esto se hace necesario buscar un apoyo que le permita a la Federación Colombiana de Municipios tomar las decisiones correctas, apropiadas y oportunas en cuanto a la seguridad de la información, acordes a la rápida evolución de los sistemas de información a nivel mundial y por lo tanto volviéndose un insumo indispensable para proteger el sistema y los procesos, basándose en las mejores prácticas existentes en la actualidad. Para suplir esta necesidad la Federación Colombiana de Municipios requiere contar con asesorías sobre los modelos de seguridad informática, las cuales deben incluir las revisiones y mejoras de políticas, normas, procedimientos y estándares, así como divulgaciones y capacitaciones para todos los usuarios de la entidad.

1.3 FORMULACIÓN DEL PROBLEMA**.**

¿Cómo el proceso de análisis y evaluación de riesgos ayudará a identificar las vulnerabilidades y amenazas que afectan la seguridad de la información de la entidad?

¿Cómo la entidad podrá alinear el Sistema de Gestión de Seguridad de la Informacion que ha venido adelantando en años anteriores al Modelo de Seguridad y Privacidad de la Información que dispuso el Ministerio de las Tecnologias de la Informacion y las Comunicaciones en el marco de la Estrategia GEL?

JUSTIFICACIÓN

La Federación Colombiana de Municipios por expreso mandato legal, ha requerido desde sus inicios, contar con una infraestructura tecnológica suficiente que garantice la seguridad de la información con un adecuado y permanente funcionamiento, y que sea susceptible de perfeccionamiento a través de la implementación de nuevas tecnologías aplicadas siempre al logro del fin perseguido, con métodos de control, enmarcados en la confidencialidad, integridad, disponibilidad y calidad de la información.

En el marco del cumplimiento de dicha función pública delegada y teniendo en cuenta que la Dirección Nacional Simit, administra un sistema de información que está disponible en internet y a pesar de las implementaciones en seguridad puede llegar a ser objeto de intentos de sabotaje o ataques cibernéticos, se hace necesario para la entidad prepararse en la protección del sistema y de sus activos de información contra posibles ataques y amenazas, la protección debe estar alineada al MSPI (Modelo de Seguridad y Privacidad de la Información) que dispuso el Ministerio de las Tecnologías de la Información y las Comunicaciones en el marco de la estrategia de Gobierno en Línea y en cumplimiento de lo señalado en el artículo 5 del decreto 2573 del 2014 y lo expresado en el Decreto 1078 de 2015.

El proyecto se desarrollara con base a las necesidades que posee la entidad en términos de fortalecer la seguridad de la información y el margen del cumplimiento normativo que están sujetas las entidades del estado colombiano, donde en el marco del cumplimiento de la función pública delegada de la Federacion Colombiana de Municipios y teniendo en cuenta que la Direccion Nacional Simit, administra un sistema de información que está disponible en internet y a pesar de las implementaciones en seguridad puede llegar a ser objeto de intentos de sabotaje o ataques cibernéticos, se hace necesario para la entidad prepararse en la protección del sistema y de sus activos de informacion contra posibles ataques y amenazas, la proteccion debe estar alineada al MSPI (Modelo de Seguridad y Privacidad de la Informacion) que dispuso el Ministerio de las Tecnologias de la Informacion y las Comunicaciones en el marco de la estrategia GEL y en cumplimiento de lo señalado en el decreto 2573 del 2014.

Si el proyecto no se logra desarrollar, la entidad tendría un impacto negativo a la hora de seguir vulnerable ante ataques informaticos y cibernéticos, con el proyecto se realizara un incremento significativo de la seguridad de la información y para la infraestructura tecnológica de la entidad.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Definir el diseño del Sistema de Gestión de Seguridad de la Informacion para la Federación Colombiana de Municipios - Dirección Nacional Simit, con base al Modelo de Seguridad y Privacidad de la Informacion segun lineamentos del Ministerio de las Tecnologias de la Informacion y las Comunicaciones en el marco de la estrategia GEL (Gobierno en Linea).

3.2 OBJETIVOS ESPECIFICOS

- Generar una investigación el marco metodológico para adoptar el Modelo de Seguridad y Privacidad de la Informacion en la FCM-DNS en cumplimiento del articulo 5 del decreto 2573 de 2014.

- Determinar el Análisis Forense Digital para la FCM.

- Precisar el asesoramiento en Ethical Hacking.

- Diseñar y asesorar la atencion de Incidentes y fraudes.

- Calcular la factibilidad y nivel de cumplimiento del uso y apropiación del SGSI para generar y socializar el plan de tratamiento de riesgos.

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

4.1 ALCANCE

El proyecto de grado está enfocado al fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) en la Federación Colombiana de Municipios – Dirección Nacional Simit. Mediante el cual abarca los siguientes aspectos:

a) Acompañamiento especializado a la institución en el logro de sus objetivos particulares en seguridad de la información. Capacitando, concientizando y sensibilizando a los funcionarios de la Federación Colombiana de Municipios – Dirección Nacional Simit.

b) Suministrar un encargado Oficial de la seguridad de la Informacion en sitio (CISO) el cual prestará sus servicios como experto en Seguridad de la información para diseñar la implementación del (SGSI) y (MSPI) en la Federacion Colombiana de Municipios - Dirección Nacional SIMIT.

c) Identificación de vulnerabilidades en los activos y sistemas de información de la Federación Colombiana de Municipios a través del Hacking Ético, herramientas y tecnicas, creando mecanismos de remediación que se deben aplicar a las vulnerabilidades encontradas.

4.2 DELIMITACION

a) El proyecto esta delimitado en el fortalecimiento de la seguridad de la información através del diseño del Sistema de Gestión de Seguridad de la Información (SGSI) basado en el Modelo de Seguridad y Privacidad de la Informacion de Gobierno en Linea, en cumplimiento del decreto 2573 del 2014.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

Nombre de la empresa: Federacion Colombiana de Municipios

5.2 MARCO CONTEXTUAL

La Federación Colombiana de Municipios es una persona jurídica de carácter privado, sin ánimo de lucro, creada mediante el concurso y consenso de los entes territoriales en ejercicio del derecho constitucional de asociación. A ella pertenecen por derecho propio todos los municipios, distritos y asociaciones de municipios del país y tiene como finalidad la defensa de sus intereses. En este sentido, la Federación Colombiana de Municipios se rige por el derecho privado, salvo en lo que concierne a la función pública asignada según los artículos 10 y 11 de la Ley 769 de 2002, cuyo fundamento constitucional se esgrime en el artículo 209 de la Constitución Política.

La Federación Colombiana de Municipios se rige por las normas del derecho privado, en lo concerniente a la función pública delegada por disposición legal, se encuentra sometida a las normas propias del derecho público, siendo aplicable entonces para el presente proceso de contratación, los procedimientos contemplados en la Ley 80 de 1993, modificada por la Ley 1150 de 2007, Ley 1474 de 2011 y el Decreto Reglamentario 1082 de 2015.

La Federación Colombiana de Municipios por expreso mandato legal, ha requerido desde sus inicios, contar con una infraestructura tecnológica suficiente que garantice un adecuado y permanente funcionamiento, y que sea susceptible de perfeccionamiento a través de la implementación de nuevas tecnologías aplicadas siempre al logro del fin perseguido, con métodos de control y calidad de la información.

En el marco del cumplimiento de dicha función pública delegada y teniendo en cuenta que la Dirección Nacional Simit, administra un sistema de información que está disponible en internet y a pesar de las implementaciones en seguridad puede llegar a ser objeto de intentos de sabotaje o ataques cibernéticos, se hace necesario para la entidad prepararse en la protección del sistema y de sus activos de información contra posibles ataques y amenazas, la protección debe estar alineada al MSPI (Modelo de Seguridad y Privacidad de la Información) que dispuso el Ministerio de las Tecnologías de la Información y las Comunicaciones en el marco de la estrategia de Gobierno en Línea y en cumplimiento de lo señalado en el artículo 5 del decreto 2573 del 2014 y lo expresado en el Decreto 1078 de 2015*.*

Así mismo la Federación Colombiana de Municipios dentro de la administración y actualización del sistema Integrado de Información sobre Multas y Sanciones por Infracciones de Tránsito debe garantizar la integridad de la información almacenada en el Sistema y blindar la infraestructura asegurando su disponibilidad para la consulta del estado de cuenta, cargue de información de las autoridades de tránsito a nivel nacional y por supuesto, la generación de paz y salvos que permitan, a los ciudadanos, realizar los trámites de tránsito.

Dado esto se hace necesario buscar un apoyo que le permita a la Federación Colombiana de Municipios tomar las decisiones correctas, apropiadas y oportunas en cuanto a la seguridad de la información, acordes a la rápida evolución de los sistemas de información a nivel mundial y por lo tanto volviéndose un insumo indispensable para proteger el sistema y los procesos, basándose en las mejores prácticas existentes en la actualidad.

Para suplir esta necesidad la Federación Colombiana de Municipios requiere contar con asesorías sobre los modelos de seguridad informática, las cuales deben incluir las revisiones y mejoras de políticas, normas, procedimientos y estándares, así como divulgaciones y capacitaciones para todos los usuarios de la entidad.

Reseña histórica:

Los alcaldes del país sentían la necesidad de tener una mayor interlocución con el Gobierno Central y tener una representatividad donde se aunarán esfuerzos para conquistar objetivos comunes.Por iniciativa de los primeros alcaldes elegidos por voto popular de los municipios de Santiago de Cali, Carlos Holmes Trujillo; Cartagena de Indias, Manuel Domingo Rojas Salgado; y Bogotá Distrito Especial, Andrés Pastrana Arango, se organizó el Primer Congreso Nacional de Municipios los días 16 y 17 de febrero de 1989.

Allí se suscribió el Acta de Constitución de la Federación Colombiana de Municipios y los primeros estatutos, que tuvieron como consideraciones importantes, impulsar el proceso de descentralización política, administrativa y fiscal en el país; fortalecer la capacidad de gestión administrativa en los entes locales; vigorizar la autonomía de los municipios de Colombia; enfrentar en conjunto los problemas comunes; incrementar la participación de los entes locales en el proceso de toma de decisiones del país; fomentar la integración, asistencia y colaboración entre los municipios.

Se iniciaron entonces las labores con el apoyo de la Federación Española de Municipios y Provincias (FEMP) y de la Fundación Friedrich Ebert en Colombia (Fescol)[1].

De esta forma se comenzaba a abrir paso para una de las reformas más importantes del siglo XX en el país: el inicio del proceso de descentralización con una nueva forma de política a nivel local que permitía incrementar la participación ciudadana, cerrarle el paso a la corrupción y promover formas de desarrollo local.

La creación de la Federación no sólo era una buena idea, era una necesidad de los alcaldes agremiarse, por cuanto en este nuevo marco institucional, eran autónomos y responsables de una gran cantidad de competencias nuevas que implicaban un gran reto para los municipios y una gran responsabilidad política.
El éxito o fracaso del nuevo modelo de Estado, dependería en buena medida de la gestión de las nuevas administraciones locales que tendrían por primera vez alcaldes elegidos popularmente[2].

Así nació la Federación Colombiana de Municipios. Inicialmente se cobró $100.000 de inscripción por cada municipio y por cada asociación de municipios para un total de 181 municipios y 6 asociaciones, con lo cual se obtuvo un capital inicial social de $21 millones 860 mil[3].

Por su parte, la Alcaldía Mayor de Bogotá Distrito Especial reconoció la personería jurídica de la nueva Federación con la resolución 0759 de 11 de diciembre de 1.989[4].

5.1.1 Objetivos Estrategicos Institucionales

PERSPECTIVA SOCIAL
- Objetivo: Responsabilidad Social
- Objetivo: Creación de Valor

PERSPECTIVA CLIENTE
- Objetivo: Confiabilidad

PERSPECTIVA PROCESO INTERNO
- Objetivo: Información Valiosa

PERSPECTIVA INNOVACIÓN
- Objetivo: Posicionamiento

[1] Historia de la Federacion Colombiana de Municipios. [En linea]. Disponible en:<http://www.fcm.org.co/?page_id=726>
[2] Historia de la Federacion Colombiana de Municipios. [En linea]. Disponible en: <http://www.fcm.org.co/?page_id=726>
[3] Historia de la Federacion Colombiana de Municipios. [En linea]. Disponible en: <http://www.fcm.org.co/?page_id=726>
[4] Historia de la Federacion Colombiana de Municipios. [En linea]. Disponible en: <http://www.fcm.org.co/?page_id=726>

Mapa Estratégico Federacion Colombiana de Municipios - Dirección Nacional Simit

Figura 1 – Mapa Estrategico FCM-Simit

Fuente: Activos de Informacion FCM.

5.1.4 Misión[5]

Contribuir al mejoramiento de los ingresos de los municipios con la operación y permanente actualización del sistema integrado de información sobre multas y sanciones por infracciones de tránsito a nivel nacional; permitiendo el acceso a la información que impida la realización de trámites de tránsito a los ciudadanos que no se encuentren a Paz y Salvo.

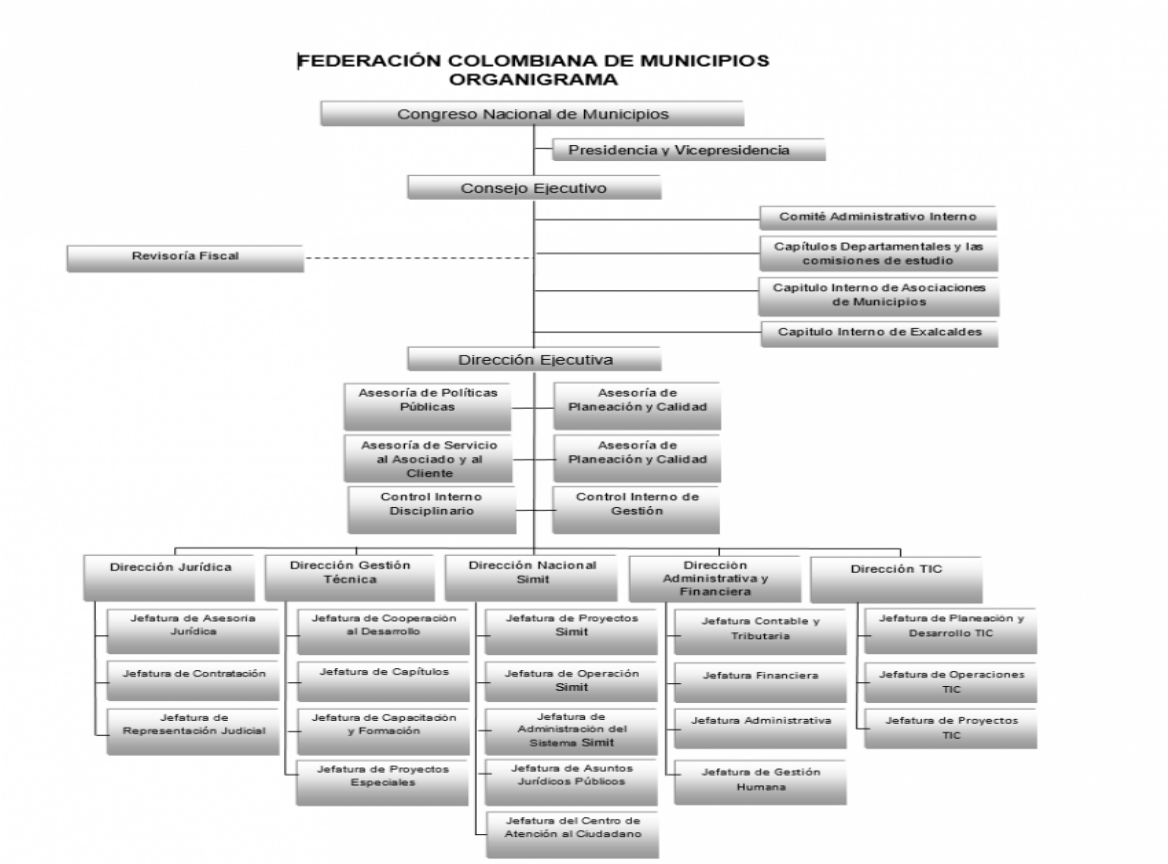
5.1.5 Visión[6]

Para el año 2020 el Sistema Integrado de Información sobre Multas y Sanciones por Infracciones de Tránsito - SIMIT será el referente en Latinoamérica con los más altos estándares de innovación, calidad y confiabilidad.

[5] Misión de la Federacion Colombiana de Municipios. [En linea]. Disponible en:<http://www.fcm.org.co/?page_id=715>
[6] Visión de la Federacion Colombiana de Municipios. [En linea]. Disponible en: <http://www.fcm.org.co/?page_id=715>

Seremos la mejor experiencia de gobierno en línea y la principal fuente de información para las políticas públicas de seguridad vial, garantizando la nivelación tecnológica de los organismos territoriales de tránsito, y consolidándonos como un sistema invulnerable que asegure la satisfacción del usuario y la rentabilidad social**.**

Figura 2 – Organigrama Federacion Colombiana de Municipios.



Fuente: Activos de Informacion FCM.

5.1.6 Mapa de Procesos

En la vista de procesos de negocio detallaremos la descomposición de los macro procesos organizacionales en los procesos que transforman realmente estas entradas en las salidas deseadas.

Dentro de la estructura funcional de la Organización solo se ha contemplado la generación de la descripción general de los procesos sin incluir detalle de procedimientos ni guías de operación.

Figura 3 – Procesos Estrategicos

Fuente: Activos de Informacion FCM.

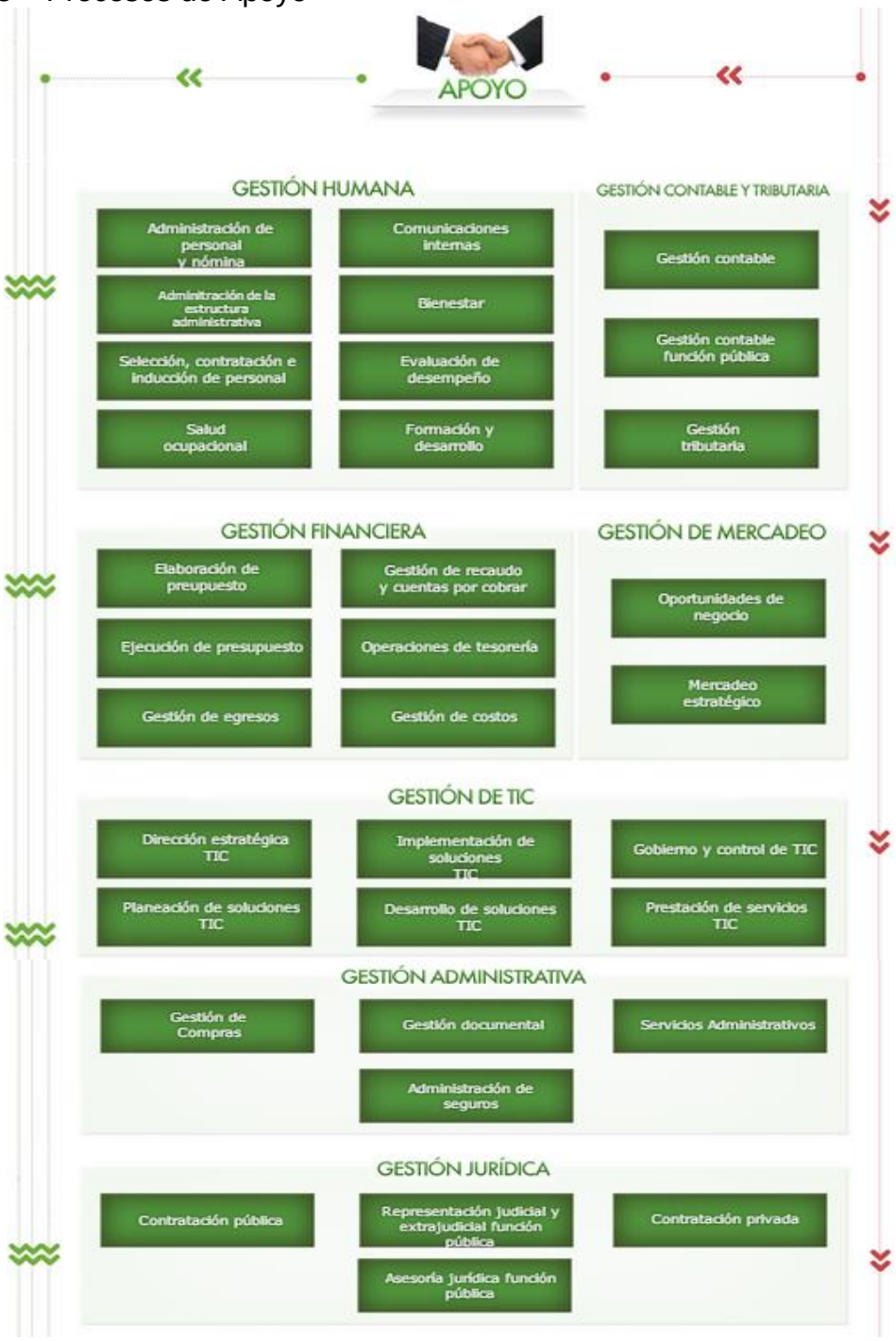
El macro proceso estratégico no posee subdivisiones organizativas de sus procesos. Engloba toda su operación en un solo proceso.

Figura 4 – Procesos Misionales

Fuente: Activos de Informacion FCM.

Vemos en el diagrama anterior los veinticuatro (26) procesos correspondientes al macro proceso misional, segmentados por las respectivas Jefaturas, Direcciones y Asesorías encargadas de cada tema.

Figura 5 – Procesos de Apoyo



Fuente: Activos de Informacion FCM.

El diagrama anterior presenta los treinta y tres (33) procesos enmarcados dentro del macro proceso de Apoyo, segmentados por las respectivas Direcciones encargadas. Las Direcciones responsables directamente de los procesos son la Dirección TIC, la Dirección Administrativa y Financiera y la Dirección Jurídica.

Figura 6 –Procesos de Control y Evaluación

Fuente: Activos de Informacion FCM.

En la imagen podemos contemplar los cinco (5) procesos que hacen parte de Control y Evaluación. Los responsables de los procesos son la Asesoría de Planeación Estratégica y Calidad y Control Interno.

Para ver todas las caracterizaciones de los procesos de la entidad, remitirse al siguiente link:

https://www.fcm.org.co/mapa-de-procesos/

5.3 MARCO TEORICO

La Federacion Colombiana de Municipios con base a los señalado por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión[1].

[1] Ministerio de Tecnologias de la Informacion y las Comunicaciones [En linea]. Disponible en: < http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html>

El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

A nivel metodológico es importante tener presente que el (MSPI) cuenta con una serie de guías anexas que ayudarán a las entidades a cumplir lo solicitado permitiendo abordar de manera detallada cada una de las fases del modelo, buscando a su vez comprender cuáles son los resultados a obtener y como desarrollarlos, incluyendo los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.

La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.

Mediante la adopción del Modelo de Seguridad y Privacidad por parte de las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

Por el anterior marco teorico, el Director del Proyecto asignado en la FCM para desarrollar el presente proyecto es el Oficial de Seguridad de la Información de la entidad, mediante el cual es el encargado de dirigir, coordinar y definir la estrategia e implementación de la Seguridad y Privacidad de la Información, con base a los lineamientos, instrumentos, artefactos y guías que dispone el programa de la Estrategia de Gobierno en Línea.

Por lo tanto, el proyecto será realizado con los recursos propios de la Dirección de Tecnologías de la Información y las Comunicaciones, y demás actores de la entidad que se involucren en el desarrollo de actividades para el diseño e Implementación del Modelo de Seguridad y Privacidad de la Información en la Federación Colombiana de Municipios – Dirección Nacional Simit.

Fomentando la proactividad y eficiencia administrativa de la entidad, en el año 2016 se evidencia avances en la implementación del Modelo de Seguridad y Privacidad de la Información que dispuso el Ministerio de las Tecnologías de la Información y las Comunicaciones,esto conforme a los lineamientos de la Estrategia de Gobierno en Línea, sin embargo lo implementado no esta alineado a la estrategia de seguridad de la información de la entidad y se debe redefinir el ejercicio del diseño

del sistema de gestión de seguridad de la información con el fin que este perfectamente alineado al MSPI vigente de Mintic – Ministerio de Tecnologias de la Información y las Comunicaciones.

5.4 MARCO LEGAL

A continuación se referencian varias leyes y normatividades las cuales hacen referencia al marco legal en Colombia:

Decreto 2573 de 2014:

El marco de cumplimiento normativo que esta sujeto el desarrollo del proyecto es el decreto 2573 de 2014 y el 1078 de 2015, teniendo encuenta todas sus disposiciones legales en la contratación publica y privada según ley 80.

Ley 1273 de 2009:

Ley que estructura los delitos informáticos en Colombia, la cual añade dos nuevos capítulos al Código Penal Colombiano:

- Capitulo Primero: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

- Capitulo Segundo: De los atentados informáticos y otras infracciones. Como se puede ver en el primer capítulo, esta Ley está muy ligada a la ISO27000, lo cual coloca al País a la vanguardia en legislación de seguridad de la información, abriendo así la posibilidad de nuevas entradas con este tema.

Ley 603 de 2000:

Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

Ley Estatutaria 1266 del 31 de Diciembre del 2008:

Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 del 5 de Enero del 2009:

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 del 30 de julio del 2009:

Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

Ley 599 de 2000:

Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de “violación ilícita de comunicaciones”, se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el “Acceso abusivo a un sistema informático”, así: “Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa.”

NORMA ISO/IEC 27001:2013:

Estándar internacional que se aplica para la gestión de la seguridad de la información. Al manejar el Sistema de Gestión de Seguridad de la Información SGSI, se busca minimizar los riesgos, para esto se deben establecer procesos y procedimientos que ayuden a la organización a llegar a la excelencia.

5.5 MARCO CONCEPTUAL

El Diseño del Sistema de Gestión de Seguridad de la Informacion con base al Modelo de Seguridad y Privacidad de la Información, se desarrollara con la recopilación de las guías de seguridad y privacidad de la información del programa de la Estrategia de Gobierno en Línea, mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL[2].

[2] Ministerio de Tecnologias de la Informacion y las Comunicaciones [En linea]. Disponible en: < http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html>

La Estrategia de Gobierno en Línea, liderada por la Dirección de Tecnologías de la Información y las Comunicaciones de la Federación Colombiana de Municipios – Dirección Nacional Simit, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de ofrecer servicios de tecnología con altos estándares de seguridad y privacidad de la información, de tal manera que contribuye con la construcción de un Estado más participativo, más eficiente y más transparente, hacia las autoridades de tránsito y municipios del País.

6. DISEÑO METODOLOGICO

6.1 Metodologia de la Investigación

La metodología investigativa del proyecto de Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) con base al Modelo de Seguridad y Privacidad de la Información según lineamentos del Ministerio de las Tecnologías de la Información y las Comunicaciones en el marco de la estrategia GEL (Gobierno en Línea), permitirá que el diseño metodológico logre describir la estrategia de seguridad de la información que requiere la institución, y generar una trasferencia social de conocimiento que contribuye de manera innovadora a la solución de problemas de seguridad de la información; por lo tanto, podemos definir que el tipo de proyecto es **aplicado y el tipo de investigación es de tipo descriptivo.**

Por ende, el proyecto de diseño del SGSI con base al MSPI, se desarrollara contemplando el repositorio y guias de conocimiento del Ministerio de las Tecnologias de la Informacion y las Comunicaciones, mediante el cual el objetivo principal es lograr avances significativos para la alineación del SGSI con el Modelo de Seguridad y Privacidad de la Información de la Federacion Colombiana de Municipios, por lo tanto la metodología para la ejecución del proyecto estará basada en la gestión de proyectos PMI y esto emplea fuentes y técnicas de recoleccino de información conforme al modelo gestión integral de proyectos de la FCM – Federacion Colombiana de Municipios, el cual esta comprendida y estructurada de la siguiente forma:

6.2 Metodologia de Desarrollo

Los proyectos en la Federación Colombiana de Municipios, generalmente se ha definido aplicar el marco metodológico para su formulación **“ Metodología General Ajustada”** con el propósito de gestionar la Formulación y Evaluación de Proyectos de Inversión Pública (MGA) de acuerdo al decreto 2844 de 2010;articulo 5; teniendo en cuenta esto, en la etapa de Inversión se desarrollan los procesos de ejecución y seguimiento del proyecto, para estos procesos la entidad gestiona dentro de su **“Modelo Gestión Integral de Proyectos”** mejores prácticas y metodologías agiles de proyectos reconocidas en la industria a nivel nacional e internacional como PMI y Scrum. para todo tipo de proyecto, incluyendo los proyectos de “construcción, desarrollo e implementación de sistemas de información”.

Figura 7 – Mapa Gestión de Proyecto MGA

Fuente: Activos de Informacion FCM.

Figura 8 – Alineacion MGA con PMI

Fuente: Activos de Informacion FCM.

Aspectos Generales – Metodología PMI:

Aplicando la metodología PMI; los Directores de Proyectos deben alinearse al Modelo Gestión Integral de Proyectos de la Federación Colombiana de Municipios.

Esto indica que se deberán desarrollar los siguientes planes de gestión para la Dirección del Proyecto:

1. Plan de Gestión de la Configuración
2. Plan de Gestión de Cambios
3. Plan de Gestión del Alcance
4. Plan de Gestión de Requisitos

5. Plan de Gestión del Tiempo
6. Plan de Gestión del Costo
7. Plan de Gestión de la Calidad
8. Plan de Gestión de Mejoras de Procesos
9. Plan de Gestión de los Recursos Humanos
10. Plan de Gestión de las Comunicaciones
11. Plan de Gestión del Riesgo
12. Plan de Gestión de las Adquisiciones
13. Plan de Gestión de los StakeHolders

El Plan de Dirección del Proyecto debe ser desarrollado de tal manera que exprese la realización de los 13 planes de gestión de proyectos para el presente proceso y proyecto, es decir que se tendrá en cuenta las 10 áreas del conocimiento, los 47 procesos y los 5 grupos de procesos para la gerencia del proyecto que indica el PMI en su 5ta Edición. **"No obstante en la reunión de kick – off, se debe acordar los planes de gestión del proyecto y la metodología que se desarrollara para la ejecución del proyecto"**.

Al finalizar el desarrollo de los planes de gestión acordados, el acta de constitución del proyecto y el plan para la dirección del Proyecto, esto se consolidará en el Plan Integral para la Dirección del proyecto que maneja la FCM.

Nota 1:
Por lo anterior todos los planes de gestión, el plan para la dirección del proyecto, el plan integral para la dirección del proyecto y toda gestión y actividad que se realice durante el ciclo de vida del proyecto, debe ser mediante los formatos que la Jefatura de Proyectos de la Dirección de las Tecnologías de la Información y las Comunicaciones posee como activos de información de acuerdo al modelo de gestión integral de proyectos de la Federación Colombiana de Municipios.

El Director del Proyecto debe agregar en el Plan de Dirección del Proyecto cada componente y variable, es decir los ITTOS (Entradas, Herramientas, Técnicas y Salidas) de los procesos que se utilizara para el desarrollo y ejecución del Proyecto según PMI.

El Modelo Integral de Gestión de Proyectos de la Federación Colombiana de Municipios está basado en el uso de las diferentes herramientas tecnológicas que posee a nivel organizacional con el fin de fortalecer el desarrollo del proyecto sin importar su tamaño y complejidad, de este modo se manejaran las herramientas, activos de la organización y sistemas de tecnología con el fin que se gestione el ciclo de vida del proyecto de manera adecuada y en equipo con el contratista, realizando un seguimiento y control de manera satisfactoria y entregando a la Federación Colombiana de Municipios el nivel de control de calidad requerida para que el proyecto sea exitoso.

Figura 8 –Modelo Gestión Integral de Proyectos FCM

Fuente: Activos de Informacion FCM.

Herramientas Tecnológicas del Modelo Integral Gestión de Proyectos:

- ✓ Plataforma Dirección y Gestión de Proyectos TALAIA
- ✓ Plataforma Comunidad FCM
- ✓ Paquete de Microsoft Office
- ✓ Project Libre – Open Project
- ✓ Skype Business
- ✓ SAP
- ✓ Documentos exigidos en los Requisitos mínimos de Entrada, Ejecución y Cierre del Proyecto.

Nota 2: Todos los entregables del proyecto deben suministrarse de manera organizada y paginada, en formato editable (MsWord) y no editable (Pdf) sobre medio magnético (CD y/o DVD), a su vez impreso con excelente resolución.

6.3 Poblacion y Muestra

Como población y muestra, en esta labor investigativa se definio en primer lugar el alcance de aplicabilidad del MSPI (Modelo de Seguridad y Privacidad de la Información) y se decide que es para todas las areas de la entidad, el cual esto implica que se revisaran y validaran todos los activos de informacion de la entidad y se solicita a la presidencia de la FCM, un equipo de profesionales idoneo para la Direccion y Gestión del proyecto de grado, a su vez se comprende que los entregables del Proyecto estaran enmarcados a nivel de cumplimiento en la incorporacion de los procesos estrategicos, misionales y de apoyo para la entidad, y esto se deriva que la gestion y estrategia de seguridad de la informacion que se diseñe e implemente aplicara para todos los funcionarios y colaboradores de la Federacion Colombiana de Municipios.

A continuación se relaciona el equipo del Proyecto en la Federacion Colombiana de Municipios:

Tabla 1: Equipo de Proyecto FCM.

Nombre y apellido	**Rol**	**Correo**	**Celular**
Ronald Cely	CISO – Oficial de Seguridad de la Información.	Ronald.cely@fcm.org.co	3165377731
Edgar Mauricio Abaunza	Jefe de Operaciones TIC	Edgar.abaunza@fcm.org.co	5934020
Germán Duque	Profesional en Administración de Infraestructura y Redes	German.duque@fcm.org.co	5934020
Astrid Barón	Profesional en Administración en Bases de Datos Oracle	Astrid.baron@fcm.org.co	5934020
Eduard Fonseca	Profesional en Administración de Servidores Windows y Linux	Eduard.fonseca@fcm.org.co	5934020
Edwin Alexander Beltrán Riveros	PMO – TIC	edwin.beltran@fcm.org.co	5934020
Alejandro Murillo Pedroza	CIO - Director TIC	Alejandro.murillo@fcm.org.co	5934020

Fuente: El Autor.

7. RESULTADOS Y DISCUSIÓN

Entregables del Proyecto: A continuación se contemplan 3 etapas para el desarrollo del proyecto y sus entregables.

Tabla 2: Etapa 1.

Etapa 1: Identificación de Vulnerabilidades y Analisis y Evaluacion de Riesgos
Diseño Metodologico para realizar un Ethical Hacking
Ejecucion de Ethical Hacking e Informe Final Ejecutivo y Tecnico de Ethical Hacking
Acta de Socializacion del Informe Ejecutivo y Tecnico del Ethical Hacking
Analisis y Evaluacion de Riesgos de los Activos de Informacion de la Entidad deacuerdo al Modelo Seguridad y Privacidad de la Informacion dispuesto por Mintic

Fuente: El Autor.

Tabla 3: Etapa 2.

Etapa 2: Diseño del MSPI, Capacitación y sensibilización en FCM
Alineacion del SGSI al MSPI
Charla Presencial sobre las politicas de Seguridad de la Informacion del MSPI en FCM
Control de Asistencia de la Charla Presencial
Plan de Sensibilización del (MSPI) Modelo de Seguridad y Privacidad de la Informacion en FCM
Plan de Implementacion para el (MSPI) Modelo de Seguridad y Privacidad de la Informacion en FCM

Fuente: El Autor.

Tabla 4: Etapa 3.

Etapa 3: Asesorías
Documentos de Diseño del centro de respuesta para atención de incidentes de seguridad CSIRT.
Diseño/Revisión de las metodologías y procedimientos forenses que debe seguir la Federación Colombiana de Municipios – Dirección Nacional SIMIT.
Socialización de cada uno de los documentos y metodologías con las personas que designe el supervisor del proyecto.

Fuente: El Autor.

7.1 Cronograma de actividades

A continuación se visualiza el cronograma del proyecto:

Tabla 5: Cronograma.

CRONOGRAMA DEL PROYECTO - DISEÑO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION EN FCM-DNS EJECUCION DEL PROYECTO DESDE EL 01 DE SEPTIEMBRE DE 2017 AL 07 DE DICIEMBRE DE 2017																			
			SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE			
ETAPAS	ACTIVIDAD	RECURSOS HUMANOS	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4	Semana 1	Semana 2	Semana 3	Semana 4
1	**Formulación y Planificación del Proyecto**																	
1.1	Formulacion, Planeación y Formalización del Anteproyecto	CISO - Ing. Ronald Cely.																
2	**Inicio del Proyecto**																	
2.1	Acta de Inicio del Proyecto	CISO - Ing. Ronald Cely.	x															
2.2	Acta de Constitución del Proyecto	CISO - Ing. Ronald Cely.	x															
2.3	Acuerdo de Confidencialidad del Proyecto	CISO - Ing. Ronald Cely.	x															
Ejecucion 3.	**Etapa 1: Identificación de Vulnerabilidades y Analisis y Evaluacion de Riesgos**																	
3.1	Diseño Metodologico para realizar un Ethical Hacking	CISO - Ing. Ronald Cely.	x	x														
3.2	Ejecucion de Ethical Hacking e Informe Final Ejecutivo y Tecnico de Ethical Hacking	CISO - Ing. Ronald Cely.	x	x	x	x												
3.3	Acta de Socializacion del Informe Ejecutivo y Tecnico del Ethical Hacking	CISO - Ing. Ronald Cely.		x	x	x												
3.4	Analisis y Evaluacion de Riesgos de los Activos de Informacion de la Entidad deacuerdo al Modelo Seguridad y Privacidad de la Informacion dispuesto por Mintic	CISO - Ing. Ronald Cely.	x	x	x	x	x											
Ejecucion 4.	**Etapa 2: Diseño del MSPI, Capacitación y sensibilización en FCM**																	
4.1	Alineacion del SGSI al MSPI	CISO - Ing. Ronald Cely.					x	x	x	x	x	x	x					
4.2	Charla Presencial sobre las politicas de Seguridad de la Informacion del MSPI en FCM	CISO - Ing. Ronald Cely.								x								
4.3	Control de Asistencia de la Charla Presencial	CISO - Ing. Ronald Cely.								x								
4.4	Plan de Sensibilización del (MSPI) Modelo de Seguridad y Privacidad de la Informacion en FCM	CISO - Ing. Ronald Cely.					x	x	x	x	x	x	x					
4.5	Plan de Implementacion para el (MSPI) Modelo de Seguridad y Privacidad de la Informacion en FCM	CISO - Ing. Ronald Cely.					x	x	x	x	x	x	x					

Tabla 5: Continuacion “Cronograma”

Ejecucion 5	Etapa 5: Asesorias																		
5.1	Documentos de Diseño del centro de respuesta para atención de incidentes de seguridad CSIRT.	CISO - Ing. Ronald Cely.										X	X						
5.2	Diseño/Revisión de las metodologías y procedimientos forenses que debe seguir la Federación Colombiana de Municipios – Dirección Nacional SIMIT.	CISO - Ing. Ronald Cely.								X	X	X	X						
5.3	Diseño de un plan metodológico para los Hacking Éticos que van a ser realizados con el fin de estandarizar futuros análisis.	CISO - Ing. Ronald Cely.								X	X	X	X						
5.4	Diseño de procedimientos y metodologías para el combate del fraude electrónico que se pueda presentar en la organización	CISO - Ing. Ronald Cely.								X	X	X	X						
5.5	Socialización de cada uno de los documentos y metodologías con las personas que designe el supervisor del proyecto.	CISO - Ing. Ronald Cely.												X					
Cierre - 6	Cierre del Proyecto																		
6.1	Acta de Socializacion y Aceptacion de Entregables del Proyecto	CISO - Ing. Ronald Cely.												X	X				
6.2	Acta de Cierre del Proyecto	CISO - Ing. Ronald Cely.													X				

8. ENTREGABLES ETAPA 1

8.1 PROCEDIMIENTO METODOLOGICO PARA REALIZAR UN ETHICAL HACKING Y ELABORACION DEL REPORTE Y/O INFORME DE SEGURIDAD INFORMATICA.

OBJETIVO

El presente documento tiene como objetivo consignar la metodología que debe ser utilizada como mejor práctica para la ejecución de Pruebas de Vulnerabilidad, Ethical Hacking y elaboración de informes de Seguridad Informática, a la infraestructura tecnológica, servicios y aplicaciones web de la Federación Colombiana de Municipios y/o colaboradores con su previa autorización.

ALCANCE

La metodología para la ejecución de pruebas de Vulnerabilidad y Ethical hacking tiene como alcance: Documentar las mejores prácticas de seguridad para la ejecución de pruebas técnicas a la infraestructura y aplicaciones Web de la FCM y/o sus colaboradores, que permitan identificar y verificar servicios vulnerables frente a diferentes tipos de ataque. Lo anterior incluye:

Pruebas sobre servicios y aplicaciones web.
Pruebas sobre servicios de red y comunicaciones.
Pruebas sobre Sistemas de información, sistemas operativos y bases de datos.

METODOLOGÍA INTEGRAL DE ETHICAL HACKING

La metodología consignada en el presente documento utiliza como base los siguientes marcos de referencia:

OSSTMM (Open Source Security Testing Methodolgy Manual)
OWASP (Open Web Application Security Project)
The National Institute of Standards and Technology (“NIST”) Special Publication 800-115
Penetration Testing Execution Standard
CEH (Certified Ethical Hacker)

De acuerdo con lo anterior, a continuación, se presenta la metodología FCM, la cual contiene 5 fases y una adicional que permiten cumplir con el objetivo propuesto.

METODOLOGÍA (“NIST”) Special Publication 800-115:
La metodología presentada está construida a través de un ciclo de 5 Fases, sin embargo, se incorpora una adicional como mejor practica por la experiencia profesional del ejecutor de las pruebas de identificación y explotación de vulnerabildiades, en las cuales se evalúan los componentes de infraestructura y aplicaciones, servicios, plataformas web, entre otras; de tal forma que sea eficiente y optima la identificación de vulnerabilidades dentro de FCM y/o entidades de los colaboradores.

Figura 9 - Listado de fases y su orden de ejecución:

Sin embargo, antes de presentar cada una de las fases, la metodología sugiere implementar las fases de acuerdo con el siguiente orden tecnico:

Ejecución de Fase 1 y Fase 2 sobre la red Externa
Ejecución de Fase 1 y Fase 2 sobre la red Interna
Ejecución de la Fase 3. sobre las redes Interna y Externa
Ejecución de la Fase 4 sobre la red Externa
Ejecución de la Fase 4 sobre la red Interna
Ejecución de la Fase 6 sobre las redes Interna y Externa

Así mismo, se deben aplicar las fases de acuerdo con el siguiente sub-orden, que corresponde la selección de algunos componentes de la Metodologia Integral de Ethical Hacking.

Servidores (Sistema operativo)
Bases de datos
Aplicaciones Cliente Servidor
Aplicaciones Web
Dispositivos de Red

Dispositivos perimetrales de seguridad y disponibilidad

FASE 1. RECONOCIMIENTO, ESCANEO DE PUERTOS Y SERVICIOS

Objetivo

Esta fase tiene como objetivo la ejecución de tareas de reconocimiento y escaneo de puertos y servicios, que permitan a la FCM hacer el levantamiento de información técnica, así como el mapa de servicios de red que actualmente tiene la infraestructura.

Actividades:

Para llevar completar con éxito esta fase se deben realizar las siguientes actividades:

Reconocimiento de los objetivos (equipos) a evaluar:

Esta tarea consiste en realizar el reconocimiento de los equipos que serán objetivo de las pruebas de vulnerabilidad y Ethical Hacking. Sin embargo, para el reconocimiento se debe llevar a cabo de 2 formas:

Reconocimiento a través de herramientas automatizadas, en las cuales es posible proporcionar los datos de conexión de cada una de las redes para que la herramienta realice el reconocimiento e identificación de equipos en la red.
Sin embargo, dado que muchos de los equipos no son reconocibles a través de herramientas automatizadas, para equipos o direcciones IP para las cuales se tenga duda, debe realizarse el reconocimiento manual a través de:

Pruebas de conexión a los servicios (Ej. Telnet, Ping, etc.)
Modificación de las banderas TCP (Ej. Syn, Ack, Urg, Psh) en cada uno de los paquetes con el fin de determinar si el equipo objetivo se encuentra activo o se encuentra protegido por un dispositivo perimetral o de red.
Ataques de ARP Spoofing. Estos ataques permiten suplantar un equipo dentro de la red con el fin de identificar la información que se transmite hacia o desde el equipo objetivo. (Mas información en la descripción de la fase 4, Explotación.)

Instalación de las herramientas para efectuar la prueba.

Para llevar a cabo esta tarea se deben consultar las herramientas necesarias para el descubrimiento de puertos y servicios, así como obtención de información, de acuerdo con lo requerido por cada aplicación evaluada. Algunas de las herramientas que se pueden usar para esta tarea son:

NMAP, SuperScan, acccheck, ace-voip, Amap, Automater, bing-ip2hosts, braa, CaseFile, CDPSnarf, cisco-torch, Cookie Cadger, copy-router-config, DMitry, dnmap, dnsenum, dnsmap, DNSRecon, dnstracer, dnswalk, DotDotPwn, enum4linux, enumIAX, entre otras.

Nota:

A la fecha se listan las anteriores herramientas como ejemplo. Sin embargo, cada vez que se utilice esta metodología debe verificarse si existen nuevas o mejoras en las herramientas utilizadas. Lo anterior con el fin de que no se utilicen herramientas no soportadas o versiones obsoletas de las mismas, así como herramientas que ya no se encuentren disponibles.

Para la red interna, conexión a la red interna por medio de un cable de red en un punto que permita tener acceso a los dispositivos a evaluar.

Dependiendo del tipo de prueba, caja negra (sin ningún privilegio) caja gris (con alguna información) o caja blanca (Con todos los privilegios), el punto de conexión debe tener los accesos requeridos para poder realizar la prueba efectivamente.

Es importante tener en cuenta que la presente metodología recomienda realizar las pruebas en el siguiente orden:

Prueba de caja Blanca a todos los equipos. Es decir, realizar la prueba con todo el acceso a los equipos objetivo.
Prueba de caja negra a todos los equipos. Es decir, simular un atacante en la red tal como si fuera un usuario sin privilegios.
Comparación de caja negra Vs Caja blanca. Aquí se puede determinar el nivel de implementación de controles de seguridad dentro de la compañía.

Para los equipos de tipo perimetral, conexión a través de internet.

Se deben realizar los mismos pasos realizados en la prueba interna.

Extraer los reportes necesarios como evidencia de la actividad.

Cada una de las actividades debe quedar documentada con el fin de poder ser analizada y verificada de forma posterior. Esto permite preparar las siguientes fases para la ejecución de las pruebas de explotación.

FASE 2. IDENTIFICACIÓN DE VULNERABILIDADES

Objetivo

Esta fase contempla la verificación de los servicios vulnerables previamente identificados. Sin embargo, las pruebas de verificación a estos servicios solo se realizan en los casos donde no se genera una afectación o degradación del servicio, de tal forma que permita identificar servicios vulnerables en un tiempo corto y también servicios vulnerables que requieren una explotación más significativa, que pueda llegar a causar afectación en dicho servicio.

Actividades

Para la ejecución de esta fase se llevan a cabo los siguientes pasos:

Instalación y estructuración de los objetivos (equipos) a evaluar. Los previamente mencionados en la fase 1.

Instalación de las herramientas para efectuar la prueba. En este caso se nombran algunas herramientas que pueden ser de ayuda para realizar el escaneo de vulnerabilidades:
Nessus, Acunetix, Nexpose, Nikto, W3AF, Wikto, Vega, Netsparker, ZAP, entre otras.

Para la red interna, conexión a la red interna por medio de un cable de red en un punto que permita tener acceso a los dispositivos a evaluar.

Nota: Tener en cuenta las recomendaciones del tipo de prueba, mencionadas en la Fase 1.

Para los equipos de tipo perimetral, conexión a través de internet.

Correr la herramienta de identificación de vulnerabilidades.

Extraer los reportes necesarios como evidencia de la actividad. Es importante tener en cuenta que una vez las vulnerabilidades hayan sido identificadas, deben extraerse los reportes necesarios, con el fin de ser analizados posteriormente, así como mantener una copia de respaldo de cada herramienta. (Ej. existen herramientas que mantienen los resultados de forma temporal. Por lo tanto, podría perderse el resultado de la prueba si no se generan los reportes.)

FASE 3. ANÁLISIS DE RESULTADOS INICIAL Y CONSTRUCCIÓN DEL PLAN DE EXPLOTACIÓN

Alcance

Esta fase tiene como alcance, el Análisis de resultados inicial y la construcción del plan de explotación sobre las vulnerabilidades identificadas en la Fase 2.

Objetivo

La construcción del plan de explotación se lleva a cabo una vez se tienen identificadas las vulnerabilidades que deben comprobarse mediante técnicas mas avanzadas que pueden llegar a generar afectación de servicio. Sin embargo, cada una de las pruebas que se documenta dentro del plan de explotación, es previamente evaluada, con el fin de determinar si la prueba genera degradación o afectación parcial/total de los servicios.

De igual forma, todo el documento de plan de explotación es presentado previamente a los involucrados con el fin de contar con la respectiva aprobación antes de proceder con la fase de explotación.

Actividades

Para la ejecución de esta fase se llevan a cabo los siguientes pasos:

Analizar los resultados obtenidos en las pruebas de vulnerabilidad realizadas en la Fase 2.

Las vulnerabilidades que deberían ser comprobadas se determinan de acuerdo con las siguientes premisas de evaluación:

Si la vulnerabilidad se encuentra descubierta por 2 herramientas con el mismo numero de CVE, entonces NO se comprueba mediante explotación. Lo anterior, dado que el script que es probado por las herramientas, determina que en efecto la vulnerabilidad no existe.
Si la vulnerabilidad identificada por la herramienta tiene exploit público en internet, pero no tiene un CVE asociado, entonces deberá comprobarse mediante explotación.
Si la vulnerabilidad identificada por la herramienta puede tener vulnerabilidades derivadas que no han sido detectadas por la herramienta, entonces deberá comprobarse si en efecto existe. Lo anterior se identifica dada la experiencia del consultor o ejecutor de las pruebas de seguridad.

Las vulnerabilidades que tengan el nivel mas critico identificado por la herramienta, que para la compañía mantenga el mismo nivel de criticidad y que cuenten con exploit en internet, entonces deberán probarse.

Si la vulnerabilidad es estándar (Por ejemplo, defectos de protocolo), con un nivel critico y se encuentra identificada en varios equipos de la red, entonces se realiza la comprobación en un solo equipo. Esto permite que se determine si los demás equipos, que tienen las mismas características, cuentan con esta vulnerabilidad.

Por experiencia del consultor o del ejecutor de las pruebas, deberán comprobarse las vulnerabilidades que sean consideradas como relevantes y con duda.
Documentar los hallazgos y construir el plan de explotación.

Para esta actividad, es importante mencionar que adicional a la comprobación de las vulnerabilidades identificadas, se deben tener en cuenta los siguientes tipos de ataque:

Identificación de acceso a recursos por sesiones CIIFs
Identificación de recursos compartidos y archivos dentro de cada equipo.
ARP Spoofing. Técnica en la cual se hace suplantación de un equipo y su respectivo Gateway (puerta de enlace) con el fin de visualizar el tráfico que se envía entre cada punto, permitiendo identificar datos sensibles como nombres de usuario, contraseñas, data, etc.

En esta prueba se pueden utilizar algunas de las siguientes herramientas: NetSCAN, Cain&Abel, Ettercap, Wireshark, entre otras.
Pruebas a la red Inalámbrica. Esta prueba incluye, la captura de los paquetes de autenticación (en caso de ser WPA-WPA2) y posteriormente efectuar un ataque de diccionario para determinar la clave respectiva.

Para esta prueba puede utilizarse la herramienta Aircrack.

Entregable:

En esta fase se entrega el Plan de Explotación. El cual es un archivo de MS Excel con el listado de pruebas a ejecutar el cual incluye:

- ID de la prueba
- Nombre de la prueba
- Descripción de la prueba
- Equipos objetivos
- Duración de la prueba
- Nivel de afectación de la prueba

Nota:

Una vez este documento sea entregado, éste deberá ser verificado y aprobado por los involucrados con el fin de ajustar el plan o proceder con la siguiente fase de Explotación.

FASE 4. EXPLOTACIÓN.

Objetivo

Esta fase contempla la ejecución de las pruebas alternativas de verificación de vulnerabilidades, que podrían llegar a generar afectación de servicio. Por lo tanto, se realizan en los horarios definidos previamente por la compañía, dentro del cual se ejecutan los ataques de forma monitoreada y controlada, con el fin de prevenir cualquier falla o afectación en las operaciones normales de los servicios evaluados.

Actividades

Para la ejecución de esta fase se llevan a cabo los siguientes pasos:

Instalación y estructuración de los objetivos (Equipos) a evaluar.
Instalación de las herramientas para efectuar las pruebas de explotación.

Como recomendación dentro de la presente metodología se sugiere el uso de el marco de trabajo para pruebas de penetración Kali Linux, Metasploit Framework o Samurai, entre otros.

Para la red interna, conexión a la red interna por medio de un cable de red en un punto que permita tener acceso a los dispositivos a evaluar. Deben tenerse encuentra los requisitos mencionados en la Fase 1.
Para los equipos de tipo perimetral, conexión a través de internet.
Para la red Wireless, la prueba se realiza dentro de las instalaciones de la compañía.
Correr las herramientas y capturar los resultados. (Tener en cuenta lo mencionado en la Fase 2.)
Actualizar el plan de explotación. Esto contempla marcar cada ataque como “Exitoso” o “No exitoso” y documentar los resultados de cada ataque.

FASE 5. ELABORACIÓN Y PRESENTACIÓN DEL REPORTE

Objetivo

Esta es la ultima fase que contempla el esquema de pruebas de Vulnerabilidad y Ethical Hacking. Por lo tanto, se consolida y se consigna toda la información recopilada dentro de las pruebas realizadas, lo que permite a la compañía, conocer

el estado final de evaluación de seguridad técnica sobre la infraestructura, así como corregir dichos hallazgos en el menor tiempo posible.

Actividades

Para la ejecución de esta fase se llevan a cabo los siguientes pasos:

Analizar los resultados obtenidos en las pruebas explotación
Documentar los hallazgos identificados en las Fases 1, 2, 3 y 4 y elaborar el informe final.

El informe final debe contener por lo menos la siguiente información:

Introducción
Objetivo del informe
Alcance. (Equipos objetivos)
Resumen ejecutivo, indicando el total de vulnerabilidades de acuerdo con su nivel de criticidad, vector de explotación (interno, externo).
Hallazgos mas representativos
Conclusiones
Recomendaciones, junto con las actividades de remediación de cada vulnerabilidad.

Realizar la presentación del informe a los involucrados.

FASE 6 (Adicional). PRUEBA DE VERIFICACIÓN DE REMEDIACIÓN.

En esta fase adicional, se realiza el escaneo de vulnerabilidades luego de efectuada la remediación. El objetivo es validar si se implementaron las recomendaciones de remediación de las vulnerabilidades relacionadas en el informe inicial. En este caso solo se aplica la Fase 2 del presente documento.

Como resultado de esta fase, se debe realizar la comparación de resultados indicando:

Vulnerabilidades remediadas
Vulnerabilidades pendientes por remediar
Vulnerabilidades nuevas.

Lo anterior se relaciona dentro del informe de resultados de las pruebas realizadas.

NIVEL DE CLASIFICACION DE LAS VULNERABILIDADES

Las vulnerabilidades se clasifican de acuerdo con los siguientes niveles:

Alto

La explotación de una vulnerabilidad con nivel Alto podría proporcionar acceso a datos y sistemas no autorizados, en la mayoría de los casos a un nivel de administración.

El riesgo contempla la exposición de información sensible, tal como identificadores de usuario (nombres), contraseñas, información propietaria, secretos, números de tarjetas de crédito, información de clientes, de colaboradores u otra información sensible de la organización. Así mismo, podría llegar a generar Denegación de Servicio que impacte de manera importante la continuidad de las operaciones.

En este nivel se encuentran aquellas vulnerabilidades que son lo suficientemente significativas para causar un impacto negativo en el negocio. Por lo tanto, se sugiere que sean corregidas de forma inmediata.

Medio

Las explotaciones de vulnerabilidades con nivel Medio podrían permitir indirectamente acceso a archivos de configuración, datos, o afectar parcialmente un sistema de información.
Se sugiere que estos hallazgos sean corregidos en un breve plazo para su análisis y resolución.

Bajo

La explotación de una vulnerabilidad con nivel Bajo podría permitir a un atacante obtener información estadística de un sistema, cuentas de usuarios u otra información que podría ser usada para crear un nuevo vector de ataque. Estos hallazgos podrán ser analizados, planificados y solucionados una vez se resuelvan los anteriores niveles de hallazgos que presentan mayor nivel de riesgo para la organización.

Recomendaciones:

Listado de posibles ataques a ejecutar como complemento a la fase 4. Explotación.

A continuación, se listan los ataques que podrían ejecutarse en caso de que exista una vulnerabilidad relacionada con el mismo. Sin embargo, esto no significa que todos los ataques apliquen a las pruebas que se realizarán en la compañía.

Pruebas de intrusión dentro de la red interna, tanto para la red alámbrica como para las redes inalámbricas.

Esta prueba consiste en la aplicación de técnicas de Sniffing, en las cuales se realiza el escaneo de paquetes transferidos a través de la red. Por lo tanto, una vez identificados los datos que viajan por la red, estos son capturados y analizados posteriormente para identificar debilidades en la transferencia de los mismos. Esta prueba es realizada a partir de la implementación de herramientas como Cain & Abel (www.oxid.it/cain.html) y Wireshark (https://www.wireshark.org)

Sin embargo, para las redes inalámbricas, aunque se llevan a cabo las mismas técnicas, esta es un poco mas avanzada. En el caso de las redes de SIMIT, se implementarán técnicas de espectro, en las cuales se pueden identificar tanto las redes inalámbricas como los clientes conectados a ellas. Estas pruebas se deben llevar a cabo bajo 2 esquemas diferentes:

- Pruebas de intrusión activas: En las cuales se realiza envío de paquetes de broadcast a cualquier canal inalámbrico con el fin de identificar respuestas por parte de los puntos de acceso (Access Point).

- Pruebas de intrusión pasivas: En esta técnica, se realiza un escaneo de espectro y frecuencias en todos los canales inalámbricos soportados, con el fin de identificar redes inalámbricas que se encuentren irradiadas dentro de estos.

Estas pruebas deben ser implementadas a través de las herramientas AirCrack (www.aircrack-ng.org) y/o Kali Linux (www.kali.org).

Pruebas de desbordamiento de buffer, intento de descubrimiento de contraseñas por medio de técnicas de fuerza bruta, ataques de diccionario o captura de información por medio de técnicas de sniffing entre otros.

Este tipo de pruebas serán ejecutadas utilizando varios tipos de herramientas, que permiten evaluar los diferentes puertos abiertos que tienen actualmente los dispositivos. Esto incluye, RPC (TCP 135-139), FTP (TCP 21), SNMP (UDP 161) y Telnet (TCP 23) entre otros, los cuales permiten la identificación de contraseñas en

texto claro, ejecución de exploits, escalamiento de privilegios y demás ataques de servicios embebidos en las plataformas.

Sin embargo, también se llevarán a cabo las pruebas de captura de contraseñas por SMB (TCP 445), con el fin de interceptar las transmisiones de cuentas del directorio activo para extraer los hashes LM y NTLM. De ser posible extraer esta ultima información, se efectuará el respectivo cracking de password por medio de tablas precomputadas. Esta prueba se debe llevar a cabo por medio de las herramientas Cain & Abel, Wireshark y Kali Linux.

Así mismo, el resumen de pruebas y las herramientas que se incluyen en esta categoría se presentan a continuación:

- Ataques de fuerza bruta

(Brutus,Hydra, Opcrack, john the ripper, metasploit, pwdump, medusa)

- Ataques “man-in-the-middle”

(Cain&Abel, ettercap, arpspoof, wireshark)

- Ataques de “buffer overflow”

(Metasploit, scapy-Python, BeEF)

- Ataques de SQL Injections

(SQLMAP, Acunetix, nikto, ZAP,Foxy-Proxy)

- Ataques de “cross-site scripting (XSS)”

(Curl, netcat, nikto, w3f, ZAP, Foxy-Proxy)

- Ataques contra configuraciones débiles de los sistemas

(Nmap, Nessus, portales web)

- Ataques contra protocolos específicos (telnet, ftp, rcp, snmp, smtp, etc)

(Snmpget, snmpset, snmpcheck, snmpwalk, metasploit, netcat, nbtscan, nmap, samdurmp, cliente telnet, rdesktop)

- Ataques contra resolución de nombres (DNS)

(Host, nslookup, maltego, dnsenum)

- Ataque sobre recursos compartidos

(NetScan)

- Ataques de puertas traseras (Backdoors)

(Msfencode)

Pruebas a la infraestructura pública, páginas, portales o aplicaciones web y demás servicios públicos del Sistema de Informacion sobre Multas y Sanciones por Infracciones de Transito.

Esta prueba consiste en enumerar los distintos URLs que se relacionan con el Sistema de Informacion sobre Multas y Sanciones por Infracciones de Transito (SIMIT), con el fin de determinar los servicios, y debilidades sobre la información publicada en internet y en el sistema Simit. Esto incluye intentos de descarga del

contenido de los sitios web, verificación de las debilidades dentro del código y malas configuraciones, así como la identificación general de vulnerabilidades.

Esta prueba se debe llevar a cabo por medio del uso de las herramientas Acunetix (www.acunetix.com) y Nexpose (www.rapid7.com/products/nexpose), entre otras.

Captura de paquetes de autenticación sobre la red inalámbrica, así como su respectivo Cracking por medio de diccionario y/o Fuerza Bruta.

Esta prueba consiste en efectuar la captura de los paquetes de autenticación de los clientes a la red inalámbrica. Esta técnica permite que dicho paquete capturado pueda ser sometido a ataques de fuerza bruta, con el fin de identificar la contraseña de la red inalámbrica. Para efectos de las pruebas, en caso de ser posible, se debe ejecutar este ataque sobres redes inalámbricas proporcionadas, las cuales posteriormente serán usadas para el ataque de diccionario y fuerza bruta de contraseñas.

Para realizar esta prueba se utilizará la herramienta AirCrack.

Suplantación del Gateway de usuarios, capturando información en transito, contraseñas, certificados, comunidades de monitoreo y demás servicio.

En esta prueba, se debe llevar a cabo el ataque IP-Spoofing, con el fin de suplantar el Gateway de la entidad, en este caso el equipo donde se reciben e intercambian paquetes de todas las redes. Posteriormente a este ataque la información capturada será analizada, identificando hash de contraseñas del dominio, comunidades de monitoreo y certificados de autenticación entre otros.

Para la ejecución de este ataque se utilizarán las siguientes herramientas: Cain & Abel (www.oxid.it/cain.html) y Wireshark (https://www.wireshark.org).

Pruebas de Cross-Site-Scripting, Cross-Site-Request-Forgery, SQL Injection y Code Injection sobre los servidores, aplicaciones web del Sistema de Informacion sobre Multas y Sanciones por Infracciones de Transito.

En esta prueba se debe llevar a cabo la identificación de vulnerabilidades relacionadas con código malicioso y acciones involuntarias como lo es XSS, CSRF e Inyección SQL. Dichas pruebas incluyen la prueba de parámetros dentro de los servidores web, el servidor web (en casos como Apache e IIS de Microsoft), así como la verificación de otro tipo de vulnerabilidades que permitan inyectar código o datos a las bases de datos por medio de este tipo de ataques. Para realizar estos ataques se utilizan las siguientes herramientas: Wikto (http://sectools.org/tool/wikto), Samurai (http://samurai.inguardians.com) y Acunetix.

Pruebas de ingeniería social a la red inalámbrica.

Esta prueba consiste en efectuar dos tipos de ataques de ingeniería social para obtener acceso a la red inalámbrica. Las pruebas son:

Prueba de detección de redes inalámbricas desde fuera de la compañía, con el fin de identificar si las redes son detectadas fuera del edificio y es posible capturar el paquete de autenticación.

Prueba de solicitud de clave de las redes inalámbricas a 5 funcionarios/contratistas de la entidad.

8.2 PRUEBAS DE VULNERABILIDAD Y ETHICAL HACKING:

INFORME EJECUTIVO DE SEGURIDAD INFORMATICA

OBJETIVO

El objetivo del presente documento es presentar de forma ejecutiva el **resultado diferencial** de las Pruebas de Vulnerabilidad y Ethical Hacking realizadas a la Infraestructura perimetral (externa) de la Federación Colombiana de Municipios, incluyendo: la descripción de las pruebas realizadas, los elementos evaluados y las vulnerabilidades identificadas junto con su nivel de severidad y riesgo, así como las conclusiones y recomendaciones.

Así mismo, este informe consigna la diferencia entre las vulnerabilidades identificadas al inicio del proyecto y las vulnerabilidades identificadas como parte del re-test (nueva evaluación), las cuales permiten determinar el nivel de remediacion que se ha implementado en la Infraestructura de la FCM.

ALCANCE DEL RE-TEST

La prueba realizada tuvo como alcance la **infraestructura Externa** de la FCM que presentó vulnerabilidades dentro del primer informe entregado:

Nota: Las direcciones IP que se deberían señalar en la siguiente tabla, se dejan en blanco y/o en (X) para garantizar la confidencialidad y protección de la información de la entidad.

Tabla 6: Direcciones IP Evaluadas

Direcciones IP evaluadas
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X

Nota: Las URLs que se deberían señalar en la siguiente tabla, se dejan en blanco o con X, para garantizar la confidencialidad y protección de la información de la FCM.

Tabla 7: URLs Evaluados

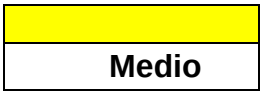
URLs Evaluados
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X
192.168.X.X

Las vulnerabilidades se clasifican de acuerdo con los siguientes niveles:

La explotación de una vulnerabilidad con nivel Alto podría proporcionar acceso a datos y sistemas no autorizados, en la mayoría de los casos a un nivel de administración.

El riesgo contempla la exposición de información sensible, tal como identificadores de usuario (nombres), contraseñas, información propietaria, secretos, números de tarjetas de crédito, información de clientes, de colaboradores u otra información sensible de la organización. Así mismo, podría llegar a generar Denegación de Servicio que impacte de manera importante la continuidad de las operaciones.

En este nivel se encuentran aquellas vulnerabilidades que son lo suficientemente significativas para causar un impacto negativo en el negocio. Por lo tanto, se sugiere que sean corregidas de forma inmediata.



La explotación de vulnerabilidades con nivel Medio podrían permitir indirectamente acceso a archivos de configuración, datos, o afectar parcialmente un sistema de información.
Se sugiere que estos hallazgos sean corregidos en un breve plazo para su análisis y resolución.

La explotación de una vulnerabilidad con nivel Bajo podría permitir a un atacante obtener información estadística de un sistema, cuentas de usuarios u otra información que podría ser usada para crear un nuevo vector de ataque.

Estos hallazgos podrán ser analizados, planificados y solucionados una vez se resuelvan los anteriores niveles de hallazgos que presentan mayor nivel de riesgo para la organización.

HERRAMIENTAS UTILIZADAS

Para la realización de las pruebas se utilizaron las siguientes herramientas, las cuales se encuentran homologadas por el CVE (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilizacion.

Nombre: Nexpose
Fabricante: Rapid7 (http://www.rapid7.com/)

Nombre: Acunetix Web Vulnerability Scanner
Fabricante: Acunetix (www.acunetix.com)

HALLAZGOS PRINCIPALES

A continuación se presenta el resultado de la verificación realizada sobre la implementación de medidas de remediacion en las vulnerabilidades identificadas como resultado de la prueba inicial.

Reducción del número de direcciones IP y URLs evaluados.

Como parte de la prueba realizada como re-test se identificó un numero menor de dispositivos en comparación con la cantidad de dispositivos evaluados inicialmente. Sin embargo, algunos de los dispositivos, aunque se encuentran activos, no presentan vulnerabilidades clasificadas como Alto, Medio o bajo. A continuación se presenta la diferencia de las direcciones IP y URLs detectadas inicialmente en contraste con las detectadas durante la prueba de Re-test:

Figura 10: Comparación de direcciones IP detectadas

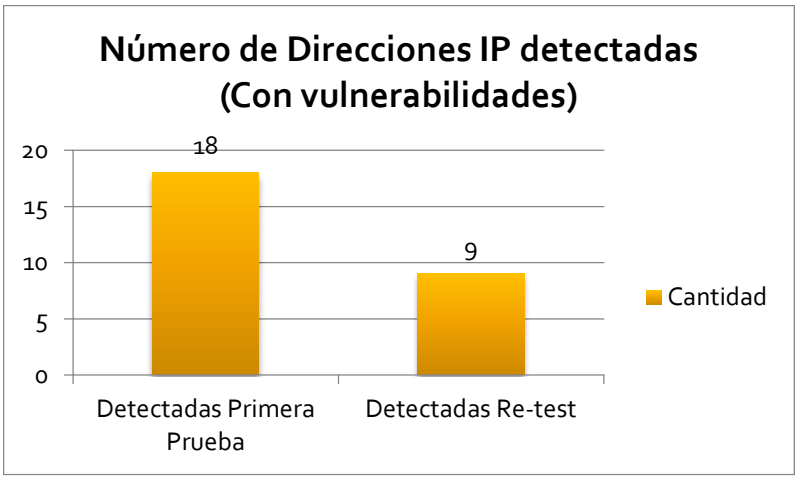
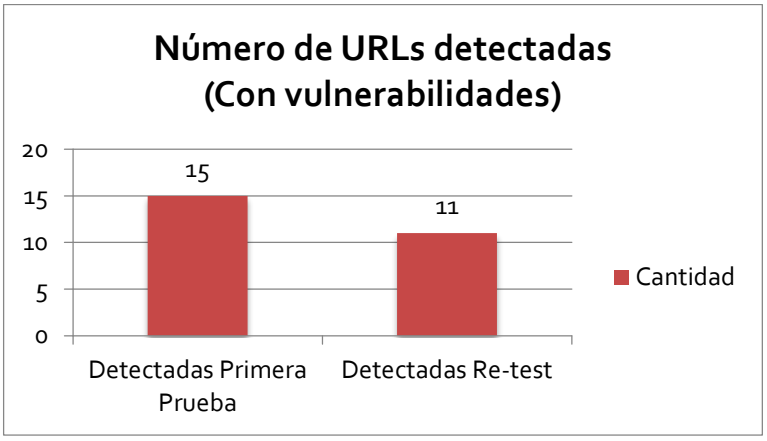


Figura 11**:** Comparación de URLs detectadas



Las direcciones IP y URLs que NO fueron detectadas, ya sea porque fueron retiradas o porque se corrigieron sus vulnerabilidades, se presentan a Continuación:

Nota: Las direcciones IP y URLs que se deberían señalar en la siguiente tabla, se dejan en blanco y/o X para garantizar la confidencialidad y protección de la información de la FCM.

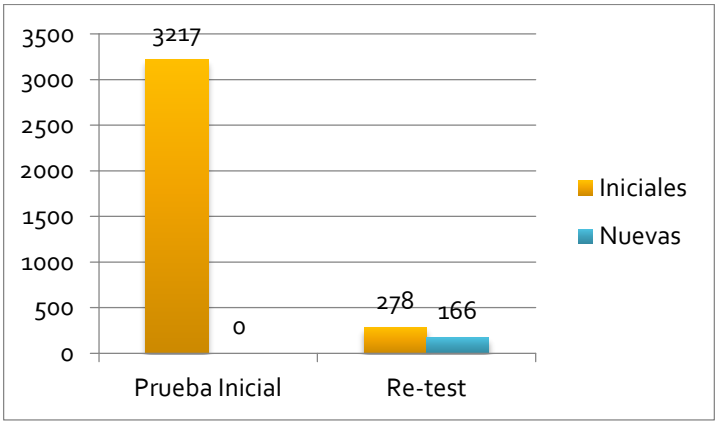
Tabla 8. Vulnerabilidades detectadas

Dirección IP/URL	Cantidad de Vulnerabilidades detectadas en primera prueba	Estado
192.168.X.X	1	Detectado, Vulnerabilidad Corregida
192.168.X.X	2	Detectado, Vulnerabilidades Corregidas
192.168.X.X	1	Detectado, Vulnerabilidad Corregida
192.168.X.X	1	Detectado, Vulnerabilidad Corregida
192.168.X.X	1377	Detectado sin vulnerabilidades de nivel alto, medio o bajo
192.168.X.X	85	Detectado sin vulnerabilidades de nivel alto, medio o bajo
192.168.X.X	532	Detectado sin vulnerabilidades de nivel alto, medio o bajo
192.168.X.X	387	Detectado sin vulnerabilidades de nivel alto, medio o bajo
192.168.X.X	10	Detectado sin vulnerabilidades de nivel alto, medio o bajo
192.168.X.X	5	No detectado
192.168.X.X	8	No detectado
192.168.X.X	10	No detectado
192.168.X.X	2	Detectado, Vulnerabilidades Corregidas

Reducción en el numero de vulnerabilidades

Con base en la reducción de dispositivos, se presenta a continuación la comparación de las vulnerabilidades identificadas a nivel Externo, de acuerdo con lo que sedetectó durante la primera prueba.

Figura 12: Comparación de vulnerabilides detectadas

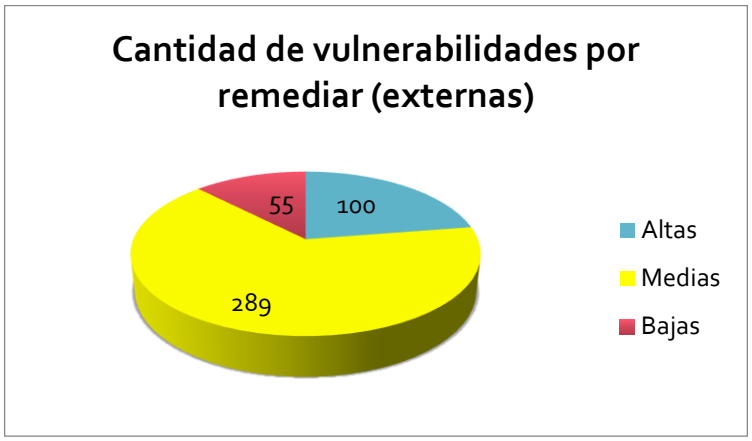


De acuerdo con lo anterior se identificó que la cantidad de vulnerabilidad se redujo notablemente con respecto a los resultados obtenidos dentro del primer informe. A la fecha se identificaron un total de **278 vulnerabilidades que persisten desde la entrega del informe anterior**, y **166 vulnerabilidades nuevas**, las cuales no aparecen en el informe anterior, pero que son producto de nuevos tipos de ataque que se han creado desde que se realizó dicha prueba. **En total, las vulnerabilidades a la fecha por remediar, que se encuentran en la red externa, es 444,** es decir la suma de las vulnerabilidades persistentes y las nuevas**.**

Vulnerabilidades pendientes por remediar

De acuerdo con los resultados obtenidos en la segunda prueba (Re-test) se presentan a continuación la distribución de las vulnerabilidades que se encuentran pendientes por remediar.

Figura 13: Vulnerabilidades pendientes por remediar



Con los resultados obtenidos las vulnerabilidades, a continuación se consignan los **hallazgos principales y más significativos** identificados dentro de la red de la Federación Colombiana de Municipios durante la prueba realizada:

Resumen de las vulnerabilidades mas significativas

Nota: *Las direcciones IP o URLs que se deberían señalar, no se mencionan o se dejan en blanco o con (X), para garantizar la confidencialidad y protección de la información de la FCM.*

Ataques de Cross Site Scripting:

Este vulnerabilidad permite que un atacante pueda efectuar robos de sesión a los clientes legítimos que acceden a la los portales para efectuar sus transacciones. Por lo tanto, cuando un usuario ingresa al sistema, este puede ser redirigido hacia otro portal, su sesión es extraíble y reproducible en otro ambiente, dentro del cual puede fugarse la información de datos personales, usuarios y contraseñas entre otros.
Impacto: **Alto**

Denegación de servicio (DoS) en los portales.
Esta vulnerabilidad permite a un atacante degradar el servicio y causar la interrupción en el acceso a los portales web de la FCM. Por lo tanto, deben implementarse medidas preventivas para mitigar los riesgos respectivos.
Impacto: **Alto/Medio**

Versión desactualizada de PHP. Se identificó un total de 233 vulnerabilidades en los siguientes equipos por falta de actualización de PHP.

Nota: Las direcciones IP que se deberían señalar, se dejan en blanco o (x) para garantizar la confidencialidad y protección de la información de la FCM.

(XXXXXXXXXX, XXXXXXXX, XXXXXXXXXXXXXX).

Esto permite ejecutar código malicioso para tomar control del servidor, o en su defecto para extraer información sensible. Por lo tanto, debe actualizarse a la mayor brevedad la versión de PHP de dichos servidores, mitigando dicho número de vulnerabilidades y reduciendo el factor de exposición.
Impacto: Alto

Version desactualizada de Apache. Se identificó un total de 92 vulnerabilidades relacionadas con la falta de actualización de Apache. Estas vulnerabilidades permiten a un atacante tomar control remoto del servidor, extraer información confidencial o causar denegación de servicio. Por lo tanto, debe realizarse la actualización lo antes posible.
Los equipos que tienen esta vulnerabilidad son:

Nota: Las direcciones IP que se deberían señalar, se dejan en blanco o con X, para garantizar la confidencialidad y protección de la información de la FCM.

(XXXXXXXXXX)
(XXXXXXXXXX)
(XXXXXXXXXX)
(XXXXXXXXXX)
Impacto: Alto

CONCLUSIONES
De acuerdo con las pruebas realizadas, se presentan a continuación las conclusiones respectivas del análisis.

El resultado de las pruebas de verificación sobre la red Externa de la Federación Colombiana de Municipios, permitió identificar los niveles de vulnerabilidad con los que se cuenta actualmente luego de efectuar actividades de remediación. Ya sea remediación realizada por restricciones de acceso a direcciones IP, actualización de versiones, retiro de equipos o cambio de URLs.

De acuerdo con los resultados obtenidos en la presente prueba, se identificó que la cantidad de vulnerabilidades inicialmente detectadas se redujo en casi un 90%. Es decir, de 3217 vulnerabilidades que se identificaron en el primer informe, solo quedan por corregir 278.

Así mismo, aunque no se identificaron muchas de las vulnerabilidades anteriores, se detectaron 166 nuevas vulnerabilidades que también deben ser

corregidas. Por lo tanto, el total de vulnerabilidades a la fecha, para la red externa (vista desde internet) de la FCM, es de 444.

La reducción de vulnerabilidades se debe en su mayoría a que no se detectaron vulnerabilidades en los equipos (XXXXXXXX, XXXXXXXXX y XXXXXXXXXXX) los cuales inicialmente tenían un total de 2296 vulnerabilidades, y que ahora, no se encuentran con dicho número.

Nota Importante:

Si no se proporciona una solución oportuna a las vulnerabilidades identificadas, la Federación Colombiana de Municipios, podría incurrir en pérdidas significativas de tipo operativo, administrativo, imagen y reputación, lo cual se traduce en pérdidas económicas de alta envergadura. Esto dado que, si un atacante obtiene acceso a través de las vulnerabilidades identificadas, podría ingresar sin autorización a la infraestructura de la FCM, detener servicios, o causar denegación de acceso y uso a los mismos. Así mismo, podría obtener información confidencial, extraerla y divulgarla, manipularla y suplantarla de tal forma que se pierda control sobre la misma, sin dejar rastro alguno dentro de los sistemas usados para tal fin. Por lo tanto, se recomienda con carácter urgente, implementar las medidas correctivas para remediar dichos hallazgos en el menor tiempo posible, e implementar las medidas de seguridad propuestas como recomendación dentro del juego de documentos del análisis de seguridad llevado a cabo.

RECOMENDACIONES

De acuerdo con los hallazgos y las vulnerabilidades identificadas, se presentan a continuación las recomendaciones generales de mitigación, las cuales permiten reducir el riesgo de exposición.

Implementar las recomendaciones técnicas y procedimientos documentados en cada una de las vulnerabilidades que se encuentran dentro el Anexo Técnico, entregado como parte de este informe, el cual es de acceso y uso exclusivo para la Federacion Colombiana de Municipios.

De la misma forma, se recomienda seguir el “Plan de acción para reducir las brechas” planteado en el informe técnico que se entregó como parte de la primera prueba realizada. Lo anterior, con el fin de implementar una remediación de las vulnerabilidades de forma apropiada sin causar una interrupción o degradación del servicio y en un corto tiempo. (Este plan se encuentra dentro el Documento Técnico). El plan propuesto contempla la implementación de las acciones correctivas de mitigación iniciando por las vulnerabilidades mas criticas de forma externa y posteriormente las criticas de forma interna. Así mismo, se

recomienda definir el plan de remediación con fechas y prioridad en los equipos más críticos de la entidad.

Para los equipos publicados de forma externa en internet, que cuentan con certificados auto-firmados o que ya están expirados, se recomienda adquirir los certificados, o crear una entidad certificadora (CA) de forma interna para firmar los certificados que utilicen las aplicaciones al interior de la FCM. Durante el presente análisis, se determinaron aun servidores que tienen estas vulnerabilidades.

Implementar las recomendaciones técnicas expuestas en el anexo técnico, con el fin de lograr remediar los ataques de Denegación de servicio al que pueden estar expuestas las URLs evaluadas dentro del presente análisis.

Nota: Como anexo a este documento se entrega un archivo confidencial para uso exclusivo de la Federación Colombiana de Municipios en formato MS Excel, con el detalle las vulnerabilidades que se detectaron durante las pruebas de Re-test. Posterior a la entrega de este informe, se realizará una sesión técnica de aclaración de dudas y programación de la remediación de dichas vulnerabilidades.

8.3 ALCANCE DEL SGSI EN FCM Y EVALUACION DE RIESGOS DE LOS ACTIVOS

El SGSI se aplicará solamente para la FCM (Federación Colombiana de Municipios) ubicada con sede principal en la ciudad de Bogotá D.C, bajo la justificación y necesidad presentada por la alta dirección de la entidad mediante el cual, presenta problemas de seguridad y ciberseguridad en todas las áreas de la organización.

Por lo tanto, se define y estructura un acto administrativo para la aplicabilidad y uso de manera inicial de la política general de seguridad de la información en la FCM.

A continuación, se define y estructura la política, se contempla el desarrollo del siguiente punto.

- Cuadro de dominios y controles seleccionados de la norma ISO/IEC 27002 de acuerdo a los alcances del SGSI.

Política General de Seguridad y Privacidad de la Información

CONFIDENCIALIDAD

Este documento es de carácter confidencial, dado su contenido y las implicaciones que éste pueda tener en aras de preservar la seguridad de la información de la **FEDERACIÓN COLOMBIANA DE MUNICIPIOS "FCM".**

Este ha sido publicado en medio impreso y magnético de acuerdo con lo establecido en el Sistema de Gestión de Seguridad de la Información (SGSI) de la **FCM,** con el único propósito que la organización, los funcionarios, contratistas y empleados en misión conozcan los lineamientos y directrices que se han articulado para asegurar y mitigar el riesgo en cuanto a la seguridad de la información. Su resguardo, manejo y/o divulgación a terceras partes son de competencia exclusiva de la organización.

Esta política será conocida y leída bajo los más estrictos criterios de confidencialidad y no será divulgada por ningún medio o propósito, ni total ni parcialmente, la reproducción o copia de esta información está totalmente prohibida, solo podrá ser usada en el ámbito laboral y en el marco de la ejecución contractual.

OBJETIVO

Presentar y socializar en forma coherente los principios y la importancia de la política de seguridad de la información que deben conocer y cumplir todos los directivos, funcionarios, empleados en misión, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Federación Colombiana de Municipios.

ALCANCE

Los principios y las políticas de seguridad de la información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, empleados en misión, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la ***Federación Colombiana de Municipios.***

Los empleados, contratistas, aliados, funcionarios en misión y demás, tienen la obligación de dar cumplimiento a los principios y políticas emitidas y aprobadas por la Dirección Ejecutiva de la Federación Colombiana de Municipios.

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Que la información es un activo de vital importancia para la Federación Colombiana de Municipios y asegurar su autenticidad, confidencialidad, integridad, disponibilidad, trazabilidad y la continuidad del negocio, es uno de los objetivos de la Dirección Ejecutiva, por el cual se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los Ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Que las normas ISO/IEC 27001 (requisitos) e ISO/IEC 27002 (Código de práctica para la gestión de la seguridad del a información), son un conjunto de estándares internacionales desarrollados por la ISO (Organización Internacional de Estandarización) e IEC (Comisión Electrotecnológica Internacional), que proporcionan un marco de gestión para la seguridad de la información en una organización.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

En el marco del cumplimiento de la estrategia de Gobierno en Línea, la Federación Colombiana de Municipios gestiona el Modelo Seguridad y Privacidad de la Información, mediante el cual comprende que el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, publica el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: **TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.**

Para **FEDERACION COLOMBIANA DE MUNICIPIOS**, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se definió en el alcance, sus funcionarios, empelados en misión, terceros, aprendices, practicantes, proveedores y aliados estratégicos de la ciudadanía en general, teniendo en cuenta que los principios y políticas sobre los que se basa el desarrollo

de las acciones o toma de decisiones alrededor del SGSI y el Modelo de Seguridad y Privacidad de la Información, estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios y políticas de la función administrativa.
- Mantener la confianza de sus asociados, clientes, socios, funcionarios, empelados en misión y aliados estratégicos.
- Apoyar la innovación tecnológica.
- Proteger los activos de información y tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de **FEDERACION COLOMBIANA DE MUNICIPIOS.**
- Garantizar la continuidad del negocio frente a incidentes.
- **FEDERACION COLOMBIANA DE MUNICIPIOS** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

A continuación, se establecen los principios de seguridad que soportan el SGSI de la **FEDERACION COLOMBIANA DE MUNICIPIOS**:

• Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los empleados, proveedores, socios de negocio o terceros**.

• Federación Colombiana De Municipios **protegerá la información** generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos **otorgados a terceros** (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

• Federación Colombiana De Municipios **protegerá la información** creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

• Federación Colombiana De Municipios **protegerá su información** de las amenazas originadas por parte **del personal**.

• Federación Colombiana De Municipios **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.

• Federación Colombiana De Municipios **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• Federación Colombiana De Municipios **implementará control de acceso** a la información, sistemas y recursos de red.

• Federación Colombiana De Municipios **garantizará que la seguridad** sea parte integral del ciclo de vida de los sistemas de información.

• Federación Colombiana De Municipios **garantizará a través de una adecuada gestión de los eventos de seguridad** y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

• Federación Colombiana De Municipios **garantizará la disponibilidad** de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

• FEDERACION COLOMBIANA DE MUNICIPIOS garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Con base a las políticas de seguridad y privacidad de la información desarrolladas, se referencia a continuación la estructura de la norma ISO 27001 que expresan el cumplimiento de la norma en la **FEDERACION COLOMBIANA DE MUNICIPIOS**:

Figura 14 Dominios Noma ISO 27001.

Fuente: Activos de Informacion FCM.

Nota: Para comprender el contexto y el cumplimiento de la política general de seguridad y privacidad de la información en la Federación Colombiana de Municipios, diríjase a ver el manual de políticas de seguridad y privacidad de la Información de la entidad.
El incumplimiento a la política general de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

NOTIFÍQUESE, COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

FIRMADO EN ORIGINAL.

GILBERTO TORO GIRALDO
Director Ejecutivo

Elaboro: Profesional Oficial de Seguridad Informática.
Revisó: Comité SGSI - FCM
Aprobó: Presidente Comité SGSI - FCM

Listas de chequeo teniendo en cuenta la norma ISO/IEC 27002 en cada uno de los Dominios y Objetivos de control

A continuación, se realiza la lista de chequeo conforme a los dominios y controles de la Norma ISO 27002, esto se realiza contemplando el nivel de madurez de cumplimiento de la norma y conforme a la matriz de valoración de riesgos previamente definida por la entidad, el cual es basada en cobit 5.0 y el MSPI (Modelo de Seguridad y Privacidad de la Información de Mintic que está alineado a DAF – Departamento Administrativo de la Función Pública):

Tabla 9. Calificaciones o Nivel de Madurez

Cada uno de los requerimientos de la hoja de los DOMINIOS ha sido calificado en una escala del 1 al 5 (Siendo 1 debilidad y 5 fortaleza) Estos valores tienen como referencia la valoración del DAF y GEL.		
Valoración	**Efectividad**	**Cumplimiento** **Con respecto al control, es un control débil, cumple o excede las expectativas**
1	**No implantado**	No existen controles – Carencia completa de documentación y procesos
2	**50%**	Controles no estándar – La organización conoce los problemas y tiene intención de solucionarlos, algunos con enfoques propios, pero nada estandarizado
3	**90%**	El Requerimiento se Cumple en forma aceptable - Aunque existen los controles, no se comunican y/o difunden para crear consciencia y no se hace entrenamiento y seguimiento
4	**95%**	Controles Eficientes - Los controles se han documentado y estandarizado, se han seguido entrenamientos, sin embargo, la aplicación de los mismos en algunos casos es por cuenta propia del individuo.
5	**Administrado**	Optimizado – Es posible administrar los controles y medir el cumplimiento de los mismos para tomar medidas cuando no estén ejecutándose de forma debida.

A continuación, se realiza la lista de chequeo conforme al Modelo de Evaluación de Nivel de Madurez definido anteriormente.

Tabla 10 Lista de Chequeo y Nivel de Madurez.

FEDERACIÓN COLOMBIANA DE MUNICIPIOS							
SISTEMA DE GESTIÓN DE SEGURIDAD INFORMATICA							
CUADRO DE DOMINIOS Y CONTROLES SELECCIONADOS Y LISTA DE VERIFICACION							
MATRIZ DE VALORACIÓN ISO 27002							
CAPÍTULO 1 - Política de Seguridad Corporativa							
Procesos entrevistados/involucrados: Jurídica, Operaciones, Administración del sistema, Proyectos, Financiera, Contable, Dirección Nacional SIMIT, Dirección Administrativa, TICS.							
	Item	**ISO Ref**	**Control**	**Aplica (SI/NO)**	**Estado del cliente / Mecanismos de salvaguarda implementados**	**Valoración**	**Oportunidad de mejora y recomendaciones**
	1.1	5	Políticas de Seguridad				
	1.1	5,1	Orientación de la dirección para la gestión de la seguridad de la información				
	1.1.1	5.1.1	Políticas para la seguridad de la información	Si	Existen políticas de seguridad Global de la información documentadas, pero falta ajustarlas de acuerdo a las necesidades de la FCM.	**4**	Ajustar la política a las necesidades de la gobernación.
	1.1.2	5.1.2	Revisión de las políticas para la seguridad de la información	Si	No se tiene un plan periódico para la revisión, evaluación del cumplimiento de las políticas de la seguridad de la información, aunque se cuenta con la política documentada.	**2**	Se deberá dejar explícita la tarea periódica de revisión y evaluación en unas fechas formales.

	2	6	Organización de la Seguridad de la Información				
	2.1	6,1	Organización Interna				
	2.1.1	6.1.1	Roles y Responsabilidad de Seguridad de la Información	Si	Existe el compromiso y la voluntad por parte de las directivas a nivel del área de Tecnología. Falta conciencia de seguridad de la información en los demás procesos, aunque se vienen adelantando campañas	**3**	Incrementar las campañas de densificación que permite tomar conciencia sobre el Sistema de Gestión de Seguridad de la Información
	2.1.2	6.1.2	Contacto con autoridades	Si	No se tiene dentro del proceso de atención de incidentes el punto en concreto, las características que debe presentar el incidente y el protocolo a seguir para el contacto con las autoridades.	**1**	Realizar un procedimiento para control de incidentes.
	2.1.3	6.1.3	Contacto con grupos de interés especial	Si	El comité de seguridad no es miembro oficial de algún grupo especializado o de interés en seguridad de la información, algunos miembros tienen relación con ISACA, con universidades en el exterior, pero de forma profesional individual.	**2**	Inscribir a los miembros del comité de seguridad de la información en listas de correo especializadas e incrementar el contacto con los grupos de interés (Linkedin).
	2.1.4	6.1.4	Seguridad de la Información en la gestión de proyectos	Si	No son claras las funciones de la seguridad de la información en la evaluación y autorización de actividades en el procesamiento de datos o protección de la información, sin embargo existen procedimientos para realizar modificaciones o adiciones de software y hardware.	**3**	Reforzar los esquemas de mantenimiento de documentos de auditorías de seguridad, como administración de Logs, revisión de bitácoras y monitoreo de incidentes en las áreas.
	2.1.5	6.1.5	Segregación de deberes	Si	Se realizan acuerdos específicos de confidencialidad tanto para la contratación como para la manipulación específica de datos o actividades en areas de procesamiento de datos.	**5**	Por la naturaleza de la organización, este punto tiene una especial madurez, incluyendo esquemas de estudios de seguridad y

							sanciones claramente especificadas
	2.2	6,2	Dispositivos móviles y teletrabajo				
	2.2.1	6.2.1	Política de dispositivos móviles	Si	No existe una política formal sobre el uso de computación móvil, de celulares, tablets y demás dispositivos móviles, aunque existen controles básicos para el backup de algunos dispositivos de altos funcionarios.	**2**	Diseñar e implementar una política de control de computación móvil, acompañada del procedimiento adecuado al control a ciertos equipos.
	2.2.2	6.2.2	Teletrabajo	Si	No existe una política formal sobre actividades de teletrabajo. Sin embargo tampoco se permite el teletrabajo en el área.	**2**	Diseñar e implementar una política de Teletrabajo, acompañada del procedimiento adecuado de control que incluya las buenas prácticas permitidas y los mecanismos de control.
	3	7	Seguridad en los Recursos Humanos				
	3.1	7.1	Previo al Empleo				
	3.1.1	7.1.1	Selección. Verificación de antecedentes	Si	La Organización cumple con este control realizando investigaciones de antecedentes disciplinarios a través del departamento de recursos humanos de la federación, que es transversal en la dirección Nacional SIMIT.	**3**	Mantener el control implementado y describir el procedimiento dentro del SGSI, faltan algunas investigaciones concretas para recolectar más información sobre la persona a contratar.
	3.1.2	7.1.2	Términos y condiciones del empleo	Si	No se cumple en todos los procesos con el control y las descripciones de responsabilidades de seguridad dentro de los contratos y acuerdos, solo se cuenta con el de confidencialidad.	**2**	Implementar auditorías a todos los procesos solicitándo la información de responsabilidades a los recién contratados.
	3.2	7,2	Durante el empleo				

	3.2.1	7.2.1	Responsabilidades de la dirección	Si	Existen supervisores de los contratos, pero no existe un oficial de seguridad de la información.	**2**	La participación en seguridad de las directivas se realiza más que por su intención en el fortalecimiento de la seguridad por requerimiento y regulaciones. Esto puede mejorar con un plan de conciencia a nivel directivo
	3.2.2	7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Si	Se realizan recordatorios sobre esquemas y controles de seguridad a través de medios tecnológicos, pero no existe un plan formal de entrenamiento o conciencia en seguridad.	**3**	Realizar el plan de concientización, el entrenamiento adecuado a los usuarios y la campaña completa de divulgación del SGSI
	3.2.3	7.2.3	Proceso disciplinario	Si	No son claros los descargos disciplinarios cuando se producen brechas de seguridad porque no se ha presentado un caso. Falta definir claramente cuales serían los pasos a seguir desde el punto de vista legal ante un incidente donde se viere involucrado un empleado de la organización.	**1**	incluir el detalle de procesos disciplinarios y descargos, dentro del manual de funciones y en el SGSI
	3.3	7.3	Terminación del contrato y cambio de empleo				
	3.3.1	7.3.1	Terminación o cambio de responsabilidades de empleo	Si	La Organización cumple con este control pero en algunos casos no hay procedimientos internos desde el punto de vista de seguridad de la información para dar de baja el usuario, sus permisos y roles. La Organización cumple con este control, sin embargo no siempre se informa sobre los activos cuando una persona sale de su empleo.	**4**	Incluír el proceso en el SGSI cuando haya sido implementado en la terminación de contratos.
	4.1	8	Gestión de Activos				

	4.1	8,1	Responsabilidad de los Activos				
	4.1.1	8.1.1	Inventario de activos	Si	La Organización cumple satisfactoriamente con este control porque cuenta con una gestión del inventario automatizado (para hardware y software) y la identificación de los activos de información desde el punto de vista de seguridad de la información.	**5**	Centralizar el inventario de todos los activos en un listado maestro, enmarcado en un procedimiento y asignado a su responsable por su mantenimiento, todo desde un mismo software.
	4.1.2	8.1.2	Propiedad de los activos	Si	Cada proceso conoce los activos de información que tiene a su cargo y tiene plenamente identificadas las propiedades de cada activo (tipo, ubicación, responsable) y conoce las consecuencias de una falla en la confidencialidad, disponibilidad e integridad a las cuales podría estar sometida en algún momento la información.	**5**	Incluír las responsabilidades sobre los activos de información en el manual de funciones de los empleados y usar un software que gestione esto junto con el punto anterior.
	4.1.3	8.1.3	Uso aceptable de los activos	Si	Existe una política que indica que se proveen los medios necesarios para asegurar que un usuario preserve y proteja los activos de información de una manera confiable, con el fin de darle un buen uso a dichos recursos, sin embargo, a falta de auditorías internas en seguridad, no se conoce que tanto es el nivel de cumplimiento de ésta política y si hay alguna violación de la misma.	**3**	Incluír el uso aceptable de los activos tecnológicos en el manual de funciones de los empleados. Realizar procesos de auditoría en términos de cumplimiento operativo.
	4.1.4	8.1.4	Devolución de los activos		Los activos son devueltos de acuerdo a los lineamientos establecidos.	**0**	Se debe realizar revisión periódica para vigilar que se encuentre la documentación correspondiente.

	4.2	8,2	Clasificación de la Información				
	4.2.1	8.2.1	Clasificación de la información	Si	No se tienen claramente identificadas las características para caracterizar/clasificar la información. Cada proceso conoce la pertinencia de la información pero carece de un procedimiento que le ayude a clasificar la información y le asigne un nivel de pertinencia (top secret, privado, publico interno, publico externo, etc).	**2**	Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso.
	4.2.2	8.2.2	Etiquetado de la información	Si	No se tienen procedimientos de etiquetado de los activos tanto en medios electrónicos como físicos que reflejen los niveles de clasificación de la información, sin embargo, se tienen identificadas las caracteristicas de los activos que permiten identificarlo y manejarlo	**3**	El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado.
	4.2.3	8.2.3	Manejo de activos de información			**0**	
	4.3	8,3	Manejo de Medios				
	4.3.1	8.3.1	Gestión de medios removibles	Si	No existe una política estricta sobre el uso de medios removibles dentro de la organización	**1**	Crear el control e incluír la política y sus excepciones documentadas en el SGSI
	4.3.2	8.3.2	Disposición de los medios	Si	La organización cuenta con elementos de destrucción documental, y realiza la disposición segura de medios cuando es requerido por parte de soporte interno.	**3**	Es necesario establecer una política rigurosa en el SGSI acompañada de un procedimiento para la destrucción de medios específicamente identificados.

	4.3.3	8.3.3	Transferencia de medios físicos	Si	No se conoce una práctica formal de protección para los medios en movimiento.	**1**	En los casos en que sea necesario transportar información, debe exigirse el cumplimiento de una política de protección para esta información. La política y procedimientos deben ser estrictas e incluídas en el SGSI
	5	9	Control de Acceso				
	5.1	9,1	Requerimientos del Negocio para el Control de Acceso				
	5.1	9.1.1	Política de Control de Acceso	SI	Existe una política de control de acceso en la política de seguridad de la información.	**4**	Implementar todas las acciones técnicas y mejoras que se puedan dar para optimizar el control de acceso (ejemplo: nuevas tecnologías biométricas).
	5.2	9.1.2	Acceso a redes y a servicios de red		Actualmente existe una política formalmente definida para el uso adecuado de los servicios de red, pero no se ejecuta de manera optima por parte de los usuarios (internet) debido a que la alta gerencia permite el uso de ciertos sitios web que podrían representar amenazas a la seguridad de la información.	**2**	Mantener y fortalecer la política de uso de los servicios de red que especifique la intención, autorización y control del mismo.
	5.2	9.2	Gestión de acceso a usuarios				

	5.2.1	9.2.1	Registro y cancelación del registro de usuarios	Si	Se realiza un proceso de registro de usuarios para cada individuo con perfiles y permisos asignados según justifique el caso. No se realiza un seguimiento periódico y formal a los usuarios en desuso del sistema. Se revisan usuarios bajo requerimiento, la administración de base de datos está a cargo de personal de TICs de la Federación Colombiana de Municpios.	**3**	Mantener la política de control de acceso de usuarios, realizar un seguimiento cronologico a usuarios creados con el fin de verificar su validación en los sistemas de información.
	5.2.2	9.2.2	Suministro de acceso de usuarios	SI	La organización cumple con un control fuerte para las contraseñas, sin ambargo es responsabilidad del usuario final mantenerlas seguras.	**3**	Durante la campaña de conscientización, exponer los riesgos al compartir el usuario de red.
	5.2.2	9.2.3	Gestión de derechos de acceso privilegiado	SI	La Organización cumple satisfactoriamente con este control, tiene controles y documentación del proceso de asignación de perfiles a los usuarios.	**4**	Mantener el control de administración de privilegios, documentarlo alinearlo con el SGSI.
	5.2.3	9.2.4	Gestión de información de autenticación secreta de usuarios	SI	Se tienen directivas sobre el uso y administración de contraseñas, sin embargo hace falta una formalidad en el procedimiento al uso de las mismas.	**4**	Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas.
	5.2.4	9.2.5	Revisión de los derechos de acceso a usuarios		No se realiza la tarea periodicamente con el detalle requerido para identificar inconvenientes con los perfiles.	**1**	Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.

	5.2.4	9.2.6	Retiro o ajuste de los derechos de acceso		Se debe exigir a los usuarios que cumplan las practicas de la organización para el usa de información de autenticación secreta.	**0**	
	5.3	9,3	Responsabilidades de los usuarios				
	5.3.1	9.3.1	Uso de información de autenticación secreta		La organización, mediante recordatorios, promueve el buen uso de las contraseñas, recomendando no escribirla y no usar una contraseña en mas de 1 sistema al tiempo.	**4**	Realizar el plan de concientización y entrenamiento formal debido a la importancia del tema.
	5.4	9.4	Control de acceso a sistemas y aplicaciones				
	5.4.1	9.4.1	Restricción de acceso a la información	SI	Se tienen restricciones a algunos sistemas de información, no a todos. Por la función actual de Sistemas de la Dirección Nacional SIMIT, se cuenta con acceso a la Base de Datos de toda la información de SIMIT, a esta se puede ingresar por medio de aplicación o por medio de herramientas que permiten ingresar directamente a la información.	**2**	Implementar controles más avanzados, como ACLs en la base de datos, que no permita a un usuario el acceso total a la información y su modificación.
	5.4.2	9.4.2	Procedimiento de ingreso seguro	SI	La organización cuenta con métodos de autenticación segura otogada por los protocolos usados para autenticar (LDAP seguro, conexiones a bases de datos segura, HTTPS para autenticación web)	**4**	Implementar métodos de doble factor de autenticación para los accesos más críticos a los sistemas de información: por ejemplo, base de datos.
	5.4.3	9.4.3	Sistema de gestión de contraseñas		La Organización cumple satisfactoriamente con este control (Políticas de LDAP)	**4**	Mantener el esquema implementado. Extender el esquema a más aplicaciones
	5.4.4	9.4.4	Uso de programas utilitarios privilegiados		la estricción existe debido a que los usuarios trabajan a través de terminales.	**4**	Los usuarios están conectados a través de terminales lo que

							permite llevar un mejor control.
	5.4.5	9.4.5	Control de acceso a códigos fuente de programas		Se debe restringir el acceso a códigos fuente de programas	**4**	Los usuarios están conectados a través de terminales lo que permite llevar un mejor control.
	6.1	10.1	Controles Criptográficos				
	6.1.1	10.1.1	Política sobre el uso de controles criptográficos	Si	La organización no emplea controles criptográficos para almacenar la información del SIMIT ni en la base de datos.	**1**	Los esquemas criptográficos deben ser obligatorios para el manejo y transporte de información utilizando la clasificación de información. Este esquema debe ser formalmente descrito en una política contenida en el SGSI
	6.1.2	10.1.2	Gestión de llaves		No hay una política formal en el área para la administración de llaves de cifrado debido a que no se tienen controles criptográficos.	**1**	Una vez implementados los controles cifrado, es necesario definir e implementar una política y procedimiento de administración metodologica de cifrado.
	7.1	11	Seguridad física y del entorno				
	7.1	11.1	Áreas seguras				
	7.1.1	11.1.1	Perímetro de Seguridad Física	Si	La Organización cumple satisfactoriamente con este control, en el primer piso del edificio y en la entrada a través de biometria para todas las áreas de la organización.	**5**	No descuidar la revisión periódica del funcionamiento de estos procedimientos y controles
	7.1.2	11.1.2	Controles de acceso físicos	Si	La Organización cumple satisfactoriamente con este control, en el primer piso del edificio y en la entrada a través de biometria para todas las	**5**	Mantener un esquema para luego ser monitoreado por el responsable.

					áreas de la organización, donde se lleva un registro automatizado de los ingresos por parte del personal.		
	7.1.3	11.1.3	Seguridad de oficinas, recintos e instalaciones	Si	No todas las áreas dentro de las instalaciones se encuentran controladas y monitoreadas. No se mantienen cerradas las puertas de las oficinas.	**3**	Incluír en el SGSI la descripción de las precauciones de seguridad en oficinas. Algunas áreas son visibles desde el exterior.
	7.1.4	11.1.4	Protección contra amenazas externas y ambientales	Si	Actualmente hay unos esquemas definidos en el area de TI para garantizar que no se generen afectaciones por parte de amenazas externas o ambientales. Por parte del edificio se tienen controles generales contra incendios.	**4**	Documentar todos los controles de protección contra amenazas externas, juntar los del edificio con los que tiene definidos TI para el centro de datos y periféricos.
	7.1.5	11.1.5	Trabajo en áreas seguras		En la actualidad no existen áreas restringidas de trabajo dentro de la dirección nacional SIMIT. Se tiene, en el centro de datos de la Federación, unos controles y en algunas oficinas de directivos.	**2**	Implementar controles de acompañamiento y registro de todos los usuarios que ingresan a áreas que manejan información sensible
	7.1.6	11.1.6	Áreas de despacho y carga		No se conocen sitios de cargue y descargue	**2**	Dar a cconocer la informaciòn a clientes internos y externos en caso de que existan puntos de cargue y descargue y si la entidad lo requiere
	7.2	11,2	Equipos				
	7.2.1	11.2.1	Ubicación y protección de los equipos	Si	Se ubican los equipos tecnológicos buscando mantener el menor nivel de exposición a terceros o visitantes.	**3**	Debe reforzarse el esquema estableciendo una directiva explicita o una política dentro del SGSI que requiera la protección y ubicación de los equipos

							tecnológicos en areas protegidas.
	7.2.2	11.2.2	Servicios de suministro	Si	La Organización cumple satisfactoriamente con este control, usando las medidas de respaldo del edificio, en donde se tiene una planta de energía que puede alimentar a los equipos de la federación lo suficiente como para apagarse de forma controlada.	**5**	Se debe mantener el esquema de UPSs y plantas eléctricas en optimas condiciones.
	7.2.3	11.2.3	Seguridad en el cableado	Si	La Organización cumple satisfactoriamente con este control, todo su cableado es certificado, marcado, protegido y separado.	**5**	Mantener el esquema. Se debe también eliminar todo cableado obsoleto o en desuso lo antes posible.
	7.2.4	11.2.4	Mantenimiento de equipos	Si	Existen contratos para el mantenimiento correctivo de los equipos de cómputo y se han llevado a cabo de forma correcta.	**5**	Se debe mantener el esquema de contratos de mantenimiento constantes sobre los equipos tecnológicos.
	7.2.5	11.2.5	Retiro de activos	Si	La Organización no cumple estrictamente un protocolo para la extracción de activos y no hay vigilancia a la salida y entrada de la misma.	**4**	Incentivar el estricto uso del protocolo de extraciòn de activos
	7.2.5	11.2.6	Seguridad de equipos y activos fuera de las instalaciones	SI	Se tienen documentados controles sobre la salida de equipos e información, sin embargo estos controles dificilmente son llevados a cabo el 100% de las veces debido a que se los empleados pueden sacar activos tecnológicos y de información por su cuenta.	**4**	El SGSI debe dictaminar las políticas de uso de equipos de cómputo fuera de las instalaciones de la organización que permitan a directivos y altos rangos, conocer los requerimientos de seguridad para el uso de estos elementos

	7.2.6	11.2.7	Disposición segura o neutralización de equipos		El área de soporte interno se encarga del manejo adecuado de los medios fijos o removibles de almacenamiento, se tiene un procedimiento para el borrado seguro de la información y reutilización de tecnología.	**4**	Se debe reforzar la práctica de disposición de medios de almacenamiento y reutilización de equipos mediante una política fuerte dentro del SGSI que no discrimine ningún caso.
	7.2.7	11.2.8	Equipos de usuario desatendido	SI	Los usuarios deben asegurarse de que a los equipos desatendidos se les da proteccion apropiada.	**3**	Actualmente se encuentra implentada una política de bloqueo automática en el tiempo establecido por la entidad.
	7.2.7	11.2.9	Política de escritorio limpio y pantalla limpia		Existe control de salvapantallas y bloqueo de estación a los 5 minutos de equipo desatendido, igualmente en los servidores y en las sesiones remotas a la base de datos.	**5**	Realizar el plan de concientización y entrenamiento encaminados al tema
	8	12	Seguridad de operaciones				
	8.1	12.1	Procedimientos operacionales y responsabilidades				
	8.1.1	12.1.1	Procedimientos de operación documentados	Si	Se mantienen manuales operativos sobre los procesos fundamentales del área, que indiquen el qué hacer y cómo hacerlo al momento de llevar a acbo alguna actividad.	**4**	Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI
	8.1.2	12.1.2	Gestión de cambios	Si	Se encuentran formatos y registros de control de cambios para los sistemas de información a petición de los usuarios para mejora de funcionalidades o corrección de problemas, sin embargo no existe un documento formal para la gestión del cambio, sólo se basa en peticiones de los usuarios.	**2**	Los registros de control de cambios deben incluír los elementos de seguridad necesarios, la protección y revisión de los mismos y su inclusión en el SGSI

	8.1.3	12.1.3	Gestión de capacidad	Si	Existe una segregación de funciones para cada rol dentro de la dirección nacional SIMIT, aunque en algunas ocasiones un rol tiene funciones que no debería tener a falta de un control estricto. Se evidenció que algunos funcionarios tiene acceso a las plataformas sin controles establecidos que les impidan realizar una acción para la cual no están autorizados.	**2**	La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuale son está autorizado.
	8.1.4	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación		Se cuentan con ambientes de Producción y Desarrollo separados. Los datos en el ambiente de desarrollo y pruebas son datos reales de producción.	**3**	Los controles y protección de los datos deben ser iguales tanto para producción como para desarrollo y pruebas dado que son los mismos. El SGSI debería incluír lineamientos de manejo de los datos en Desarrollo y Pruebas con respecto a la confidencialidad de la información.
	8.2	12.2	Protección contra códigos maliciosos	Si			
	8.2.1	12.2.1	Controles contra códigos maliciosos		Actualmente la organización tiene sistemas de información antivirus licenciados que previenen la ejecución del código malicioso, tanto en servidores como en estaciones de trabajo.	**5**	Crear el esquema de revisión a toda la red, incrementar los controles manualmente a equipos detectados con infección. Realizar una revisión completa cada cierto periodo de tiempo, se recomienda cada mes para activos críticos, cada 3 meses para el resto.

	8.3	12.3	Copias de Respaldo Si				
	8.3.1	12.3.1	Respaldo de la información		La Organización cumple satisfactoriamente con este control y se tiene una política de backup documentada haciendo uso de un software cliente-servidor que respalda además las estaciones de trabajo.	**5**	Mantener esta politica y sociabilizarla al grupo de usuarios.
	8.4	12.4	Registro y Seguimiento Si				
	8.4.1	12.4.1	Registro de eventos	Si	La Organización no cumple con este control. Aunque se tienen los registros y las configuraciones de auditoría, estos no se revisan de manera formal y periódica.	**2**	Realizar revisiones periódicas a los registros y determinar un política de almacenamiento que detalle los términos y responsabilidades, así como los mecanismos de seguridad para tales registros.
	8.4.2	12.4.2	Protección de la información de registro	Si	La organización no tiene controles específicos para la protección del repositorio de base de datos del monitoreo y el sistema de archivos donde reciden los registros de auditoría.	**1**	El acceso a los registros debe ser exclusivo para los auditores, administradores de la plataforma y oficial de seguridad. Estos registros deben estar asegurados en un sistema de archivos protegido.

	8.4.3	12.4.3	Registros del administrador y del operador	Si	La organización cumple con pruebas de desempeño de la red pero no se realizan intruciones activas en la red (ejem. sniffer).	**3**	Mantener las revisiones periódicas, definir los periodos en el procedimiento de monitoreo y su relación con el de reacción a incidentes, verificar los Logs de auditoría de la actividad de administradores y operadores habilitados para est fin.
	8.4.4	12.4.4	Sincronización de relojes		Se tienen registros sobre la sincronía de sistemas en la organización y se hacen a través de NTP contra la superintendencia de industria y comercio.	**5**	Se debe mantener el procedimiento de sincronización de todos los Sistemas y Aplicaciones, con un sistema unificado para toda la plataforma tecnológica de la organización.
	8.5	12.5	Control de software operacional	Si			
	8.5.1	12.5.1	instalación de software en los sistemas operativos		Existen procedimientos de control de cambios para las aplicaciones, estos son autorizados por la interventoria, el concesionario y la FCM. Se solicitan los casos de uso de prueba a los desarrolladores.	**4**	Mantener el esquema implementado de revisión de sistemas y de puesta en producción.
	8,6	12,6	Gestión de vulnerabilidad técnica	Si			
	8.6.1	12.6.1	Gestión de las vulnerabilidades técnicas	SI	La dirección nacional SIMIT no realiza pruebas de vulnerabilidad a sus sistemas críticos. Sin embargo, el consecionario asegura realizar pruebas periódicas de seguridad (pentest).	**2**	Dada la critricidad de la información, debe mantenerse el esquema de pruebas internas (ya sea por capacitación de un funcionario o por tercerización) que permita una revisión periódica interna al

							respecto y no depender de las pruebas que realice el consecionario.
	8.6.2	12.6.2	Restricciones sobre la instalación de software		Los usuarios tienen restringido la instalaciòn de software debido a que trabajan a travès de terminales	**4**	Aunque existe la restricción se debe recordar la importancia de la no instalaciòn
	8.7	12.7	Consideraciones relacionadas con la auditoría interna		Si		
	8.7.1	12.7.1	Controles de auditorías de sistemas de información		Las auditorías no se realizan sobre los registros y sistemas de información, aunque tienen un comité que define unos procesos de auditoría.	**2**	Documentar e implementar dentro del SGSI, los casos y controles a tener en cuenta para las actividades de auditoría sobre sistemas en producción.
	9	13	. Seguridad de las comunicaciones				
	9.1	13.1	Gestión de la seguridad de las redes		Si		
	9.1.1	13.1.1	Controles de redes	Si	A pesar de contar con los elementos necesarios para el monitoreo de la red, no se realizan controles adecuados sobre tráfico, conexiones o revisión de anomalías. Sin embargo se tienen controles de acceso a la red por medio de VLANs.	**2**	Se debe utilizar una estrategia para la arquitectura de seguridad en la red LAN (desde el punto de vista de correlación de eventos y monitoreo de seguridad), para ubicar y configurar correctamente todos los elementos de seguridad y monitoreo en la red. Esto debe estar acompañado de una política de seguridad en el SGSI.

	9.1.2	13.1.2	Seguridad de los Servicios de Red	SI	La organización cumple con este control mediante un firewall que protege y restringe el acceso a las aplicaciones.	**3**	Generar una politica para mantener un adecuado control sobre todos los servicios de red e implementar un sistema de detección y prevención de intrusos interno.
	9.1.3	13.1.3	Separación en las redes		Existe una segmentación de la red a través de VLANS.	**5**	Mantener y monitorear la segmentación de la red junto con los equipos conectos a ella.
	9.2	13.2	Transferencia de información Si				
	9.2.1	13.2.1	Políticas y procedimientos de transferencia de información	Si	Los lineamientos con respecto a intercambio de información son incluídos a nivel de contrataciones y de acuerdos con entes reguladores, a través de acuerdos de confidencialidad, pero no se cuenta con controles para el intercambio seguro de información dentro de la organización, ni con sus terceros, los controles con los que se cuenta son los implementados por los Bancos que proveen algún servicio.	**2**	Implementar una metodologia para realizar un intercambio de información seguro. Se recomienda el uso de (boxcriptor) para encriptar el contenido que se publica en Dropbox.
	9.2.2	13.2.2	Acuerdos sobre transferencia de información	Si	Ademas de los acuerdos de confidencialidad, no se hacen controles adicionales sobre el intercambio de información.	**2**	El manejo de información y su intercambio con terceros debería incluír acuerdos sobre su transporte y almacenamiento seguros al tratar y manipular la información segura (por ejemplo comprimir y cifrar la información)

	9.2.3	13.2.3	Mensajería Electrónica	Si	El correo electrónico es el medio principal de comunicación de la organización. También se utiliza como repositorio de registros, actas, y otro tipo de constancias auditables. No se cuenta con encripción de mensajería.	**2**	Se debe mantener el esquema de seguridad sobre el correo a nivel de contingencias, antivirus, antispam y revisar periódicamente la efectividad de todos los controles, adicionalmente se requiere encripción, via PGP o S/MIME.
	9.2.4	13.2.4	Acuerdos de confidencialidad o de no divulgación		Se realizan acuerdos de confidencialidad específicos para la labor con terceros que implican la manipulación de información y el ingreso a areas, sin embargo, se da a conocer a algunos terceros sobre la política de seguridad pero no se hace firmar un documento que deje plena constancia de que el tercero conoce dichas políticas y acepta cumplirlas dentro de su ámbito de aplicación.	**3**	Incluír la política de seguridad en los acuerdos y contratos con terceros en su ámbito de aplicación.
	10	14	Adquisición, desarrollo y mantenimiento de sistemas				
	10.1	14..1	Procesamiento correcto en aplicaciones SI				
	10.1.1.	14.1.1	Análisis y especificación de requisitos de Seguridad de la información	Si	Los requisitos relacionados con seguridad de la informacion se deben incluir en los requisitos para nuevas sistemas de informacion o para mejoras a los sistemas de informacion existentes.	**3**	Si se lleva a cabo un análisis de los requisitos de seguridad, pero no se realiza de una forma específica, simplemente se emiten conceptos y recomendaciones. El mismo procedimiento no se tiene documentado, determinar los mecanismos utilizados frente a la definición de

							los requisitos de seguridad.
	10.1.2	14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Si	La informacion involucrada en los servicios de las aplicaciones que pasan sobre redes publicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgacion y modificacion no autorizadas	**4**	Los controles de seguridad implementados frente a los servicios de aplicación en redes públicas corresponden a Firewall. Así mismo las redes de la entidad se encuentran segregadas por medio de VLAN`s.
	10.1.3	14.1.3	Protección de transacciones de los servicios de las aplicaciones		La informacion involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la trasmision incompleta el enrrutamiento errado, la alteracion no autorizada de mensajes, la divulgacion no autorizada y la duplicacion o reproduccion de mensajes no autorizada	**4**	Conforme la información brindada durante el levantamiento de información, se asegura que las transacciones de los servicios son protegidas con los protocolos seguros.
	10.2	14.2	Seguridad en los procesos de desarrollo y soporte		Si		
	10.2.1	14.2.1	Política de desarrollo seguro	Si	El desarrollo cumple con los estandares	**4**	Vigilar con frecuencia el cumpliminento de los estàndares
	10.2.2	14.2.2	Procedimientos de control de cambios de sistemas	Si	La Organización cumple satisfactoriamente con este control	**5**	Mantener el esquema implementado.
	10.2.3	14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Si	La Organización cumple satisfactoriamente con este control, sin embargo no hay un documento formal para aprobar cambios en los sistemas operativos.	**3**	Mantener el esquema implementado. Realizar una plantilla de control de cambios (RACI)

							para los sistemas operativos.
	10.2.4	14.2.4	Restricciones en los cambios a los paquetes de software.	Si	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente	**4**	Con respecto a la informaciòn recaudada se evidencia que hay desarrollo in house y se lleva a control de cambios
	10.2.5	14.2.5	Principios de construcción de los sistemas seguros	Si	Se deben establecer, documentar y mantener principios para la construccion de sistemas seguros, y aplicarlos a cualquier actividad de implementacion de sistemas de informacion.	**3**	
	10.2.6	14.2.6	Ambiente de desarrollo seguro	Si	No se cuenta con un estándar para el desarrollo seguro de aplicaciones, por lo tanto en algunos casos se pueden aceptar entradas no esperadas por las aplicaciones o la base de datos. Depende de la aplicación filtrar los datos de los formularios o campos de texto. Existe un WAF que proteje los sistemas SIMIT de entradas maliciosas.	**4**	Implementar un estándar de desarrollo seguro de aplicaciones que cumpla con las políticas específicas de seguridad, en la revisión de entradas, procesamiento y salidas de información.
	10.2.7	14.2.7	Desarrollo contratado externamente		La Organización no cumple satisfactoriamente con este control mas alla de su funcionabilidad.	**2**	Se debe crear una guía fundamental de principios de seguridad a tener en cuenta por parte de los terceros y hacer recepción y aprobación del código fuente o en su defecto al software funcional.
	10.2.8	14.2.8	Pruebas de Seguridad de sistemas	Si	Durante el desarrollo se deben llevar a cabo pruebas de	**0**	Conforme lo establecido por el área de Tecnología, ellos

					funcionalidad de la seguridad		tienen implementados flujos de pruebas y casos de usos para las pruebas de seguridad y aceptación de los sistemas. Así mimso se solicita al proveedor unas pruebas de las mismas.
	10.2.9	14.2.9	Prueba de aceptación de sistemas		La organización no tiene un procedimiento formal para la aceptación de sistemas de tal forma que se le exija a los proveedores cumplir ciertos lineamientos de seguridad antes de poner un sistema en producción.	**1**	Procedimiento de establecimiento de requerimientos para la aceptación de nuevos sistemas ó modificaciones sobre los existentes.
	10.3	14.3	Datos de Prueba				
	10.3.1	14.3.1	Protección de datos de prueba		Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente	**3**	Según se evidencia FCM tiene protegidos los datos de prueba
	11	15	Relaciones con los proveedores				
	11.1	15.1	Seguridad de la información en las relaciones con los proveedores				
	11.1.1	15.1.1	Política de Seguridad de la información para las relaciones con proveedores		Los requisitos de seguridad de la informacion para mitigar los riesgos asociadas con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	**4**	En las etapas precontractuales se lleva a cabo un proceo de indentificación de los posibles riesgos que puenda llegar a materializarse, con el fin de buscar los controles para mitigarlos, así mismo se desarrollan cláusulas de confidencialidad con los proveedores

	11.1.2	15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores		Se deben establecer y acordar todos los requisitos de seguridad de la informacion pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la informacion de la organizacion.	**3**	Se realiza un análisis conforme las disposiciones del gobierno dependiendo los tipos de contratación a celebrar.
	11.1.3	15.1.3	Cadena de suministro de tecnología de información y comunicación.		Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la informacion asociadas con la cadena de suministro de productos y servicios de tecnologia de infonmacion y comunicacion.	**3**	Para cualquier nuevo proyecto TIC se tiene en cuenta el análisis de los riesgos de seguridad de la información ante la planeación, análisis y viabilidad de los proyectos, pero no se evidenció documentación.
	11.2	15.2	Gestión de la prestación de servicios de proveedores				
	11.2.1	15.2.1	Seguimiento y revisión de los servicios de los proveedores		Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestacion de servicios de los proveedores.	**0**	Se realiza un seguimiento mensuelmente frente a la supervisión de los contratos, en donde se revisa el cumplimiento del objeto contractual y determinar el nievel de cumplimiento del contrato.
	11.2.2	15.2.2	Gestión de cambios en los servicios de los proveedores		Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las politicas, procedimientos y controles de seguridad de la informacion existentes , teniendo en cuenta la criticidad de la informacion, sistemas y procesos del negocio involucrados, y la	**0**	Existe un formato que se diligencia frente al cumplimiento del proveedor, así mismo se realiza la respectiva evaluación y se solicita si es necesario cambios frente a los servicios.

					reevaluacion de los riesgos.		
	12	16	Gestión de incidentes de seguridad de la información				
	12.1	16.1	Gestión de incidentes y mejoras en la seguridad de la información		Si		
	12.1.1	16.1.1	Responsabilidades y procedimientos	Si	No hay un documento formal y divulgado sobre las responsabilidades de cada rol en un incidente de seguridad de la información.	**1**	Documentar y divulgar formalmente el proceso implementado dentro del marco del SGSI.
	12.1.2	16.1.2	Reporte de eventos de Seguridad de la información.	Si	Se tiene un procedimiento de identificación y tratamiento de incidentes concernientes a la seguridad de la información, pero no se tiene conciencia de los mismos en la organización.	**3**	Durante la campaña de concientizacion y entrenamiento, identificar claramente los incidentes relacionados con la seguridad de la información y su reporte. La caracterización debe traducirse en la forma como se hace seguimiento en la mesa de ayuda y dentro del grupo de seguridad
	12.1.3	16.1.3	Reporte de debilidades de seguridad de la información		Se identifican las debilidades teóricas concernientes a la seguridad en todos los aspectos (análisis de riesgos de seguridad de la información interno y periódico)	**5**	Actualizar rapidamente el análisis de riesgo de la infraestructura adquirida recientemente en la Federación Colombiana de Municipios - Dirección Nacional SIMIT, ya que esto genera un gran cambio en la identificación de debilidades y vulnerabilidades.

	12.1.4	16.1.4	Evaluación de eventos de Seguridad de la información y decisiones sobre ellos		Los eventos de seguridad de la informacion se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la informacion	**0**	No existe un procedimiento asociado a incidentes de seguridad de la información.
	12.1.5	16.1.5	Respuesta a incidentes de seguridad de la información	Si	Los eventos de seguridad de la informacion se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la informacion	**0**	
	12.1.6	16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Si	No se realizan estudios (por ejemplo: análisis forenses) de los incidentes de seguridad. Algunos intentos de intrusión son monitoreados.	**1**	Además de tipificar esta labor como parte de las actividades de un oficial de seguridad, definir el procedimiento adecuado en el SGSI y realizar la revisión a todos los reportes de incidentes e incluírlos en el plan de mejoramiento.
	12.1.7	16.1.7	Recolección de evidencia		No se tiene la conciencia de la gravedad de un incidente de seguridad (a nivel de usuarios finales) lo que hace lento el proceso de recolección de evidencia si se llegare a presentar.	**1**	Diseñar e implemetnar el procedimiento detallado de recolección de evidencia que permita de forma efectiva obtener toda la información necesaria y conscientizar a los usuarios del impacto que puede tener un incidente y las demoras que representaría en su trabajo para la toma de evidencias.
	13	17	Aspectos de Seguridad de la información de la gestión de continuidad de negocio				
	13.1	17.1	Continuidad de Seguridad de la información		Si		

	13.1.1	17.1.1	Planificación de la continuidad de la seguridad de la información	Si	Se debería mantener un esquema único de planes de continuidad del negocio para garantizar que dichos planes son consistentes, para tratar los requisitos de seguridad y para identificar las prioridades de prueba y mantenimiento.	**2**	Unificar los términos de análisis para el impacto y los riesgos evaluados en los planes de continuidad del negocio.
	13.1.2	17.1.2	Implementación de la continuidad de la seguridad de la información	Si	No se han implementado los planes de continuidad del negocio en todos los procesos críticos, aparte del de TI.	**2**	Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria.
	13.1.3	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información		No se realizan revisiones a los planes de continuidad del negocio. Se tiene un plan pero al no ejecutarse carecen de elementos y experiencia para su actualización.	**2**	Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
	13.2	17.2	Redundancia				
	13.2.1	17.2.1	Disponibilidad de instalaciones de procesamiento de información		Las instalaciones de procesamiento de informacion se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad	**0**	FCM cuenta con centros de procesamiento de información alternos que brindan la disponibilidad requerida por la entidad.
	14	18	Cumplimiento				
	14.1	18.1	Cumplimiento de recursos legales y contractuales				
	14.1.1	18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Si	La Organización cumple satisfactoriamente con este control, se cuenta con los controles establecidos para la función publica y con las exigencias de los entes externos como la contraloría y la DIAN.	**4**	Extender la investigación de legislaciones aplicables a los temas de seguridad de la información.

	14.1.2	18.1.1	Derechos de propiedad intelectual	Si	La Organización cumple satisfactoriamente con este control, tiene pleno respeto por el licenciamiento del software en todos sus sistemas. Se tiene implementado un control donde se realiza un reporte anual acerca de licenciamiento de Software, este es realizado por TICs.	**5**	Mantener el esquema implementado. Generar una política de cumplimiento sobre la propiedad intelectual.
	14.1.3	18.1.1	Protección de registros	Si	Los registros organizacionales tienen salvaguarda y se aplican una serie de medidas como la retención y clasificación por tipos, sin embargo no se tiene una política para el control de medios de almacenamiento removibles.	**4**	Establecer procedimientos especiales de seguridad para los registros organizacionales de clasificación ultra-secreta.
	14.1.4	18.1.1	Privacidad y protección de información de datos personales	Si	La Organización cumple satisfactoriamente con este control, tiene una política de protección de datos personales.	**3**	Extender la investigación de legislaciones aplicables a los temas de derecho a la intimidad.
	14.1.5	18.1.1	Reglamentación de controles criptográficos		No se tienen identificados o aplicados los lineamientos específicos sobre uso de controles criptográficos a la información	**1**	Debe realizarse la adecuada revisión de cuales regulaciones afectan el uso de controles criptográficos y considerarlos para su implementación
	14.2	18.2	Revisiones de Seguridad de la información		Si		

	14.2.1	18.2.1	Revisión independiente de la seguridad de la información	Si	Existen políticas de seguridad de la información documentadas, pero falta sociabilizarlas y crear conciencia mediante programas formales y recurrentes. Actualmente el alcance de la política cubre globalmente la seguridad de la información, la organización de seguridad de la información, gestión de activos, gestión del personal, seguridad física y del entorno, gestión de las operaciones y comunicaciones, control de acceso, adquisición, desarrollo y mantenimiento de los sistemas de información, gestión de incidentes y gestión de la continiudad del negocio.	**2**	Existen políticas de seguridad de la información documentadas, pero falta sociabilizarlas y crear conciencia mediante programas formales y recurrentes. Actualmente el alcance de la política cubre globalmente la seguridad de la información, la organización de seguridad de la información, gestión de activos, gestión del personal, seguridad física y del entorno, gestión de las operaciones y comunicaciones, control de acceso, adquisición, desarrollo y mantenimiento de los sistemas de información, gestión de incidentes y gestión de la continiudad del negocio.

	14.2.2	18.2.2	Cumplimiento con las políticas y normas de Seguridad	Si	Existen políticas de seguridad de la información documentadas, pero falta sociabilizarlas y crear conciencia mediante programas formales y recurrentes. Actualmente el alcance de la política cubre globalmente la seguridad de la información, la organización de seguridad de la información, gestión de activos, gestión del personal, seguridad física y del entorno, gestión de las operaciones y comunicaciones, control de acceso, adquisición, desarrollo y mantenimiento de los sistemas de información, gestión de incidentes y gestión de la continiudad del negocio.	**2**	Existen políticas de seguridad de la información documentadas, pero falta sociabilizarlas y crear conciencia mediante programas formales y recurrentes. Actualmente el alcance de la política cubre globalmente la seguridad de la información, la organización de seguridad de la información, gestión de activos, gestión del personal, seguridad física y del entorno, gestión de las operaciones y comunicaciones, control de acceso, adquisición, desarrollo y mantenimiento de los sistemas de información, gestión de incidentes y gestión de la continiudad del negocio.
	14.2.3	18.2.3	Revisión del cumplimiento técnico	Si	Existen políticas de seguridad de la información documentadas, pero falta sociabilizarlas y crear conciencia mediante programas formales y recurrentes. Actualmente el alcance de la política cubre globalmente la seguridad de la información, la organización de seguridad de la información, gestión de activos, gestión del personal, seguridad física y del entorno,	**2**	Existen políticas de seguridad de la información documentadas, pero falta sociabilizarlas y crear conciencia mediante programas formales y recurrentes. Actualmente el alcance de la política cubre globalmente la seguridad de la información, la organización de seguridad de la

					gestión de las operaciones y comunicaciones, control de acceso, adquisición, desarrollo y mantenimiento de los sistemas de información, gestión de incidentes y gestión de la continuidad del negocio.		información, gestión de activos, gestión del personal, seguridad física y del entorno, gestión de las operaciones y comunicaciones, control de acceso, adquisición, desarrollo y mantenimiento de los sistemas de información, gestión de incidentes y gestión de la continuidad del negocio.

Medición del nivel de madurez en cada dominio

Ahora teniendo realizado la lista de chequeo, se realiza la evaluación de Nivel de Madurez de Cumplimiento conforme a la Tabla de Calificaciones previamente expuesta.

Tabla 11:Nivel de madurez por dominio

Dominio	Porcentaje Cumplimiento	Tabla de Calificaciones			
1. Política de Seguridad	2%	Cada uno de los requerimientos de las hojas de los DOMINIOS ha sido calificado en una escala del 1 al 5 (Siendo 1 debilidad y 5 fortaleza) Estos valores tienen como referencia la valoración del DAF			
2. Organización de la Seguridad de la Información	6%				
3. Seguridad en los Recursos Humanos	5%	**Valoración**	**Efectividad**	**Cumplimiento**	**FCM DIR SIMIT**
4. Gestión de Activos	7%			**Con respecto al control, es un control debil, cumple o excede las expectativas**	
5. Control de Acceso	13%	**1**	**No implantado**	No existen controles – Carencia completa de documentación y procesos	11%
6. Controles Criptográficos	1%	**2**	**50%**	Controles no estandar – La organización conoce los problemas y tiene intención de solucionarlos, algunos con enfoques propios, pero nada estandarizado	24%
7. Seguridad física y del entorno	18%	**3**	**90%**	El Requerimiento se Cumple en forma aceptable - Aunque existen los controles, no se comunican y/o difunden para crear consciencia y no se hace entrenamiento y seguimiento	21%
8. Seguridad de operaciones	14%	**4**	**95%**	Controles Eficientes - Los controles se han documentado y estandarizado, se han seguido entrenamientos, sin embargo la aplicación de los mismos en algunos casos es por cuenta propia del individuo.	22%
9. Seguridad de las comunicaciones	6%	**5**	**Administrado**	Optimizado – Es posible administrar los controles y medir el cumplimiento de los mismos para tomar medidas cuando no estén ejecutándose de forma debida.	14%

Continuacion Tabla 11.		
10. Adquisición, desarrollo y mantenimiento de sistemas	13%	
11. Relaciones con los proveedores	3%	
12. Gestión de incidentes de seguridad de la información	3%	
13. Aspectos de Seguridad de la información de la gestión de continuidad de negocio	2%	
14. Cumplimiento	7%	
	100%	

Figuras del Nivel de Cumplimiento con base al SGSI.

Figura 15. Nivel de Madurez con base al SGSI.

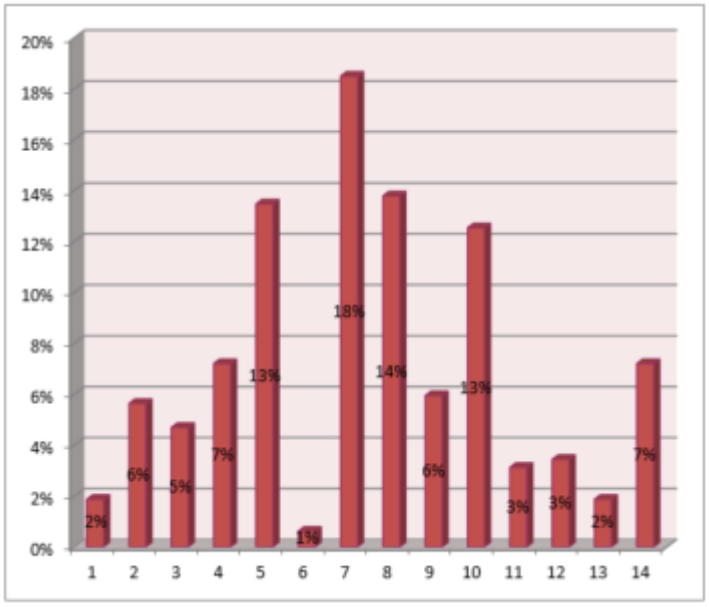


Figura 16. Nivel de Madurez con base al SGSI.

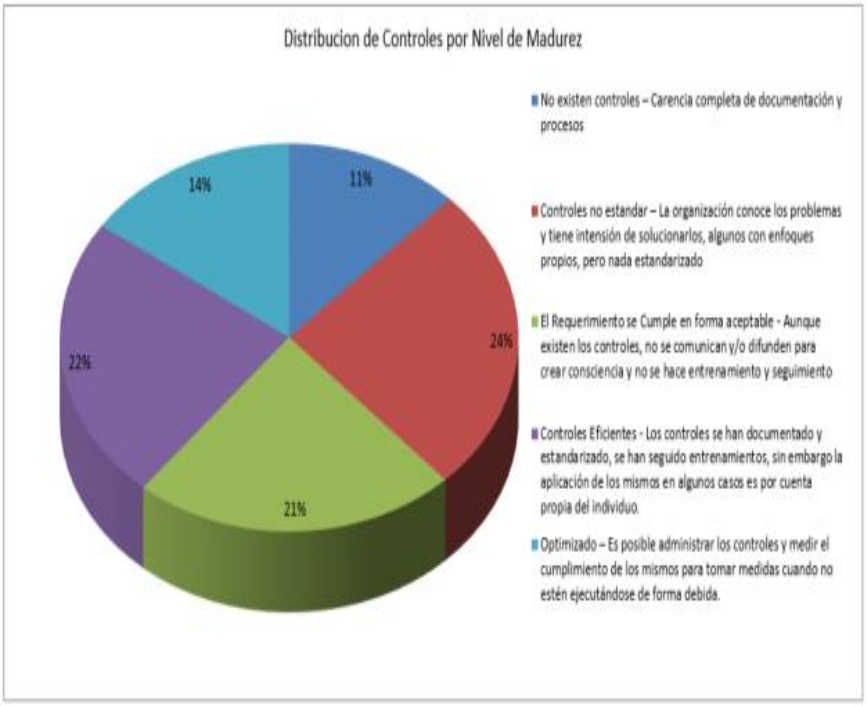
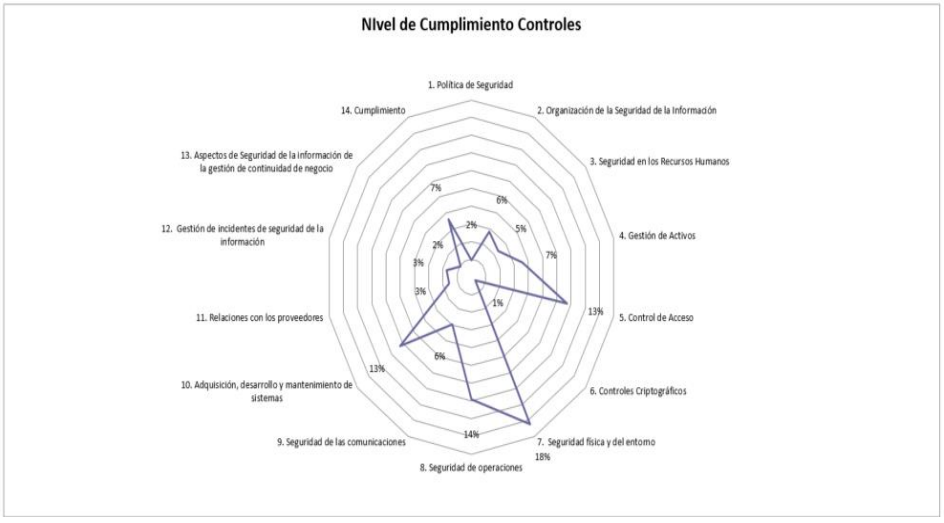


Figura 17. Nivel de Madurez con base al SGSI.



Declaracion de Aplicabilidad – SOA.

Tabla 12: Declaracion de aplicabilidad -SOA

	DECLARACIÓN DE APLICABILIDAD DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN ISO 27001:2013							
N° A5	Dominio - Control		#Controles	Control	Controles Implementados	Controles para Tratamiento	Exclusión (S/N)	Justificación
	Política de seguridad de la información		2					
A.5.1	Directrices de la Dirección en Seguridad de la Información.							
A.5.1.1	Política para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Se incluye como parte integral de los requisitos del estándar para el SGSI de la entidad. Tiene asociado el numeral 5.2. de la norma de la referencia.
A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas de seguridad de información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúas.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Se incluye como parte integral de los requisitos del estándar para el SGSI en la entidad. Tiene asociado el numeral 5.2. de la norma de la referencia.
A6	Organización de la seguridad de la información		7					
A.6.1	Organización Interna.		5					
A.6.1.1	Roles y responsabilidades para la seguridad de la información.	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Se incluye como parte integral de los requisitos del estándar para el SGSI en la entidad. Tiene asociado el numeral 5.3. de la norma de la referencia.

A.6.1.2	Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad, se debe contar con este control implementado.
A.6.1.3	Contacto con las autoridades	Se deben mantener contactos apropiados con las autoridades pertinentes.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, cumplir con la regulación del Gobierno colombiano, además de contar con entidades externas que prestan servicios de TI, se debe contar con este control implementado.
A.6.1.4	Contacto con grupos de interés especiales	Se debe mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información y asociaciones de	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad, se debe contar con este control implementado.
A.6.1.3	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad, se debe contar con este control implementado.
A6.2	Dispositivos móviles y teletrabajo		2					
A.6.2.1	Política para dispositivos móviles	Se debe adoptar una política y unas medidas de seguridad de soporte, para la gestión de los riesgos introducidos por el uso de dispositivos móviles.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, cumplir con la regulación del Gobierno colombiano, además de contar con entidades externas que prestan servicios de TI, se debe contar con este control implementado.

A.6.2.2	Teletrabajo	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza el teletrabajo.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	La Entidad cuenta con esta modalidad de trabajo dando cumplimiento a la Ley 1221 de 2008 Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
A7	Seguridad de los recursos humanos		6					
A7.1	Antes de asumir el empleo		2					
A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo. Se deben llevar a cabo d acuerdo con las leyes, reglamentos y ética pertinente, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a la que se va a tener acceso y a los riesgos percibidos.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad, por la naturaleza de su entidad y en particular para los procesos de selección de personal, se debe contar con este control implementado.

A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades obligaciones y las de la organización en cuanto a seguridad de información.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad, por la naturaleza de su entidad y en particular para los procesos de selección de personal, se debe contar con este control implementado.
A.7.2	Durante la vigencia del empleo		3					
A.7.2.1	Responsabilidades de la dirección	La Dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad, por la naturaleza de su entidad y en particular para los procesos de selección

								de personal, se debe contar con este control implement ado.

A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la organización y en donde sea pertinente, los contratistas deben recibir la educación y la formación en la toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad, por la naturaleza de su entidad y en particular para los procesos de selección de personal, se debe contar con este control implementado.
A.7.2.3	Proceso disciplinario	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra los empleados que hayan cometido una violación a la seguridad de la información.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.7.3	Terminación o cambio de empleo		1					

A.7.3.1	Responsabilidades en la terminación.	Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se debe hacer cumplir.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.8	Gestión de activos		10					
A8.1	Responsabilidad por los activos		4					
A.8.1.1	Inventario de activos	Se deben identificar los activos asociados con la información e instalaciones de procesamiento de información, y se debe elaborar y mantener un	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Se incluye como parte integral de los requisitos del estándar para el SGSI en la entidad de acuerdo con la definición del alcance.
A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Se incluye como parte integral de los requisitos del estándar para el SGSI en la entidad de acuerdo con la definición del alcance.
A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Se incluye como parte integral de los requisitos del estándar para el SGSI en la entidad de acuerdo con la definición del alcance.

A.8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Se incluye como parte integral de los requisitos del estándar para el SGSI en la entidad de acuerdo con la definición del alcance.
A.8.2	Clasificación de la información: Asegurar que la información recibe		3					
A.8.2.1	Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Se incluye como parte integral de los requisitos del estándar para el SGSI en la entidad.
A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo al esquema de clasificación de información adoptado por la organización.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.

A.8.2.3	Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por el organismo.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Se incluye como parte integral de los requisitos del estándar para el SGSI en la entidad.
A.8.3	Manejo de medios: Evitar la divulgación, la modificación, el retiro o la		3					

A.8.3.1	Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	Gestión de medios removibles	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.8.3.2	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales	Disposición de los medios	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.8.3.3	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	Transferencia de medios fisicos	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.9	Control de acceso		14					
A 9.1	Requisito del negocio para el control de acceso: Limitar el acceso a		2					
A.9.1.1	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.9.1.2	Acceso a redes y a servicios en red	Solo se debe permitir el acceso de lso usuarios a la red y a los servicios de red	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe

		para los que hayan sido autorizados específicamente.						contar con este control implementado.
A.9.2	Gestión de acceso de usuarios: Asegurar el acceso de usuarios		6					
A.9.2.1	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.9.2.2	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios, para todos los sistemas y servicios.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.

A.9.2.5	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.

A.9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o sedebn ajustar cuando se	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.9.3	Responsabilidades de los usuarios: Hacer que los usuarios rindan		1					
A.9.3.1	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las practicas	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.9.4	Control de acceso a sistemas y aplicaciones: Evitar el acceso no		5					
A.9.4.1	Restricciones de acceso a la información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar

								con este control implementado.
A.9.4.2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.

A.9.4.4	Uso de los programas utilitarios privilegiados	Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de las aplicaciones.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.9.4.5	Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se

								debe contar con este control implementado.
A.10	Criptografía		2					
A.10.1	Controles criptográficos: Asegurar el uso apropiado y eficaz de la		2					
A.10. 1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad informática, explícitamente y por el intercambio de datos con entidades externas, se debe contar con este control implementado.
A.10. 1.2	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad informática, explícitamente y por el intercambio de datos con entidades externas, se debe contar con este control implementado.
A.11	ida. Seguridad física y del entorno		13					
A.11.1	Áreas seguras: Prevenir el acceso físico no autorizado, el daño y la		6					
A.11.1 .1	Perímetro de seguridad física.	Se deben definir y usar perímetros de seguridad y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad información, explícitamente y debido a que las instalaciones de la Entidad contienen información sensible, se debe contar con este control implementado.

A.11.1.2	Controles de acceso físico	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se le permita el acceso a personal autorizado.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad información, explícitamente y debido a que las instalaciones de la Entidad contienen información sensible, se debe contar con este control implementado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar la seguridad física a oficinas, recintos e instalaciones.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad información, explícitamente y debido a que las instalaciones de la Entidad contienen información sensible, se debe contar con este control implementado.
A.11.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos y accidentes.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad información, explícitamente y debido a que las instalaciones de la Entidad contienen información sensible, se debe contar con este control implementado.
A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad información, explícitamente y debido a que las instalaciones de la Entidad contienen información sensible, se debe contar con este control implementado.

A.11.1.6	Áreas de despacho y carga	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.11.2	Equipos: Prevenir la pérdida, daño, robo o compromiso de activos, y la		7					

A.11.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir el riesgo de amenaza y peligros del entorno, y las posibilidades de acceso no autorizado.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.11.2.2	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.

A.11.2.3	Seguridad del Cableado	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.11.2.4	Mantenimiento de equipos	Los equipos deben mantener correctamente para asegurar disponibilidad e integridad continuas.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.11.2.5	Retiro de activos	Los equipos, información, software no se deben retirar de su sitio sin autorización previa.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	Se deben aplicar medidas de seguridad a los activos que se encuentren fuera de las instalaciones de la organización teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.

A.11.2.7	Disposición segura o reutilización de equipos	Se debe verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito de forma segura, antes de su disposición o	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.11.2.8	Equipos de usuario desatendido	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.11.2.9	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removible, y una política de pantalla limpia en las instalaciones de procesamiento de	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad para el fortalecimiento del control interno en la entidad y por su componente público, se debe contar con este control implementado.
A.12	Seguridad de las operaciones		16					
A.12.1	Procedimientos operacionales y responsabilidades: Asegurar las		4					
A.12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, explícitamente se debe controlar las operaciones efectuadas, por tanto se debe contar con este

								control implementado.
A.12. 1.2	Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sitemas de procesamiento de información que afectan la seguridad de la información.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, explícitamente se debe controlar las operaciones efectuadas, por tanto se debe contar con este control implementado.

A.12. 1.3	Gestión de capacidad	Se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, explícitamente se debe controlar las operaciones efectuadas, por tanto, se debe contar con este control implementado.
A.12. 1.4	Separación de los ambientes de desarrollo, pruebas y operación.	Se deben separar los ambientes de desarrollo, de prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, explícitamente se debe contar con ambientes de desarrollo y prueba de los sistemas de información, por tanto se debe contar con este control implementado.
A.12.2	Protección contra códigos maliciosos: Asegurarse de que la		1					

A12.2.1.	Controles contra códigos maliciosos	Se deben implementar controles de detección de prevencion y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la informacion, explicitamente se debe contar con controles contra codigos maliciosos que protejan la infraestructura de la SNS, por tanto se debe contar con este control implementado.
A12.3.	Copias de Respaldo: Proteger contra la perdida de daños		1					
A12.3.1.	Respaldo de la Informacion	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una politica de copias de respaldo acordadas.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, explicitamente se debe contar con controles de respaldo de la información para preservar la disponibilidad de la información, por tanto se debe contar con este control implementado.
A12.4.	Registro y Seguimiento: Registrar eventos y generar evidencia		4					
A12.4.1.	Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones fallas y eventos de seguridad de la informacion.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la informacion, explicitamente se debe contar con controles de registro de eventos que puedan afectar la seguridad de la información, por tanto se debe contar con este control implementado.

A12.4.2.	Protección de la infomación de registro.	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la informacion, explicitamente se debe contar con controles de registro de eventos que puedan afectar la seguridad de la información, por tanto se debe contar con este control implementado.
A12.4.3.	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la informacion, explicitamente se debe contar con controles de registro de eventos que puedan afectar la seguridad de la información, por tanto se debe contar con este control implementado.
A12.4.4.	Sincronización de Relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la informacion, explicitamente se debe contar con la sincronización de relojes en los sistemas de información, por tanto se debe contar con este control implementado.
A12.5.	Control de Software Operacional: Asegurarse de la integridad de los sistemas operacionales.		1					

A12.5.1.	Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, se debe contar con controles para la instalación de software, por tanto se debe contar con este control implementado.
A12.6.	Gestión de las vulnerabilidad técnica: Prevenir el		4	,				
A12.6.1.	Gestión de las vulnerabilidades técnicas	Se obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, se debe contar con controles para la gestión de vulnerabilidades técnicas, por tanto se debe contar con este control implementado.
A12.6.2.	Restricciones sobre la instalación de software.	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, se debe contar con controles para la instalación de software, por tanto se debe contar con este control implementado.
A12.7.	Consideraciones sobre auditorias de sistemas de infomación:		1					

A12.7. 1.	Controles de auditoria de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, explícitamente se debe contar con controles de auditoría, por tanto se debe contar con este control implementado.
A13.	SEGURIDAD DE LAS COMUNICACIONES		7					
A13.1.	Gestión de la seguridad de las redes: Asegurar la protección de la		3					
A.13. 1.1.	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información y para dar un adecuado uso a las redes de información, se debe contar con este control implementado.
A13.1 .2.	Seguridad de los servicios de red.	Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información y para dar un adecuado uso a las redes de información, se debe contar con este control implementado.
A 13.1.3 .	Separación en las redes.	Los grupos de servicios de información, usuarios y sistemas de información se deben separar de las redes.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información y para dar un adecuado uso a las redes de información, se debe contar con este control implementado.

A13.2.	Transferencia de información: Mantener la seguridad de la		4					
A13.2.1	Politicas y procedimientos de transferencia de información.	Se debe contar con políticas, procedimietos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de isntalaciones de comunicaciones.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad informática, explicitamente y por el intercambio de datos con entidades externas, se debe contar con este control implementado.
A13.2.2.	Acuerdos sobre transferencia de información.	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad informática, explicitamente y por el intercambio de datos con entidades externas, se debe contar con este control implementado.
A13.2.3.	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería eletrónica.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad informática, explicitamente y por el intercambio de datos con entidades externas, se debe contar con este control implementado.
A13.2.4.	Acuerdos de confidencialidad o de no divulgación.	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad informática, explicitamente y por el intercambio de datos con entidades externas, se debe contar

		protección de la información.						con este control implementado.
A14.	ADQUISICION Y MANTEMIENTO DE SISTEMAS		13					
A14.1.	Requisitos de seguridad de los sistemas de información: Asegurar		3					
A14.1.1.	Análisis y especificación de requisitos de seguridad de la información.	Los requsitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, y especificamente con el desarrollo de sistemas de información en su fase inicial, se debe contar con este control implementado.
A14.1.2.	Seguridad de servicios de las aplicaciones en redes públicas.	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, y especificamente los sistemas de información que son expuestas a redes públicas, se debe contar con este control implementado.

A14.1.3.	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la trasmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, y especificamente en la protección de los servicios de las aplicaciones, se debe contar con este control implementado.
A14.2.	Seguridad en los procesos de desarrollo y de soporte: Asegurar		9					
A14.2.1.	Política de desarrollo seguro.	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrolladores dentro de la organización.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, la Entidad debe contar con una política de Desarrollo Seguro clara, por tanto se debe contar con este control implementado.
A14.2.2.	Procedimiento de control de cambios en sistemas.	Los cambios a los sistemas dentro dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, se debe controlar los cambios en los sistemas de información, por tanto se debe contar con este control implementado.
A14.2.3.	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.	Cuando se cambian las plataformas de operación, se debn revisar las aplicaciones críticas del negocio, y	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, se debe controlar los cambios en los sistemas de información, por tanto se debe contar con este

		someter a prueba para asegurar que no haya impacta adverso en las operaciones o seguridad de la						control implementado.
A14.2.4.	Restricciones en los cambios a los paquetes de software	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, se debe restringir los cambios en los paquetes de software, por tanto se debe contar con este control implementado.
A14.2.5.	Principios de construccion de los sistemas seguros.	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad informática se debn establecer los principios de construcción de sistemas de información seguros, por tanto se debe contar con este control implementado.
A14.2.6.	Ambiente de desarrollo seguro.	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas de comprendan todo el ciclo de	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad informática, se debe contar con ambientes de desarrollo seguro, protegidos adecuadamente para las actividades de desarrollo de los sistemas de información, por tanto se debe contar con este control implementado.

		vida de desarrollo						
A14.2.7.	Desarrollo contratado externamente	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad informática, los servicios de desarrollo tercerizados se deben controlar adecuadamente, por tanto se debe contar con este control implementado.
A14.2.8.	Pruebas de seguridad de Sistemas	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de seguridad.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad informática se deben realizar pruebas de seguridad a los sistemas de información durante el desarrollo, por tanto se debe contar con este control implementado.
A.14.2.9.	Prueba de aceptación de Sistemas	Para los Sistemas de información nuevos, actualizaciones y nuevas versiones, se debn establecer programas de prueba para aceptación y criterios de aceptación relacionados.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad informática se deben realizar pruebas de aceptación a los sistemas de información, por tanto se debe contar con este control implementado.
A14.3.	Datos de prueba: Asegurar la protección de los datos usados para		1					

A14.3.1.	Protección de datos de prueba.	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información se deben proteger los datos de prueba adecuadamente en los sistemas de información, por tanto se debe contar con este control implementado.
A15.	RELACIONES CON LOS PROVEEDORES		5					
A15.1.	Seguridad de la información en las relaciones con los		3					
A15.1.1.	Política de seguridad de la información para las relaciones con proveedores.	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, la Entidad debe contar con la Politica de seguridad de la información en la relación con los proveedores a fin de mitigar los riesgos que se puedan presentar durante la prestaciión de los servicios, por tanto se debe contar con este control implementado
A15.1.2.	Tratamiento de la seguridad dentro de los acuerdos con proveedores.	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, la Entidad debe contar con la Politica de seguridad de la información en la relación con los proveedores a fin de mitigar los riesgos que se puedan presentar durante la prestaciión de los servicios, por tanto se debe

		suministrar componentes de infraestructura de TI para la información de la						contar con este control implementado
A15.1.3.	Cadena de suministro de tecnología de información y comunicación.	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, la Entidad debe contar con la Politica de seguridad de la información en la relación con los proveedores a fin de mitigar los riesgos que se puedan presentar durante la prestaciión de los servicios, por tanto se debe contar con este control implementado
A15.2.	Gestión de la prestación de servicios de proveedores: Mantener		2					

A15.2.1.	Seguimiento y revisión de los servicios de los proveedores.	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de los servicios de los proveedores.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, la Entidad debe hacer seguimiento y revisión a los servicios prestados por los proveedores a fin de mitigar los riesgos que se puedan presentar durante la prestaciión de los servicios, por tanto se debe contar con este control implementado

A15.2.2.	Gestión de cambios en los servicios de los proveedores.	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información , sistemas y procesos del negocio involucrados, y la	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información, la Entidad debe hacer seguimiento a la gestión de los cambios en la revisión a los servicios prestados por los proveedores a fin de mitigar los riesgos que se puedan presentar durante la prestación de los servicios, por tanto se debe contar con este control implementado
A16.	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA		7					
A16.1.	Gestión de incidentes y mejoras en la seguridad de la		7					
A16.1.1.	Responsabilidades y procedimientos.	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información la Entidad debe gestionar adecuadamente los incidentes de seguridad de la información, por tanto se debe contar con este control implementado.
A16.1.2.	Reporte de eventos de seguridad de la información.	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información la Entidad promover el reporte de eventos de seguridad de la información, por tanto se debe contar con este control implementado.

A16.1.3.	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información la Entidad promover el reporte de debilidades de seguridad de la información, por tanto se debe contar con este control implementado.
A16.1.4.	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información la Entidad debe gestionar adecuadamente los incidentes de seguridad de la información, por tanto se debe contar con este control implementado.
A16.1.5.	Respuesta a incidentes de seguridad de la información.	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información la Entidad debe gestionar adecuadamente los incidentes de seguridad de la información, por tanto se debe contar con este control implementado.
A16.1.6.	Aprendizaje obtenido de los incidentes de seguridad de la información.	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se deb usar para reducir la posibilidad o el impacto de	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información la Entidad debe gestionar adecuadamente los incidentes de seguridad de la información, por tanto se debe contar con este control implementado.

		incidentes futuros.						
A16.1.7.	Recolección de evidencia.	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de seguridad de la información la Entidad debe gestionar adecuadamente los incidentes de seguridad de la información, por tanto se debe contar con este control implementado.
A17.	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE		4					
A17.1.	Continuidad de seguridad de la informacion: La continuidad de		3					

A17.1.1.	Planificación de la continuidad de la seguridad de la información.	La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de la información se debe planear la continuidad de la seguridad de la información en situaciones adversas, por tanto se debe contar con este control implementado.

A17.1.2.	Implementación de la continuidad de la seguridad de la información.	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de la información se debe planear la continuidad de la seguridad de la información en situaciones adversas, por tanto se debe contar con este control implementado.
A17.1.3.	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de la información se debe verificar, revisar y evaluar la continuidad de la seguridad de la información en situaciones adversas, por tanto se debe contar con este control implementado.
A17.2.	Redundancias: Asegurar la disponibilidad de instalaciones de		1					
A17.2.1.	Disponibilidad de instalaciones de procesamiento de información.	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Como principio de la información se debe contar con redundancias en las instalaciones de procesamiento de información para tener disponibilidad de la información, por tanto se debe contar con este control implementado.
A18.	CUMPLIMIENTO		8					
A18.1.	Cumplimiento de requisitos legales y contractuales: Evitar el		5					

A18.1.1.	Identificación de la legislación aplicable y de los requisitos contractuales.	Todos los requisitos estaturios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Se debe identificar adecuadamente la legislación aplicable con el SGSI para cumplir con regulación vigente gobierno colombiano, por tanto se debe cumplir con este control implementado
A18.1.2.	Derechos de propiedad intelectual.	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	La Entidad debe promover el cumplimiento a la reglamentación vigente relacionados con propiedad intelectual y el uso de software patentado, por tanto se debe cumplir con este control implementado
A18.1.3.	Protección de registros.	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada de acuerdo con los requisitos legislativos, de reglamentación contractuales	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	La Entidad debe proteger adecuadamente los registros que se generen durante su gestión, por tanto se debe cumplir con este control implementado
A18.1.4.	Privacidad y Protección de información de datos personales.	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	La Entidad debe promover el cumplimiento a la reglamentación vigente relacionados con privacidad y protección de datos

		reglamentación pertinentes, cuando sea aplicable.						personales, por tanto se debe cumplir con este control implementado
A18.1.5.	Reglamentación de controles criptográficos.	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Dando cumplimiento a la reglamentación vigente en cuanto al uso de controles criptograficos, la Entidad implementa los controles adecuados pasra esta labor
A18.2.	Revisiones de seguridad de la información: Asegurar que la		3					
A18.2.1.	Revisión independiente de la seguridad de la información.	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Se incluye como parte integral de los requisitos del estándar para el SGSI en la entidad. Tiene asociado el numeral 9 de la norma de la referencia.
A18.2.2.	Cumplimiento con las políticas y normas de seguridad.	Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI. Decreto 2573 de 2014	SI	SI	NO	Por disposición del Gobierno Nacional, la seguridad de la información debe estar presente en los procesos de la Entidades del Estado.

		seguridad apropiadas, y						
A18.2.3.	Revisión del cumplimiento técnico	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	1	Control mediante Política Implementada. Ver: Manual de Políticas del SGSI.	SI	SI	NO	Para preservar la seguridad en los sistemas de información, se hacen análisis de vulnerabilidades a los mismos, de igual manera se revisa que se están dando cumplimiento a las políticas de seguridad

RESPONSABLE DE DOCUMENTO

Comité del Sistema de Gestion de Seguridad de la Información.

NOTIFÍQUESE, COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Firmado en Original

GILBERTO TORO GIRALDO
Director Ejecutivo

Elaboro: Profesional Oficial de Seguridad de la Información.
Revisó: Comité SGSI - FCM
Aprobó: Presidente Comité SGSI - FCM

Ahora teniendo en cuenta que se estableció el alcance del SGSI en la entidad, se procede el análisis y evaluación de riesgos de loa activos de información:

Levantamiento de Información:

Durante este proceso de levantamiento de información, se identifican un total de ciento un (101) activos de información, asociados a cinco (05) procesos que son:

- ✓ Area de TICs
- ✓ Dir. Administrativa y Financiera
- ✓ Jurídica
- ✓ Operaciones no Concesionadas
- ✓ Proyectos - PMO

Lo anterior se encuentra debidamente relacionado en la hoja de cálculo “Activos y Valoración Cualitativa” del libro de Excel® anexo al final del presente documento.

Una vez identificados los activos de información y sus procesos asociados, se establecen responsables para cada proceso.

Análisis de Riesgos

Para esta actividad, se desarrolla una matriz de inventario, en dicha matriz se establecen de manera cuantitativa, los parámetros que permiten medir la probabilidad, impacto que pueden tener los diferentes riesgos identificados, sobre cada uno de los activos de información, esto da como resultado la valoración del riesgo, a continuación, en la tabla No. 13, se observa cómo se realiza la valoración del riesgo, teniendo en cuenta la probabilidad y el impacto.

Tabla 13: Metodología para la valoración del riesgo

METODOLOGÍA PARA LA VALORACIÓN DEL RIESGO EN LOS ACTIVOS DE INFORMACIÓN MAGERIT

PROBABILIDAD DEL RIESGO

	Nomenclatura	Categoría	Valoración
Probabilidad	MA	Prácticamente seguro	5
	A	Probable	4
	M	Posible	3
	B	Poco probable	2
	MB	muy raro	1

IMPACTO DEL RIESGO

	Nomenclatura	Categoría	Valoración
Impacto	MA	Muy Alto	5
	A	Alto	4
	M	Medio	3
	B	Bajo	2
	MB	Muy Bajo	1

VALORACIÓN DEL RIESGO

IMPACTO						
	MA	5	10	15	20	25
	A	4	8	12	16	20
	M	3	6	9	12	15
	B	2	4	6	8	10
	MB	1	2	3	4	5
	RIESGO	MB	B	M	A	MA
		PROBABILIDAD				

Fuente: el autor

Una vez, definida la escala de valoración de riesgos, se establece el rango de valores para la calificación cualitativa de los riesgos, teniendo en cuenta las categorías propias de la metodología *MAGERIT*, como son:

- ✓ Critico
- ✓ Importante
- ✓ Apreciable
- ✓ Bajo
- ✓ Despreciable

Esto se observa con mayor claridad, a continuación, en la siguiente tabla:

Tabla 14: Valoración del riesgo

VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente: el autor

Identificación y Valoración de Activos

Una vez se ha establecido la metodología de riesgos, se requiere identificar los activos que la organización tiene, esto se ha realizado basado en los siguientes criterios:

1. Dato
2. Aplicación
3. Personal
4. Instalaciones
5. Servicios
6. Tecnología

Con el objetivo de identificar las amenazas para cada uno de estos, se realiza un análisis subjetivo que permita identificar el nivel de riesgos de acuerdo a los siguientes dominios:

1. **Autenticidad**, Es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
2. **Trazabilidad**, Se encarga de asegurar que en todo momento se podrá determinar quién hizo qué y en qué momento.
3. **Confidencialidad**, Garantiza que la información llegue solamente a las personas autorizadas
4. **Integridad**, Mantiene la trazabilidad de las características y contenido de la información.
5. **Disponibilidad**, Confirma la disposición de los servicios a ser usados cuando sea necesario.

Cada uno de los anteriores son valorados para cada uno de los activos encontrados en la organización, a continuación se listan los activos analizados.

Tabla 15. Activos analizados

ID	Nombre del activo de información	Tipo de Activo	ID	Nombre del activo de información	Tipo de Activo	ID	Nombre del activo de información	Tipo de Activo
1	Banco de Proyectos (Proyectos)	Dato	35	Carpeta Corrrespondencia DAF	Dato	69	Solicitud de contrataciòn laboral	Dato
2	Modulo Proyectos SAP	Aplicación	36	Carpeta daf tesorería	Dato	70	Tesorería.	Dato
3	Política pública.	Aplicación	37	Carpeta DIR	Dato	71	Backups base de datos simit.	Servicios
4	Portafolio de sevicios SIMIT	Dato	38	Carpeta Presupuesto	Dato	72	Base de datos de desarrollo.	Dato
5	Actas de Seguimiento a la gestón procesal	Dato	39	Carpetas de Gestión documental	Dato	73	Base de datos de pruebas.	Dato
6	Comodato	Dato	40	Certificaciones permanencia de alcaldes	Dato	74	Base de datos producción.	Dato
7	Consultas y conceptos	Dato	41	Certificaciones.	Dato	75	Bodega de Datos	Dato
8	Contratos Interadministrativo	Dato	42	Chip (consolidado de información de la contaduría general de la nación)	Dato	76	Canal de comunicaciones.	Servicios
9	Procesos Contractuales	Dato	43	Control de Ingreso al edificio de alcaldes y funcionarios públicos (SUPERACCES)	Dato	77	Datacenter.	Instalaciones

10	Procesos Judiciales	Dato	44	Cronograma de vencimientos fiscales.	Dato	78	Firewall.	Instalaciones
11	Seguimiento a Polizas	Dato	45	Cuentas por pagar Proveedores.	Dato	79	Portales Empresariales	Tecnología
12	Solicitud de Pedido y Contrato marco Dígital	Dato	46	Derechos de petición.	Dato	80	Servidores store wise.	Servicios
13	Tutelas	Dato	47	Documentos de soporte de contratos de Interventoría a concesiones	Dato	81	Switch core.	Instalaciones
14	Bases de datos logística y proveedores.	Dato	48	Documentos de Nomina	Dato	82	UPS.	Instalaciones
15	Capitulo de Autoridades de Tránsito	Dato	49	Estados financieros.	Dato	83	VPN site to site.	Servicios
16	Carpeta de servicios simit.	Dato	50	Estudios previos contractuales Y Fichas Técnicas.	Dato	84	Actualizaciones SDF	Personal
17	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	Aplicación	51	Facturación Clientes.	Dato	85	Aplicativo SIMIT	Servicios
18	Contratos de Interventoría (Documentos de soporte de contratos de Interventoría a concesiones)	Dato	52	Firma digital certicámara	Dato	86	Archivo de planes de acción (últimos 5 años)	Dato
19	Directorio de Autoridades de Tránsito	Aplicación	53	Firma digital Dian	Dato	87	Archivos de Recaudo Externo	Personal
20	Fondos de Cobertura	Dato	54	Firma Escaneadas Directores	Dato	88	Bases de datos (sistema de distribución de transferencias)	Dato
21	Logística de eventos (FCM - SIMIT).	Personal	55	Gastos de personal	Dato	89	Bitacora de Casos SIMIT	Dato
22	Manuales de operación no concesionada.	Dato	56	Historia Laboral	Dato	90	Conciliaciones.	Dato
23	Pagos especiales.	Dato	57	Informes a Dian	Dato	91	Consecionarios Públicos Entidades Privadas que operan	Dato
24	Seguimiento a PQRS	Tecnología	58	Informes contraloría.	Dato	92	Consolidados de transferencias.	Dato

25	Seguimiento Techo Concesionados (Seguimiento de Ingreso a Concesionados)	Dato	59	Informes de Alcaldías	Dato	93	Distribucio Recaudo local	Dato
26	Soporte a Capacitación	Aplicación	60	Inventario y movimientos de Almacén	Dato	94	Estadísticas contraloría	Dato
27	Soportes de pago (transferencias).	Aplicación	61	Listas de asistencia de los procesos relacionados a gestión humana (induccìon, socializaciones, actividades, capacitaciones) FÍSICOS	Dato	95	Procedimientos Y Consultas PL/SQL	Aplicación
28	Archivos Contabilidad SDF	Dato	62	Mesa de ayuda.	Personal	96	Recaudo Local Información Base de Datos	Dato
29	Archivos Información Contratos Gremiales	Dato	63	Planes de acción.	Dato	97	Reportes y Estadisticas SIMIT	Dato
30	Bancos -Token.	Tecnología	64	Reportes Dane	Dato	98	Servicios de Impresión	Servicios
31	Base de datos alcaldes	Dato	65	Secretaria de hacienda distrital.	Dato	99	Software de deuda.	Dato
32	Base de datos de los colaboradores	Dato	66	Seguimiento de Contratos Gremial	Dato	100	Software de Distribucion Financiera (SDF).	Dato y Aplicación
33	Base de Datos Municipios Colombianos	Dato	67	SIGECCOM	Dato	101	Software gestor de tránsito (Reporte data nueva)	Dato
34	Borrador de resoluciones relacionadas a la planta de personal y cambios de estructura	Dato	68	Sistema de información SAP	Aplicación			

Se realiza la entrevista a los implicados de cada proceso:

Tabla 16. Entrevista Implicados de los Procesos

1	Nombre Entrevistado 1:	Ronald Cely	Cargo	Project Manager	Proceso	Proyectos - PMO
2	Nombre Entrevistado 2:	Martha Sanchez	Cargo	Jefe de Asuntos Juridicos	Proceso	Juridico
3	Nombre Entrevistado 3:	Luz Dary Serna	Cargo	Jefe de Operaciones no Concesionadas	Proceso	Operaciones no Concesionadas
4	Nombre Entrevistado 4:	Dinorha Patricia Abadia	Cargo	Director Adminitrativo y Financiero	Proceso	Administrativo y Financiero
5	Nombre Entrevistado 5:	Alejandro Murillo	Cargo	Dir. De tecnologías de la Información y comunicaciones	Proceso	TICs

Se realiza la evaluación de riesgos de los activos de información frente a cada proceso y dominios de seguridad de la información:

Tabla 17. Evaluacion de Riesgos de los Activos

INFORMACIÓN DE LOS ACTIVOS								
No.	**DATOS DEL ACTIVO DE INFORMACION**			**DOMINIOS**				
	Nombre del activo de información	**Proceso propietario del activo**	**Responsable**	**Dominio Autenticidad(B / M /A**	**Dominio Trazabilidad (B / M /A / MA/ MB)**	**Dominio Confidencilidad**	**Dominio Integridad (B / M /A / MA/ MB)**	**Dominio Disponibilidad**
1	Banco de Proyectos (Proyectos)	Proyectos	Ronald Cely	M	MA	M	A	MA
2	Modulo Proyectos SAP	Proyectos	Ronald Cely	MA	MA	MA	MA	MA

3	Política pública.	Proyectos	Ronald Cely	B	A	B	A	A
4	Portafolio de sevicios SIMIT	Proyectos	Ronald Cely	M	M	M	M	M
5	Actas de Seguimiento a la gestón procesal	Juridica	Martha Sanchez	MA	M	MA	MA	M
6	Comodato	Juridica	Martha Sanchez	B	M	B	A	M
7	Consultas y conceptos	Juridica	Martha Sanchez	B	M	B	A	M
8	Contratos Interadministrativo	Juridica	Martha Sanchez	B	M	B	A	M
9	Procesos Contractuales	Juridica	Martha Sanchez	B	M	B	A	M
10	Procesos Judiciales	Juridica	Martha Sanchez	B	M	B	A	M
11	Seguimiento a Polizas	Juridica	Martha Sanchez	B	M	B	A	M
12	Solicitud de Pedido y Contrato marco Dígital	Juridica	Martha Sanchez	B	M	B	A	M
13	Tutelas	Juridica	Martha Sanchez	B	A	B	M	A
14	Bases de datos logística y proveedores.	Operaciones no Concesionadas	Luz Dary Serna	M	M	M	M	M
15	Capitulo de Autoridades de Tránsito	Operaciones no Concesionadas	Luz Dary Serna	M	M	M	M	M
16	Carpeta de servicios simit.	Operaciones no Concesionadas	Luz Dary Serna	A	MA	A	A	MA
17	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	Operaciones no Concesionadas	Luz Dary Serna	A	A	A	A	A

18	Contratos de Interventoría (Documentos de soporte de contratos de Interventoría a concesiones)	Operaciones no Concesionadas	Luz Dary Serna	B	B	B	B	B
19	Directorio de Autoridades de Tránsito	Operaciones no Concesionadas	Luz Dary Serna	A	A	A	A	A
20	Fondos de Cobertura	Operaciones no Concesionadas	Luz Dary Serna	A	A	A	MA	A
21	Logística de eventos (FCM - SIMIT).	Operaciones no Concesionadas	Luz Dary Serna	M	M	M	M	M
22	Manuales de operación no concesionada.	Operaciones no Concesionadas	Luz Dary Serna	M	A	M	A	A
23	Pagos especiales.	Operaciones no Concesionadas	Luz Dary Serna	A	MA	A	MA	MA
24	Seguimiento a PQRS	Operaciones no Concesionadas	Luz Dary Serna	B	A	B	M	A
25	Seguimiento Techo Concesionados (Seguimiento de Ingreso a Concesionados)	Operaciones no Concesionadas	Luz Dary Serna	A	A	A	A	A
26	Soporte a Capacitación	Operaciones no Concesionadas	Luz Dary Serna	B	A	B	A	A
27	Soportes de pago (transferencias).	Operaciones no Concesionadas	Luz Dary Serna	M	A	M	MA	A

28	Archivos Contabilidad SDF	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	MA	MA	MA	M	MA
29	Archivos Información Contratos Gremiales	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	MA	MA	MA	M	MA
30	Bancos -Token.	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	MA	MA	MA	MA	MA
31	Base de datos alcaldes	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	MA	MA	MA	M	MA
32	Base de datos de los colaboradores	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	MA	MA	MA	MA	MA
33	Base de Datos Municipios Colombianos	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	A	MA	A	MA	MA
34	Borrador de resoluciones relacionadas a la planta de personal y cambios de estructura	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	A	A	A	A	A
35	Carpeta Corrrespondencia DAF	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	A	A	A	A	A
36	Carpeta daf tesorería	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	M	M	M	M	M
37	Carpeta DIR	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	M	M	M	M	M
38	Carpeta Presupuesto	Dir. Administrativ	Dinorha Patricia Abadia	B	A	B	A	A

		a y Financiera						
39	Carpetas de Gestión documental	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	B	A	B	A	A
40	Certificaciones permanencia de alcaldes	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	M	A	M	M	A
41	Certificaciones.	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	B	A	B	B	A
42	Chip (consolidado de información de la contaduría general de la nación)	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	M	M	M	A	M
43	Control de Ingreso al edificio de alcaldes y funcionarios públicos (SUPERACCES)	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	M	A	M	A	A
44	Cronograma de vencimientos fiscales.	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	B	A	B	B	A
45	Cuentas por pagar Proveedores.	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	B	A	B	A	A
46	Derechos de petición.	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	B	M	B	M	M
47	Documentos de soporte de contratos de Interventoría a concesiones	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	M	M	M	M	M
48	Documentos de Nomina	Dir. Administrativ	Dinorha Patricia Abadia	M	M	M	A	M

		a y Financiera						
49	Estados financieros.	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	A	A	A	A	A
50	Estudios previos contractuales Y Fichas Técnicas.	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	M	A	M	MA	A
51	Facturación Clientes.	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	M	M	M	A	M
52	Firma digital certicámara	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	MA	MA	MA	MA	MA
53	Firma digital Dian	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	MA	MA	MA	MA	MA
54	Firma Escaneadas Directores	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	MA	MA	MA	MA	MA
55	Gastos de personal	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	B	A	B	A	A
56	Historia Laboral	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	B	M	B	B	M
57	Informes a Dian	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	M	A	M	A	A
58	Informes contraloría.	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	M	A	M	M	A
59	Informes de Alcaldías	Dir. Administrativ	Dinorha Patricia Abadia	B	A	B	A	A

		a y Financiera						
60	Inventario y movimientos de Almacén	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	A	A	A	A	A
61	Listas de asistencia de los procesos relacionados a gestión humana (induccìon, socializaciones, actividades, capacitaciones) FÍSICOS	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	M	B	M	A	B
62	Mesa de ayuda.	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	B	MA	B	A	MA
63	Planes de acción.	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	M	M	M	M	M
64	Reportes Dane	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	A	A	A	A	A
65	Secretaria de hacienda distrital.	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	M	M	M	M	M
66	Seguimiento de Contratos Gremial	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	MA	MA	MA	MA	MA
67	SIGECCOM	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	MA	MA	MA	MA	MA
68	Sistema de información SAP	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	MA	MA	MA	MA	MA

69	Solicitud de contrataciòn laboral	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	B	A	B	A	A
70	Tesorería.	Dir. Administrativa y Financiera	Dinorha Patricia Abadia	MA	A	MA	MA	A
71	Backups base de datos simit.	Area de Tics	Alejandro M.	MA	MA	MA	MA	MA
72	Base de datos de desarrollo.	Area de Tics	Alejandro M.	MA	MA	MA	A	MA
73	Base de datos de pruebas.	Area de Tics	Alejandro M.	MA	MA	MA	A	MA
74	Base de datos producción.	Area de Tics	Alejandro M.	MA	MA	MA	MA	MA
75	Bodega de Datos	Area de Tics	Alejandro M.	MA	MA	MA	MA	MA
76	Canal de comunicaciones.	Area de Tics	Alejandro M.	MA	MA	MA	MA	MA
77	Datacenter.	Area de Tics	Alejandro M.	MA	MA	MA	MA	MA
78	Firewall.	Area de Tics	Alejandro M.	A	MA	A	A	MA
79	Portales Empresariales	Area de Tics	Alejandro M.	B	MA	B	M	MA
80	Servidores store wise.	Area de Tics	Alejandro M.	A	MA	A	A	MA
81	Switch core.	Area de Tics	Alejandro M.	A	A	A	A	A
82	UPS.	Area de Tics	Alejandro M.	B	A	B	B	A
83	VPN site to site.	Area de Tics	Alejandro M.	MA	MA	MA	MA	MA
84	Actualizaciones SDF	Area de Tics	Alejandro M.	A	A	A	A	A
85	Aplicativo SIMIT	Area de Tics	Alejandro M.	MA	MA	MA	MA	MA
86	Archivo de planes de acción (últimos 5 años)	Area de Tics	Alejandro M.	M	A	M	M	A
87	Archivos de Recaudo Externo	Area de Tics	Alejandro M.	A	A	A	A	A
88	Bases de datos (sistema de distribución de transferencias)	Area de Tics	Alejandro M.	MA	MA	MA	MA	MA
89	Bitacora de Casos SIMIT	Area de Tics	Alejandro M.	A	MA	A	A	MA
90	Conciliaciones.	Area de Tics	Alejandro M.	B	A	B	A	A

91	Consecionarios Públicos Entidades Privadas que operan	Area de Tics	Alejandro M.	MA	MA	MA	MA	MA
92	Consolidados de transferencias.	Area de Tics	Alejandro M.	M	M	M	M	M
93	Distribucio Recaudo local	Area de Tics	Alejandro M.	MA	MA	MA	MA	MA
94	Estadísticas contraloría	Area de Tics	Alejandro M.	B	M	B	M	M
95	Procedimientos Y Consultas PL/SQL	Area de Tics	Alejandro M.	A	MA	A	MA	MA
96	Recaudo Local Información Base de Datos	Area de Tics	Alejandro M.	MA	MA	MA	MA	MA
97	Reportes y Estadisticas SIMIT	Area de Tics	Alejandro M.	A	A	A	A	A
98	Servicios de Impresión	Area de Tics	Alejandro M.	B	M	B	B	M
99	Software de deuda.	Area de Tics	Alejandro M.	MA	MA	MA	MA	MA
100	Software de Distribucion Financiera (SDF).	Area de Tics	Alejandro M.	MA	MA	MA	MA	MA
101	Software gestor de transito (Reporte data nueva)	Area de Tics	Alejandro M.	MA	MA	MA	MA	MA

Evaluacion de los activos frente a atributos de evaluación establecidos y su ubicación:

Tabla 18.Evaluacion de los activos frente a los atributos establecidos.

No.	DATOS DEL ACTIVO DE INFORMACION	ATRIBUTOS								
	Nombre del activo de información	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes ó	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera:		
								Leve	Importante	Grave
1	Banco de Proyectos (Proyectos)				X		X		X	
2	Modulo Proyectos SAP				X		X		X	
3	Política pública.				X		X		X	
4	Portafolio de sevicios SIMIT				X		X		X	
5	Actas de Seguimiento a la gestón procesal			X			X		X	
6	Comodato					X		X		
7	Consultas y conceptos					X		X		
8	Contratos Interadministrativo					X		X		
9	Procesos Contractuales					X		X		
10	Procesos Judiciales					X		X		
11	Seguimiento a Polizas					X		X		
12	Solicitud de Pedido y Contrato marco Dígital					X		X		
13	Tutelas						X		X	
14	Bases de datos logística y proveedores.					X		X		
15	Capitulo de Autoridades de Tránsito		X					X		
16	Carpeta de servicios simit.	X				X	X	X		
17	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)			X	X		X		X	

18	Contratos de Interventoría (Documentos de soporte de contratos de Interventoría a concesiones)		X					X		
19	Directorio de Autoridades de Tránsito						X		X	
20	Fondos de Cobertura				X				X	
21	Logística de eventos (FCM - SIMIT).				X		X	X		
22	Manuales de operación no concesionada.			X		X		X		
23	Pagos especiales.	X			X		X		X	
24	Seguimiento a PQRS						X	X		
25	Seguimiento Techo Concesionados (Seguimiento de Ingreso a Concesionados)						X		X	
26	Soporte a Capacitación			X			X			
27	Soportes de pago (transferencias).				X	X			X	
28	Archivos Contabilidad SDF			X		X			X	
29	Archivos Información Contratos Gremiales			X		X			X	
30	Bancos -Token.				X	X				X
31	Base de datos alcaldes			X		X			X	
32	Base de datos de los colaboradores	X			X	X				X
33	Base de Datos Municipios Colombianos						X		X	
34	Borrador de resoluciones relacionadas a la planta de personal y cambios de estructura						X		X	
35	Carpeta Corrrespondencia DAF						X		X	
36	Carpeta daf tesorería				X				X	
37	Carpeta DIR				X	X			X	
38	Carpeta Presupuesto				X	X			X	

39	Carpetas de Gestión documental				X				X	
40	Certificaciones permanencia de alcaldes					X		X		
41	Certificaciones.						X	X		
42	Chip (consolidado de información de la contaduría general de la nación)						X	X		
43	Control de Ingreso al edificio de alcaldes y funcionarios públicos (SUPERACCES)	X			X	X	X		X	
44	Cronograma de vencimientos fiscales.					X		X		
45	Cuentas por pagar Proveedores.				X				X	
46	Derechos de petición.				X			X		
47	Documentos de soporte de contratos de Interventoría a concesiones				X				X	
48	Documentos de Nomina				X	X			X	
49	Estados financieros.				X	X			X	
50	Estudios previos contractuales Y Fichas Técnicas.				X				X	
51	Facturación Clientes.		X		X	X			X	
52	Firma digital certicámara			X	X	X				X
53	Firma digital Dian			X	X	X				X
54	Firma Escaneadas Directores			X	X	X				X
55	Gastos de personal				X				X	
56	Historia Laboral					X		X		
57	Informes a Dian						X		X	
58	Informes contraloría.		X					X		
59	Informes de Alcaldías					X	X		X	
60	Inventario y movimientos de Almacén				X	X			X	

61	Listas de asistencia de los procesos relacionados a gestión humana (induccìòn, socializaciones, actividades, capacitaciones) FÍSICOS				X				X	
62	Mesa de ayuda.					X			X	
63	Planes de acción.					X			X	
64	Reportes Dane						X		X	
65	Secretaria de hacienda distrital.						X	X		
66	Seguimiento de Contratos Gremial				X				X	
67	SIGECCOM				X				X	
68	Sistema de información SAP	X			X	X				X
69	Solicitud de contrataciòn laboral				X				X	
70	Tesorería.				X	X			X	
71	Backups base de datos simit.	X	X	X		X	X			X
72	Base de datos de desarrollo.	X	X	X		X			X	
73	Base de datos de pruebas.	X	X	X		X			X	
74	Base de datos producción.	X	X	X		X	X			X
75	Bodega de Datos	X	X		X	X	X			X
76	Canal de comunicaciones.					X	X			X
77	Datacenter.	X		X			X			X
78	Firewall.	X				X				X
79	Portales Empresariales						X			X
80	Servidores store wise.	X		X		X			X	
81	Switch core.	X		X		X			X	
82	UPS.					X			X	
83	VPN site to site.	X					X		X	
84	Actualizaciones SDF					X		X		
85	Aplicativo SIMIT	X	X		X	X	X			X
86	Archivo de planes de acción (últimos 5 años)			X		X		X		

87	Archivos de Recaudo Externo					X		X		
88	Bases de datos (sistema de distribución de transferencias)	X				X				X
89	Bitacora de Casos SIMIT	X		X		X	X		X	
90	Conciliaciones.						X	X		
91	Consecionarios Públicos Entidades Privadas que operan		X			X				X
92	Consolidados de transferencias.			X					X	
93	Distribucio Recaudo local		X			X				X
94	Estadísticas contraloría						X		X	
95	Procedimientos Y Consultas PL/SQL	X				X	X		X	
96	Recaudo Local Información Base de Datos		X			X				X
97	Reportes y Estadisticas SIMIT					X	X		X	
98	Servicios de Impresión					X		X		
99	Software de deuda.		X			X				X
100	Software de Distribucion Financiera (SDF).			X	X	X				X
101	Software gestor de transito (Reporte data nueva)		X			X				X

Ubicación de los activos:

Tabla 19. Ubicación de los activos.

No.	DATOS DEL ACTIVO DE INFORMACION	UBICACIÓN	
	Nombre del activo de información	**Físico**	**Electrónico**
1	Banco de Proyectos (Proyectos)	A-Z	Servidor
2	Modulo Proyectos SAP	Servidor	Servidor
3	Política pública.	A-Z	Servidor
4	Portafolio de sevicios SIMIT	A-Z	Servidor
5	Actas de Seguimiento a la gestón procesal	A-Z	Servidor
6	Comodato	A-Z	Servidor
7	Consultas y conceptos	A-Z	Servidor
8	Contratos Interadministrativo	A-Z	Servidor
9	Procesos Contractuales	A-Z	Servidor
10	Procesos Judiciales	A-Z	Servidor
11	Seguimiento a Polizas	A-Z	Servidor
12	Solicitud de Pedido y Contrato marco Dígital	A-Z	Servidor
13	Tutelas	A-Z	Computdor
14	Bases de datos logística y proveedores.	Servidor	Servidor
15	Capitulo de Autoridades de Tránsito	A-Z	Servidor
16	Carpeta de servicios simit.	Servidor	Servidor
17	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	Servidor	Servidor

18	Contratos de Interventoría (Documentos de soporte de contratos de Interventoría a concesiones)	A-Z	Servidor
19	Directorio de Autoridades de Tránsito	Servidor	Servidor
20	Fondos de Cobertura	Servidor	Servidor
21	Logística de eventos (FCM - SIMIT).	A-Z	Servidor
22	Manuales de operación no concesionada.	A-Z	Servidor
23	Pagos especiales.	A-Z	Servidor
24	Seguimiento a PQRS	A-Z	Servidor
25	Seguimiento Techo Concesionados (Seguimiento de Ingreso a Concesionados)	A-Z	Servidor
26	Soporte a Capacitación	Servidor	Servidor
27	Soportes de pago (transferencias).	A-Z	Servidor
28	Archivos Contabilidad SDF	Servidor	Servidor
29	Archivos Información Contratos Gremiales	Servidor	Servidor
30	Bancos -Token.	Dispositivo	Dispositivo
31	Base de datos alcaldes	Servidor	Servidor
32	Base de datos de los colaboradores	Servidor	Servidor
33	Base de Datos Municipios Colombianos	Servidor	Servidor
34	Borrador de resoluciones relacionadas a la planta de personal y cambios de estructura	Servidor	Sevidor
35	Carpeta Corrrespondencia DAF	Servidor	Sevidor
36	Carpeta daf tesorería	Servidor	Sevidor
37	Carpeta DIR	Servidor	Sevidor
38	Carpeta Presupuesto	Servidor	Sevidor
39	Carpetas de Gestión documental	Servidor	Sevidor

40	Certificaciones permanencia de alcaldes	Servidor	Servidor
41	Certificaciones.	Servidor	Servidor
42	Chip (consolidado de información de la contaduría general de la nación)	Servidor	Servidor
43	Control de Ingreso al edificio de alcaldes y funcionarios públicos (SUPERACCES)	A-Z	Servidor
44	Cronograma de vencimientos fiscales.	Servidor	Servidor
45	Cuentas por pagar Proveedores.	A-Z	Sevidor
46	Derechos de petición.	A-Z	Servidor
47	Documentos de soporte de contratos de Interventoría a concesiones	A-Z	Servidor
48	Documentos de Nomina	Servidor	Servidor
49	Estados financieros.	A-Z	Servidor
50	Estudios previos contractuales Y Fichas Técnicas.	A-Z	Servidor
51	Facturación Clientes.	A-Z	Servidor
52	Firma digital certicámara	Servidor	Servidor
53	Firma digital Dian	Servidor	Sevidor
54	Firma Escaneadas Directores	Servidor	Sevidor
55	Gastos de personal	Servidor	Sevidor
56	Historia Laboral	A-Z	Sevidor
57	Informes a Dian	Servidor	Servidor
58	Informes contraloría.	A-Z	Sevidor
59	Informes de Alcaldías	A-Z	Servidor
60	Inventario y movimientos de Almacén	Servidor	Sevidor

61	Listas de asistencia de los procesos relacionados a gestión humana (induccìon, socializaciones, actividades, capacitaciones) FÍSICOS	Servidor	Sevidor
62	Mesa de ayuda.	Tics	Tics
63	Planes de acción.	Servidor	Servidor
64	Reportes Dane	A-Z	Sevidor
65	Secretaria de hacienda distrital.	Servidor	Servidor
66	Seguimiento de Contratos Gremial	Servidor	Sevidor
67	SIGECCOM	Servidor	Sevidor
68	Sistema de información SAP	Servidor	Servidor
69	Solicitud de contrataciòn laboral	Servidor	Sevidor
70	Tesorería.	Servidor	Servidor
71	Backups base de datos simit.	Servidor	Servidor
72	Base de datos de desarrollo.	Servidor	Servidor
73	Base de datos de pruebas.	Servidor	Servidor
74	Base de datos producción.	Servidor	Servidor
75	Bodega de Datos	Aplicación	Servidor
76	Canal de comunicaciones.	Servidor	Servidor
77	Datacenter.	Servidor	Servidor
78	Firewall.	Servidor	Servidor
79	Portales Empresariales	Aplicación	Servidor
80	Servidores store wise.	Servidor	Servidor
81	Switch core.	Dispositivo	Dispositivo
82	UPS.	Dispositivo	Dispositivo
83	VPN site to site.	Servidor	Servidor
84	Actualizaciones SDF	Personal	Personal
85	Aplicativo SIMIT	Servidor	Servidor
86	Archivo de planes de acción (últimos 5 años)	Servidor	Servidor
87	Archivos de Recaudo Externo	Personal	Personal

88	Bases de datos (sistema de distribución de transferencias)	Servidor	Servidor
89	Bitacora de Casos SIMIT	Servidor	Servidor
90	Conciliaciones.	A-Z	Servidor
91	Consecionarios Públicos Entidades Privadas que operan	Servidor	Servidor
92	Consolidados de transferencias.	Servidor	Servidor
93	Distribucio Recaudo local	Servidor	Servidor
94	Estadísticas contraloría	A-Z	Servidor
95	Procedimientos Y Consultas PL/SQL	Aplicación	Servidor
96	Recaudo Local Información Base de Datos	Servidor	Servidor
97	Reportes y Estadisticas SIMIT	A-Z	Servidor
98	Servicios de Impresión	Dispositivo	Dispositivo
99	Software de deuda.	Servidor	Servidor
100	Software de Distribucion Financiera (SDF).	Servidor	Servidor
101	Software gestor de transito (Reporte data nueva)	Servidor	Servidor

Valoracion cuantitativa de la evaluación de riesgos de los activos:

Tabla 20. Valoracion Cuantitativa de evaluación los activos.

Nombre	Riesgo	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
Banco de Proyectos (Proyectos)	IMPORTANTE	15	25	15	20	25	20
Modulo Proyectos SAP	CRITICO	25	25	25	25	25	25
Política pública.	IMPORTANTE	9	20	9	20	20	16
Portafolio de sevicios SIMIT	APRECIABLE	15	15	15	15	15	15
Actas de Seguimiento a la gestón procesal	CRITICO	25	15	25	25	15	21
Comodato	APRECIABLE	9	15	9	20	15	14
Consultas y conceptos	APRECIABLE	9	15	9	20	15	14
Contratos Interadministrativo	APRECIABLE	9	15	9	20	15	14
Procesos Contractuales	APRECIABLE	9	15	9	20	15	14
Procesos Judiciales	APRECIABLE	9	15	9	20	15	14
Seguimiento a Polizas	APRECIABLE	9	15	9	20	15	14
Solicitud de Pedido y Contrato marco Dígital	APRECIABLE	9	15	9	20	15	14
Tutelas	APRECIABLE	9	20	9	15	20	15
Bases de datos logística y proveedores.	APRECIABLE	15	15	15	15	15	15
Capitulo de Autoridades de Tránsito	APRECIABLE	15	15	15	15	15	15
Carpeta de servicios simit.	CRITICO	20	25	20	20	25	22
Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	IMPORTANTE	20	20	20	20	20	20
Contratos de Interventoría (Documentos de soporte de contratos de Interventoría a concesiones)	BAJO	9	9	9	9	9	9
Directorio de Autoridades de Tránsito	IMPORTANTE	20	20	20	20	20	20
Fondos de Cobertura	CRITICO	20	20	20	25	20	21
Logística de eventos (FCM - SIMIT).	APRECIABLE	15	15	15	15	15	15
Manuales de operación no concesionada.	IMPORTANTE	15	20	15	20	20	18
Pagos especiales.	CRITICO	20	25	20	25	25	23
Seguimiento a PQRS	APRECIABLE	9	20	9	15	20	15
Seguimiento Techo Concesionados	IMPORTANTE	20	20	20	20	20	20

(Seguimiento de Ingreso a Concesionados)							
Soporte a Capacitación	IMPORTANTE	9	20	9	20	20	16
Soportes de pago (transferencias).	IMPORTANTE	15	20	15	25	20	19
Archivos Contabilidad SDF	CRITICO	25	25	25	15	25	23
Archivos Información Contratos Gremiales	CRITICO	25	25	25	15	25	23
Bancos -Token.	CRITICO	25	25	25	25	25	25
Base de datos alcaldes	CRITICO	25	25	25	15	25	23
Base de datos de los colaboradores	CRITICO	25	25	25	25	25	25
Base de Datos Municipios Colombianos	CRITICO	20	25	20	25	25	23
Borrador de resoluciones relacionadas a la planta de personal y cambios de estructura	IMPORTANTE	20	20	20	20	20	20
Carpeta Corrrespondencia DAF	IMPORTANTE	20	20	20	20	20	20
Carpeta daf tesorería	APRECIABLE	15	15	15	15	15	15
Carpeta DIR	APRECIABLE	15	15	15	15	15	15
Carpeta Presupuesto	IMPORTANTE	9	20	9	20	20	16
Carpetas de Gestión documental	IMPORTANTE	9	20	9	20	20	16
Certificaciones permanencia de alcaldes	IMPORTANTE	15	20	15	15	20	17
Certificaciones.	APRECIABLE	9	20	9	9	20	13
Chip (consolidado de información de la contaduría general de la nación)	IMPORTANTE	15	15	15	20	15	16
Control de Ingreso al edificio de alcaldes y funcionarios públicos (SUPERACCES)	IMPORTANTE	15	20	15	20	20	18
Cronograma de vencimientos fiscales.	APRECIABLE	9	20	9	9	20	13
Cuentas por pagar Proveedores.	IMPORTANTE	9	20	9	20	20	16
Derechos de petición.	APRECIABLE	9	15	9	15	15	13
Documentos de soporte de contratos de Interventoría a concesiones	APRECIABLE	15	15	15	15	15	15
Documentos de Nomina	IMPORTANTE	15	15	15	20	15	16
Estados financieros.	IMPORTANTE	20	20	20	20	20	20
Estudios previos contractuales Y Fichas Técnicas.	IMPORTANTE	15	20	15	25	20	19
Facturación Clientes.	IMPORTANTE	15	15	15	20	15	16
Firma digital certicámara	CRITICO	25	25	25	25	25	25
Firma digital Dian	CRITICO	25	25	25	25	25	25

Firma Escaneadas Directores	CRITICO	25	25	25	25	25	25
Gastos de personal	IMPORTANTE	9	20	9	20	20	16
Historia Laboral	APRECIABLE	9	15	9	9	15	11
Informes a Dian	IMPORTANTE	15	20	15	20	20	18
Informes contraloría.	IMPORTANTE	15	20	15	15	20	17
Informes de Alcaldías	IMPORTANTE	9	20	9	20	20	16
Inventario y movimientos de Almacén	IMPORTANTE	20	20	20	20	20	20
Listas de asistencia de los procesos relacionados a gestión humana (inducciòn, socializaciones, actividades, capacitaciones) FÍSICOS	APRECIABLE	15	9	15	20	9	14
Mesa de ayuda.	IMPORTANTE	9	25	9	20	25	18
Planes de acción.	APRECIABLE	15	15	15	15	15	15
Reportes Dane	IMPORTANTE	20	20	20	20	20	20
Secretaria de hacienda distrital.	APRECIABLE	15	15	15	15	15	15
Seguimiento de Contratos Gremial	CRITICO	25	25	25	25	25	25
SIGECCOM	CRITICO	25	25	25	25	25	25
Sistema de información SAP	CRITICO	25	25	25	25	25	25
Solicitud de contrataciòn laboral	IMPORTANTE	9	20	9	20	20	16
Tesorería.	CRITICO	25	20	25	25	20	23
Backups base de datos simit.	CRITICO	25	25	25	25	25	25
Base de datos de desarrollo.	CRITICO	25	25	25	20	25	24
Base de datos de pruebas.	CRITICO	25	25	25	20	25	24
Base de datos producción.	CRITICO	25	25	25	25	25	25
Bodega de Datos	CRITICO	25	25	25	25	25	25
Canal de comunicaciones.	CRITICO	25	25	25	25	25	25
Datacenter.	CRITICO	25	25	25	25	25	25
Firewall.	CRITICO	20	25	20	20	25	22
Portales Empresariales	IMPORTANTE	9	25	9	15	25	17
Servidores store wise.	CRITICO	20	25	20	20	25	22
Switch core.	IMPORTANTE	20	20	20	20	20	20
UPS.	APRECIABLE	9	20	9	9	20	13
VPN site to site.	CRITICO	25	25	25	25	25	25
Actualizaciones SDF	IMPORTANTE	20	20	20	20	20	20
Aplicativo SIMIT	CRITICO	25	25	25	25	25	25
Archivo de planes de acción (últimos 5 años)	IMPORTANTE	15	20	15	15	20	17

Archivos de Recaudo Externo	IMPORTANTE	20	20	20	20	20	20
Bases de datos (sistema de distribución de transferencias)	CRITICO	25	25	25	25	25	25
Bitacora de Casos SIMIT	CRITICO	20	25	20	20	25	22
Conciliaciones.	IMPORTANTE	9	20	9	20	20	16
Consecionarios Públicos Entidades Privadas que operan	CRITICO	25	25	25	25	25	25
Consolidados de transferencias.	APRECIABLE	15	15	15	15	15	15
Distribucio Recaudo local	CRITICO	25	25	25	25	25	25
Estadísticas contraloría	APRECIABLE	9	15	9	15	15	13
Procedimientos Y Consultas PL/SQL	CRITICO	20	25	20	25	25	23
Recaudo Local Información Base de Datos	CRITICO	25	25	25	25	25	25
Reportes y Estadisticas SIMIT	IMPORTANTE	20	20	20	20	20	20
Servicios de Impresión	APRECIABLE	9	15	9	9	15	11
Software de deuda.	CRITICO	25	25	25	25	25	25
Software de Distribucion Financiera (SDF).	CRITICO	25	25	25	25	25	25
Software gestor de transito (Reporte data nueva)	CRITICO	25	25	25	25	25	25

Posterior al haber realizado en analisis y evaluación de riesgos de los activos de información y conforme a sus resultados, determinaremos las amenazas y vulnerabilides y de aquí se genera el plan de tratatamiendo de riesgos junto con los controles sugeridos por la norma ISO 27001:2013.

Tabla 21. Determinacion de Amenazas y Vulnerabilidades.

No. De Amenazas y Vulnerabilidades	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades
1	Tutelas	15	[A.11] Acceso no autorizado	Acceso no autorizado a la informacion.
2	Tutelas	15	[A.11] Acceso no autorizado	Debilidad en las contraseñas de la Red
3	Tutelas	15	[A.11] Acceso no autorizado	Falta de auditoría a la actividad de los usuarios en acceso a la informacion.
4	Tutelas	15	[A.11] Acceso no autorizado	Falta de comunicación entre la Dirección Administrativa y Sistemas con respecto a la salida de personal de la Federación
5	Tutelas	15	[A.11] Acceso no autorizado	Falta de controles de acceso lógico
6	Tutelas	15	[A.11] Acceso no autorizado	Préstamo de usuarios y contraseñas

7	Tutelas	15	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
8	Tutelas	15	[E.15] Alteración de la información	Acceso no autorizado a la informacion.
9	Tutelas	15	[E.15] Alteración de la información	Falta de controles de acceso lógico
10	Tutelas	15	[E.15] Alteración de la información	Falta de revisión periódica del archivo de auditoria
11	Tutelas	15	[E.15] Alteración de la información	Segregación inadecuada de funciones
12	Tutelas	15	[E.1] Errores de los usuarios	Falta de documentación
13	Tutelas	15	[E.1] Errores de los usuarios	Segregación inadecuada de funciones
14	Tutelas	15	[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de controles sobre la gestión del cambio
15	Tutelas	15	[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de planes de contingencia o procedimientos de recuperación
16	Tutelas	15	[E.28] Indisponibilidad del personal	Falta de contingencias de respaldo de personal crítico
17	Tutelas	15	[E.28] Indisponibilidad del personal	Falta de documentación

18	Tutelas	15	[A.6] Abuso de privilegios de acceso	Falta de control de licenciamiento
19	Tutelas	15	[A.6] Abuso de privilegios de acceso	Falta de controles de acceso lógico
20	Tutelas	15	[A.6] Abuso de privilegios de acceso	Falta de revisión periódica del archivo de auditoria
21	Tutelas	15	[A.6] Abuso de privilegios de acceso	Préstamo de usuarios y contraseñas
22	Tutelas	15	[A.6] Abuso de privilegios de acceso	Segregación inadecuada de funciones
23	Modulo Proyectos SAP	25	[A.5] Suplantación de la identidad del usuario	Segregación inadecuada de funciones
24	Modulo Proyectos SAP	25	[E.15] Alteración de la información	Falta de controles de acceso lógico
25	Modulo Proyectos SAP	25	[E.15] Alteración de la información	Segregación inadecuada de funciones
26	Modulo Proyectos SAP	25	[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de Acuerdos de Niveles de Servicio con el Proveedor
27	Modulo Proyectos SAP	25	[E.1] Errores de los usuarios	Segregación inadecuada de funciones

28	Modulo Proyectos SAP	25	[E.28] Indisponibilidad del personal	Falta de contingencias de respaldo de personal crítico
29	Archivo de planes de acción (últimos 5 años)	17	[E.15] Alteración de la información	Falta de controles de acceso lógico
30	Archivo de planes de acción (últimos 5 años)	17	[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de planes de contingencia o procedimientos de recuperación
31	Archivo de planes de acción (últimos 5 años)	17	[E.28] Indisponibilidad del personal	Falta de documentación
32	Archivo de planes de acción (últimos 5 años)	17	[A.6] Abuso de privilegios de acceso	Falta de control de licenciamiento
33	Archivo de planes de acción (últimos 5 años)	17	[A.11] Acceso no autorizado	Debilidad en las contraseñas del sistema operativo
34	Archivo de planes de acción (últimos 5 años)	17	[A.11] Acceso no autorizado	Falta de comunicación entre la Direccion Administrativa y sistemas

35	Archivo de planes de acción (últimos 5 años)	17	[A.15] Modificación de información	Copias no restringidas de datos o software
36	Archivo de planes de acción (últimos 5 años)	17	[A.15] Modificación de información	Falta de controles de acceso lógico
37	Archivo de planes de acción (últimos 5 años)	17	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los archivos
38	Archivo de planes de acción (últimos 5 años)	17	[A.15] Modificación de información	Posibilidad de edición de los archivos generados en los sistemas de información
39	Archivo de planes de acción (últimos 5 años)	17	[A.15] Modificación de información	Préstamo de usuarios y contraseñas
40	Archivo de planes de acción (últimos 5 años)	17	[A.4] Manipulación de la configuración	Segregación inadecuada de funciones
41	Archivo de planes de acción (últimos 5 años)	17	[N.*]Desastres naturales	Falta de planes de contingencia o procedimientos de recuperación
42	Archivo de planes de acción (últimos 5 años)	17	[E.18] Destrucción de la información	Falta de controles de almacenamiento y resguardo sobre los archivos

43	Archivo de planes de acción (últimos 5 años)	17	[E.18] Destrucción de la información	Préstamo de usuarios y contraseñas
44	Archivo de planes de acción (últimos 5 años)	17	[E.25] Perdidas de equipos	Falta de controles en el translado de los dispositivos
45	Portafolio de sevicios SIMIT	15	[A.5] Suplantación de la identidad del usuario	Ubicación inadecuada de la estación de trabajo
46	Portafolio de sevicios SIMIT	15	[A.15] Modificación de información	Copias no restringidas de datos o software
47	Portafolio de sevicios SIMIT	15	[A.15] Modificación de información	Falta de controles de acceso lógico
48	Portafolio de sevicios SIMIT	15	[E.18] Destrucción de la información	Copias no restringidas de datos o software
49	Actas de Seguimiento a la gestón procesal	22	[A.5] Suplantación de la identidad del usuario	Debilidad en las contraseñas del sistema
50	Actas de Seguimiento a la gestón procesal	22	[A.5] Suplantación de la identidad del usuario	Préstamo de usuarios y contraseñas

51	Actas de Seguimiento a la gestón procesal	22	[E.1] Errores de los usuarios	Segregación inadecuada de funciones
52	Actas de Seguimiento a la gestón procesal	22	[E.15] Alteración de la información	Acceso no autorizado a utilidades del sistema de información
53	Aplicativo SIMIT	25	[A.5] Suplantación de la identidad del usuario	Falta de auditoría a la actividad sobre el sistema de información
54	Aplicativo SIMIT	25	[A.5] Suplantación de la identidad del usuario	Préstamo de usuarios y contraseñas
55	Aplicativo SIMIT	25	[A.6] Abuso de privilegios de acceso	Falta de auditoría a la actividad sobre el sistema de información
56	Aplicativo SIMIT	25	[E.15] Alteración de la información	Acceso no autorizado a utilidades del sistema de información
57	Aplicativo SIMIT	25	[E.15] Alteración de la información	Segregación inadecuada de funciones
58	Aplicativo SIMIT	25	[E.4] Errores de configuración	Acceso de los desarrolladores a ambientes productivos
59	Aplicativo SIMIT	25	[E.1] Errores de los usuarios	Segregación inadecuada de funciones
60	Aplicativo SIMIT	25	[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de Acuerdos de Niveles de Servicio con el Proveedor

61	Aplicativo SIMIT	25	[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de planes de contingencia o procedimientos de recuperación
62	Servicios de Impresión	11	[E.18] Destrucción de la información	Falta de controles de acceso lógico
63	Estadísticas contraloría	13	[E.15] Alteración de la información	Segregación inadecuada de funciones
64	Procedimientos Y Consultas PL/SQL	23	[A.11] Acceso no autorizado	Debilidad en las contraseñas de la Red
65	Procedimientos Y Consultas PL/SQL	23	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
66	Procedimientos Y Consultas PL/SQL	23	[A.7] Uso no previsto	Acceso no autorizado a la informacion.
67	Procedimientos Y Consultas PL/SQL	23	[E.15] Alteración de la información	Acceso no autorizado a la informacion.
68	Bitacora de Casos SIMIT	22	[E.28] Indisponibilidad del personal	Falta de documentación
69	Bitacora de Casos SIMIT	22	[E.15] Alteración de la información	Acceso no autorizado a la informacion.
70	Bitacora de Casos SIMIT	22	[E.15] Alteración de la información	Falta de revisión periódica del archivo de auditoria

71	Reportes y Estadisticas SIMIT	20	[A.6] Abuso de privilegios de acceso	Falta de controles de acceso lógico
72	Reportes y Estadisticas SIMIT	20	[A.6] Abuso de privilegios de acceso	Segregación inadecuada de funciones
73	Reportes y Estadisticas SIMIT	20	[E.19] Divulgación de la información	Préstamo de usuarios y contraseñas
74	Software gestor de transito (Reporte data nueva)	25	[A.5] Suplantación de la identidad del usuario	Debilidad en las contraseñas del sistema
75	Software gestor de transito (Reporte data nueva)	25	[A.5] Suplantación de la identidad del usuario	Falta de auditoría a la actividad sobre el sistema de información
76	Software gestor de transito (Reporte data nueva)	25	[A.8] Difusión de software dañino	Falta de controles sobre la gestión del cambio
77	Software gestor de transito (Reporte data nueva)	25	[A.6] Abuso de privilegios de acceso	Copias no restringidas de datos o software
78	Software gestor de transito (Reporte data nueva)	25	[A.6] Abuso de privilegios de acceso	Falta de controles de acceso lógico

79	Sistema de información SAP	25	[A.5] Suplantación de la identidad del usuario	Debilidad en las contraseñas del sistema
80	Sistema de información SAP	25	[A.5] Suplantación de la identidad del usuario	Falta de auditoría a la actividad sobre el sistema de información
81	Sistema de información SAP	25	[A.8] Difusión de software dañino	Falta de controles sobre la gestión del cambio
82	Sistema de información SAP	25	[A.6] Abuso de privilegios de acceso	Copias no restringidas de datos o software
83	Sistema de información SAP	25	[A.6] Abuso de privilegios de acceso	Falta de controles de acceso lógico
84	Archivos Contabilidad SDF	22	[A.15] Modificación de información	Clasificación de la información de manera inadecuada (en términos de confidencialidad, integridad y disponibilidad)
85	Archivos Contabilidad SDF	22	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
86	Archivos Contabilidad SDF	22	[A.15] Modificación de información	Segregación inadecuada de funciones
87	Documentos de Nomina	17	[A.15] Modificación de información	Clasificación de la información de manera inadecuada (en términos de confidencialidad, integridad y disponibilidad)
88	Documentos de Nomina	17	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
89	Documentos de Nomina	17	[A.15] Modificación de información	Segregación inadecuada de funciones

90	Archivos Información Contratos Gremiales	22	[A.15] Modificación de información	Clasificación de la información de manera inadecuada (en términos de confidencialidad, integridad y disponibilidad)
91	Archivos Información Contratos Gremiales	22	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
92	Archivos Información Contratos Gremiales	22	[A.4] Manipulación de la configuración	Segregación inadecuada de funciones
93	Archivos Información Contratos Gremiales	22	[E.18] Destrucción de la información	Falta de controles de almacenamiento y resguardo sobre los archivos
94	Base de datos de los colaboradores	25	[A.15] Modificación de información	Clasificación de la información de manera inadecuada (en términos de confidencialidad, integridad y disponibilidad)
95	Base de datos de los colaboradores	25	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
96	Base de datos de los colaboradores	25	[A.4] Manipulación de la configuración	Segregación inadecuada de funciones
97	Base de datos de los colaboradores	25	[E.18] Destrucción de la información	Falta de controles de almacenamiento y resguardo sobre los archivos

98	Historia Laboral	11	[A.15] Modificación de información	Clasificación de la información de manera inadecuada (en términos de confidencialidad, integridad y disponibilidad)
99	Historia Laboral	11	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
100	Historia Laboral	11	[A.4] Manipulación de la configuración	Segregación inadecuada de funciones
101	Historia Laboral	11	[E.18] Destrucción de la información	Falta de controles de almacenamiento y resguardo sobre los archivos
102	Base de Datos Municipios Colombianos	23	[A.5] Suplantación de la identidad del usuario	Acceso lógico no autorizado al sistema
103	Base de Datos Municipios Colombianos	23	[A.5] Suplantación de la identidad del usuario	Falta de controles de acceso lógico
104	Base de Datos Municipios Colombianos	23	[A.5] Suplantación de la identidad del usuario	Segregación inadecuada de funciones
105	Base de Datos Municipios Colombianos	23	[A.6] Abuso de privilegios de acceso	Acceso de los desarrolladores a ambientes productivos
106	Base de Datos Municipios Colombianos	23	[E.15] Alteración de la información	Segregación inadecuada de funciones

107	Base de Datos Municipios Colombianos	23	[E.1] Errores de los usuarios	Segregación inadecuada de funciones
108	Base de Datos Municipios Colombianos	23	[E.28] Indisponibilidad del personal	Falta de conocimiento del soporte de la aplicación
109	Base de datos alcaldes	22	[A.5] Suplantación de la identidad del usuario	Acceso lógico no autorizado al sistema
110	Base de datos alcaldes	22	[A.5] Suplantación de la identidad del usuario	Falta de controles de acceso lógico
111	Base de datos alcaldes	22	[A.5] Suplantación de la identidad del usuario	Segregación inadecuada de funciones
112	Base de datos alcaldes	22	[A.6] Abuso de privilegios de acceso	Acceso de los desarrolladores a ambientes productivos
113	Base de datos alcaldes	22	[E.15] Alteración de la información	Segregación inadecuada de funciones
114	Base de datos alcaldes	22	[E.1] Errores de los usuarios	Segregación inadecuada de funciones
115	Base de datos alcaldes	22	[E.28] Indisponibilidad del personal	Falta de conocimiento del soporte de la aplicación

116	Borrador de resoluciones relacionadas a la planta de personal y cambios de estructura	20	[A] Ataques deliberados	Falta de controles de acceso físico
117	Borrador de resoluciones relacionadas a la planta de personal y cambios de estructura	20	[A.8] Difusión de software dañino	Falta de controles sobre el software descargado de Internet
118	Borrador de resoluciones relacionadas a la planta de personal y cambios de estructura	20	[I.7] Condiciones inadecuadas de temperatura o humedad	Falta de planes de contingencia o procedimientos de recuperación
119	Borrador de resoluciones relacionadas a la planta de personal y cambios de estructura	20	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Mantenimiento inadecuado de la estación de trabajo

120	Borrador de resoluciones relacionadas a la planta de personal y cambios de estructura	20	[E.18] Destrucción de la información	Copias no restringidas de datos o software
121	Certificaciones permanencia de alcaldes	17	[A] Ataques deliberados	Falta de controles de acceso físico
122	Certificaciones permanencia de alcaldes	17	[A.8] Difusión de software dañino	Falta de controles sobre el software descargado de Internet
123	Certificaciones permanencia de alcaldes	17	[I.7] Condiciones inadecuadas de temperatura o humedad	Falta de planes de contingencia o procedimientos de recuperación
124	Certificaciones permanencia de alcaldes	17	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Mantenimiento inadecuado de la estación de trabajo
125	Certificaciones permanencia de alcaldes	17	[E.18] Destrucción de la información	Copias no restringidas de datos o software
126	Facturación Clientes.	17	[A.11] Acceso no autorizado	Acceso no autorizado a la informacion
127	Facturación Clientes.	17	[A.11] Acceso no autorizado	Falta de auditoría a la actividad de los usuarios en acceso a la informacion.

128	Facturación Clientes.	17	[A.11] Acceso no autorizado	Falta de controles de acceso lógico
129	Facturación Clientes.	17	[A.11] Acceso no autorizado	Acceso no autorizado a la informacion.
130	Cuentas por pagar Proveedores.	16	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
131	Cuentas por pagar Proveedores.	16	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
132	Cuentas por pagar Proveedores.	16	[A.15] Modificación de información	Préstamo de usuarios y contraseñas
133	Cuentas por pagar Proveedores.	16	[E.28] Indisponibilidad del personal	Falta de contingencias de respaldo de personal crítico
134	Informes contraloría.	17	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
135	Informes contraloría.	17	[E.18] Destrucción de la información	Falta de controles de acceso físico
136	Carpeta daf tesorería	15	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
137	Carpeta daf tesorería	15	[E.18] Destrucción de la información	Falta de controles de acceso físico
138	Carpeta daf tesorería	15	[A.15] Modificación de información	Falta de controles de acceso físico
139	Carpeta DIR	15	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos

140	Carpeta DIR	15	[E.18] Destrucción de la información	Falta de controles de acceso físico
141	Carpeta DIR	15	[A.15] Modificación de información	Falta de controles de acceso físico
142	Carpeta Presupuesto	16	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
143	Carpeta Presupuesto	16	[E.18] Destrucción de la información	Falta de controles de acceso físico
144	Carpeta Presupuesto	16	[A.15] Modificación de información	Falta de controles de acceso físico
145	Carpeta Corrrespondencia DAF	20	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
146	Carpeta Corrrespondencia DAF	20	[E.18] Destrucción de la información	Falta de controles de acceso físico
147	Carpeta Corrrespondencia DAF	20	[A.15] Modificación de información	Falta de controles de acceso físico
148	Procesos Contractuales	15	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
149	Procesos Contractuales	15	[E.18] Destrucción de la información	Falta de controles de acceso físico
150	Procesos Contractuales	15	[A.15] Modificación de información	Falta de controles de acceso físico
151	Procesos Judiciales	15	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
152	Procesos Judiciales	15	[E.18] Destrucción de la información	Falta de controles de acceso físico

153	Procesos Judiciales	15	[A.15] Modificación de información	Falta de controles de acceso físico
154	Reportes Dane	20	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
155	Reportes Dane	20	[E.18] Destrucción de la información	Falta de controles de acceso físico
156	Reportes Dane	20	[A.15] Modificación de información	Falta de controles de acceso físico
157	Seguimiento a Polizas	15	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
158	Seguimiento a Polizas	15	[E.18] Destrucción de la información	Falta de controles de acceso físico
159	Seguimiento a Polizas	15	[A.15] Modificación de información	Falta de controles de acceso físico
160	Solicitud de Pedido y Contrato marco Dígital	15	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
161	Solicitud de Pedido y Contrato marco Dígital	15	[E.18] Destrucción de la información	Falta de controles de acceso físico
162	Solicitud de Pedido y Contrato marco Dígital	15	[A.15] Modificación de información	Falta de controles de acceso físico
163	Derechos de petición.	13	[A.7] Uso no previsto	Acceso no autorizado a la informacion.

164	Estados financieros.	20	[A.6] Abuso de privilegios de acceso	Copias no restringidas de datos o software
165	Estados financieros.	20	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
166	Estados financieros.	20	[A.7] Uso no previsto	Falta de políticas de manejo de contraseñas críticas
167	Comodato	15	[A.11] Acceso no autorizado	Falta de controles de acceso lógico
168	Comodato	15	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
169	Comodato	15	[A.7] Uso no previsto	Acceso no autorizado a la informacion.
170	Consultas y conceptos	15	[A.11] Acceso no autorizado	Falta de controles de acceso lógico
171	Consultas y conceptos	15	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
172	Consultas y conceptos	15	[A.7] Uso no previsto	Acceso no autorizado a la informacion.
173	Contratos Interadministrativo	15	[A.11] Acceso no autorizado	Falta de controles de acceso lógico
174	Contratos Interadministrativo	15	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
175	Contratos Interadministrativo	15	[A.7] Uso no previsto	Acceso no autorizado a la informacion.

176	Estudios previos contractuales Y Fichas Técnicas.	20	[A.11] Acceso no autorizado	Falta de controles de acceso lógico
177	Estudios previos contractuales Y Fichas Técnicas.	20	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
178	Estudios previos contractuales Y Fichas Técnicas.	20	[A.7] Uso no previsto	Acceso no autorizado a la informacion.
179	Control de Ingreso al edificio de alcaldes y funcionarios públicos (SUPERACCES)	18	[A.6] Abuso de privilegios de acceso	Falta de controles de acceso lógico
180	Control de Ingreso al edificio de alcaldes y funcionarios públicos (SUPERACCES)	18	[A.6] Abuso de privilegios de acceso	Segregación inadecuada de funciones
181	Control de Ingreso al edificio de alcaldes y funcionarios públicos (SUPERACCES)	18	[A.11] Acceso no autorizado	Segregación inadecuada de funciones

182	Control de Ingreso al edificio de alcaldes y funcionarios públicos (SUPERACCES)	18	[A.7] Uso no previsto	Acceso no autorizado a utilidades de la estación de trabajo
183	Informes de Alcaldías	16	[A.6] Abuso de privilegios de acceso	Falta de controles de acceso lógico
184	Informes de Alcaldías	16	[E.15] Alteración de la información	Falta de controles de acceso lógico
185	Carpetas de Gestión documental	16	[E.1] Errores de los usuarios	Segregación inadecuada de funciones
186	Carpetas de Gestión documental	16	[E.19] Divulgación de la información	Falta de conciencia de seguridad de la informacion
187	Carpetas de Gestión documental	16	[A.7] Uso no previsto	Falta de conciencia de seguridad de la informacion
188	Carpetas de Gestión documental	16	[E.15] Alteración de la información	Segregación inadecuada de funciones
189	Carpetas de Gestión documental	16	[E.19] Divulgación de la información	Circunstancias personales o coacción
190	Carpetas de Gestión documental	16	[A.5] Suplantación de la identidad del usuario	Circunstancias personales o coacción
191	Carpetas de Gestión documental	16	[E.19] Divulgación de la información	Falta de controles en la desvinculación
192	Consolidados de transferencias.	15	[A.11] Acceso no autorizado	Acceso no autorizado a la informacion.

193	Consolidados de transferencias.	15	[A.11] Acceso no autorizado	Falta de controles de acceso lógico
194	Consolidados de transferencias.	15	[A.11] Acceso no autorizado	Préstamo de usuarios y contraseñas
195	Consolidados de transferencias.	15	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
196	Bases de datos (sistema de distribución de transferencias)	25	[A.11] Acceso no autorizado	Debilidad en las contraseñas del sistema
197	Bases de datos (sistema de distribución de transferencias)	25	[A.5] Suplantación de la identidad del usuario	Falta de auditoría a la actividad sobre el sistema de información
198	Bases de datos (sistema de distribución de transferencias)	25	[A.5] Suplantación de la identidad del usuario	Préstamo de usuarios y contraseñas

199	Bases de datos (sistema de distribución de transferencias)	25	[E.15] Alteración de la información	Falta de controles de acceso lógico
200	Bases de datos (sistema de distribución de transferencias)	25	[E.4] Errores de configuración	Falta de auditoría a la actividad sobre el sistema de información
201	Bases de datos (sistema de distribución de transferencias)	25	[E.4] Errores de configuración	Falta de controles sobre la gestión del cambio
202	Bases de datos (sistema de distribución de transferencias)	25	[E.17] Degradación de la información	Errores de digitación
203	Software de deuda.	25	[A.11] Acceso no autorizado	Debilidad en las contraseñas del sistema
204	Software de deuda.	25	[A.5] Suplantación de la identidad del usuario	Falta de auditoría a la actividad sobre el sistema de información
205	Software de deuda.	25	[A.5] Suplantación de la identidad del usuario	Préstamo de usuarios y contraseñas

206	Software de deuda.	25	[E.15] Alteración de la información	Falta de controles de acceso lógico
207	Software de deuda.	25	[E.4] Errores de configuración	Falta de auditoría a la actividad sobre el sistema de información
208	Software de deuda.	25	[E.4] Errores de configuración	Falta de controles sobre la gestión del cambio
209	Software de deuda.	25	[E.17] Degradación de la información	Errores de digitación
210	SIGECCOM	25	[A.5] Suplantación de la identidad del usuario	Debilidad en las contraseñas del sistema
211	SIGECCOM	25	[A.5] Suplantación de la identidad del usuario	Falta de auditoría a la actividad sobre el sistema de información
212	SIGECCOM	25	[A.5] Suplantación de la identidad del usuario	Falta de auditoría a la actividad sobre el sistema de información
213	SIGECCOM	25	[A.5] Suplantación de la identidad del usuario	Falta de controles de acceso lógico
214	SIGECCOM	25	[A.6] Abuso de privilegios de acceso	Acceso de los desarrolladores a ambientes productivos
215	SIGECCOM	25	[A.5] Suplantación de la identidad del usuario	Segregación inadecuada de funciones
216	SIGECCOM	25	[E.15] Alteración de la información	Acceso no autorizado a utilidades del sistema de información

217	SIGECCOM	25	[E.15] Alteración de la información	Segregación inadecuada de funciones
218	Software de Distribucion Financiera (SDF).	25	[A.5] Suplantación de la identidad del usuario	Debilidad en las contraseñas del sistema
219	Software de Distribucion Financiera (SDF).	25	[A.5] Suplantación de la identidad del usuario	Falta de auditoría a la actividad sobre el sistema de información
220	Software de Distribucion Financiera (SDF).	25	[A.5] Suplantación de la identidad del usuario	Falta de auditoría a la actividad sobre el sistema de información
221	Software de Distribucion Financiera (SDF).	25	[A.5] Suplantación de la identidad del usuario	Falta de controles de acceso lógico
222	Software de Distribucion Financiera (SDF).	25	[A.6] Abuso de privilegios de acceso	Acceso de los desarrolladores a ambientes productivos

223	Software de Distribucion Financiera (SDF).	25	[A.5] Suplantación de la identidad del usuario	Segregación inadecuada de funciones
224	Software de Distribucion Financiera (SDF).	25	[E.15] Alteración de la información	Acceso no autorizado a utilidades del sistema de información
225	Software de Distribucion Financiera (SDF).	25	[E.15] Alteración de la información	Segregación inadecuada de funciones
226	Conciliaciones.	16	[A.15] Modificación de información	Almacenamiento de material inflamable o volátil
227	Conciliaciones.	16	[A.15] Modificación de información	Clasificación de la información de manera inadecuada (en términos de confidencialidad, integridad y disponibilidad)
228	Conciliaciones.	16	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
229	Archivos de Recaudo Externo	20	[A.11] Acceso no autorizado	Debilidad en las contraseñas de la Red
230	Archivos de Recaudo Externo	20	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
231	Actualizaciones SDF	20	[A.11] Acceso no autorizado	Acceso no autorizado a la informacion.

232	Actualizaciones SDF	20	[A.11] Acceso no autorizado	Debilidad en las contraseñas de la Red
233	Actualizaciones SDF	20	[A.11] Acceso no autorizado	Falta de auditoría a la actividad de los usuarios en acceso a la informacion.
234	Actualizaciones SDF	20	[A.11] Acceso no autorizado	Falta de comunicación entre la Dirección Administrativa y Sistemas con respecto a la salida de personal de la Federación
235	Actualizaciones SDF	20	[A.11] Acceso no autorizado	Falta de controles de acceso lógico
236	Actualizaciones SDF	20	[A.11] Acceso no autorizado	Préstamo de usuarios y contraseñas
237	Actualizaciones SDF	20	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
238	Actualizaciones SDF	20	[E.15] Alteración de la información	Acceso no autorizado a la informacion.
239	Actualizaciones SDF	20	[E.15] Alteración de la información	Falta de controles de acceso lógico
240	Actualizaciones SDF	20	[A.11] Acceso no autorizado	Acceso no autorizado a la informacion.
241	Actualizaciones SDF	20	[A.11] Acceso no autorizado	Debilidad en las contraseñas de la Red

242	Actualizaciones SDF	20	[A.11] Acceso no autorizado	Falta de auditoría a la actividad de los usuarios en acceso a la informacion.
243	Actualizaciones SDF	20	[A.11] Acceso no autorizado	Falta de comunicación entre la Dirección Administrativa y Sistemas con respecto a la salida de personal de la Federación
244	Actualizaciones SDF	20	[A.11] Acceso no autorizado	Falta de controles de acceso lógico
245	Actualizaciones SDF	20	[A.11] Acceso no autorizado	Préstamo de usuarios y contraseñas
246	Actualizaciones SDF	20	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
247	Actualizaciones SDF	20	[E.15] Alteración de la información	Acceso no autorizado a la informacion.
248	Actualizaciones SDF	20	[E.15] Alteración de la información	Falta de controles de acceso lógico
249	Bases de datos (sistema de distribución de transferencias)	25	[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de planes de contingencia o procedimientos de recuperación

250	Bases de datos (sistema de distribución de transferencias)	25	[E.28] Indisponibilidad del personal	Falta de contingencias de respaldo de personal crítico
251	Bases de datos (sistema de distribución de transferencias)	25	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
252	Bases de datos (sistema de distribución de transferencias)	25	[A.15] Modificación de información	Copias no restringidas de datos o software
253	Bases de datos (sistema de distribución de transferencias)	25	[A.15] Modificación de información	Préstamo de usuarios y contraseñas
254	Certificaciones.	13	[A] Ataques deliberados	Falta de controles de acceso físico
255	Certificaciones.	13	[A.8] Difusión de software dañino	Falta de controles sobre el software descargado de Internet
256	Certificaciones.	13	[I.7] Condiciones inadecuadas de temperatura o humedad	Falta de planes de contingencia o procedimientos de recuperación
257	Certificaciones.	13	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Mantenimiento inadecuado de la estación de trabajo

258	Certificaciones.	13	[E.18] Destrucción de la información	Copias no restringidas de datos o software
259	Gastos de personal	16	[E.19] Divulgación de la información	Falta de controles de acceso físico
260	Gastos de personal	16	[E.19] Divulgación de la información	Segregación inadecuada de funciones
261	Gastos de personal	16	[E.19] Divulgación de la información	Clasificación de la información de manera inadecuada (en términos de confidencialidad, integridad y disponibilidad)
262	Gastos de personal	16	[A.15] Modificación de información	Falta de controles de integridad a los documentos
263	Planes de acción.	15	[E.19] Divulgación de la información	Falta de controles de acceso físico
264	Planes de acción.	15	[E.19] Divulgación de la información	Segregación inadecuada de funciones
265	Planes de acción.	15	[E.19] Divulgación de la información	Clasificación de la información de manera inadecuada (en términos de confidencialidad, integridad y disponibilidad)
266	Planes de acción.	15	[A.15] Modificación de información	Falta de controles de integridad a los documentos
267	Planes de acción.	15	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
268	Planes de acción.	15	[I.7] Condiciones inadecuadas de temperatura o humedad	Monitoreo inadecuado de las condiciones ambientales
269	Planes de acción.	15	[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de planes de contingencia o procedimientos de recuperación
270	Planes de acción.	15	[E.28] Indisponibilidad del personal	Falta de documentación

271	Seguimiento de Contratos Gremial	25	[E.28] Indisponibilidad del personal	Falta de documentación
272	Seguimiento de Contratos Gremial	25	[E.19] Divulgación de la información	Falta de controles de almacenamiento y resguardo sobre los archivos
273	Seguimiento de Contratos Gremial	25	[E.1] Errores de los usuarios	Falta de documentación
274	Seguimiento de Contratos Gremial	25	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de planes de contingencia o procedimientos de recuperación
275	Inventario y movimientos de Almacén	20	[E.28] Indisponibilidad del personal	Falta de documentación
276	Inventario y movimientos de Almacén	20	[E.19] Divulgación de la información	Falta de controles de almacenamiento y resguardo sobre los archivos
277	Inventario y movimientos de Almacén	20	[E.1] Errores de los usuarios	Falta de documentación
278	Inventario y movimientos de Almacén	20	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de planes de contingencia o procedimientos de recuperación

279	Listas de asistencia de los procesos relacionados a gestión humana (inducciòn, socializaciones, actividades, capacitaciones) FÍSICOS	15	[E.28] Indisponibilidad del personal	Falta de documentación
280	Listas de asistencia de los procesos relacionados a gestión humana (inducciòn, socializaciones, actividades, capacitaciones) FÍSICOS	15	[E.19] Divulgación de la información	Falta de controles de almacenamiento y resguardo sobre los archivos

281	Listas de asistencia de los procesos relacionados a gestión humana (inducciòn, socializaciones, actividades, capacitaciones) FÍSICOS	15	[E.1] Errores de los usuarios	Falta de documentación
282	Listas de asistencia de los procesos relacionados a gestión humana (inducciòn, socializaciones, actividades, capacitaciones) FÍSICOS	15	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Falta de planes de contingencia o procedimientos de recuperación
283	Chip (consolidado de información de la contaduría general de la nación)	17	[A.15] Modificación de información	Clasificación de la información de manera inadecuada (en términos de confidencialidad, integridad y disponibilidad)

284	Chip (consolidado de información de la contaduría general de la nación)	17	[A.15] Modificación de información	Falta de controles de acceso físico
285	Chip (consolidado de información de la contaduría general de la nación)	17	[E.19] Divulgación de la información	Falta de controles de almacenamiento y resguardo sobre los documentos
286	Chip (consolidado de información de la contaduría general de la nación)	17	[E.18] Destrucción de la información	Clasificación de la información de manera inadecuada (en términos de confidencialidad, integridad y disponibilidad)
287	Chip (consolidado de información de la contaduría general de la nación)	17	[E.18] Destrucción de la información	Falta de controles de almacenamiento y resguardo sobre los documentos
288	Chip (consolidado de información de la contaduría general de la nación)	17	[A] Ataques deliberados	Falta de controles de acceso físico

289	Mesa de ayuda.	18	[E.1] Errores de los usuarios	Segregación inadecuada de funciones
290	Mesa de ayuda.	18	[E.19] Divulgación de la información	Falta de conciencia de seguridad de la informacion
291	Mesa de ayuda.	18	[A.7] Uso no previsto	Falta de conciencia de seguridad de la informacion
292	Mesa de ayuda.	18	[E.15] Alteración de la información	Segregación inadecuada de funciones
293	Mesa de ayuda.	18	[E.19] Divulgación de la información	Circunstancias personales o coacción
294	Mesa de ayuda.	18	[A.5] Suplantación de la identidad del usuario	Circunstancias personales o coacción
295	Mesa de ayuda.	18	[E.19] Divulgación de la información	Falta de controles en la desvinculación
296	Mesa de ayuda.	18	[E.1] Errores de los usuarios	Segregación inadecuada de funciones
297	Tesorería.	23	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
298	Tesorería.	23	[A.15] Modificación de información	Falta de controles de acceso lógico
299	Tesorería.	23	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los archivos

300	Tesorería.	23	[A.15] Modificación de información	Préstamo de usuarios y contraseñas
301	Tesorería.	23	[A.4] Manipulación de la configuración	Falta de controles en el traslado de los dispositivos
302	Tesorería.	23	[E.19] Divulgación de la información	Falta de controles de almacenamiento y resguardo sobre los archivos
303	Informes a Dian	18	[A.5] Suplantación de la identidad del usuario	Ubicación inadecuada de la estación de trabajo
304	Informes a Dian	18	[A.15] Modificación de información	Copias no restringidas de datos o software
305	Informes a Dian	18	[A.15] Modificación de información	Falta de controles de acceso lógico
306	Informes a Dian	18	[E.18] Destrucción de la información	Copias no restringidas de datos o software
307	Secretaria de hacienda distrital.	15	[A.5] Suplantación de la identidad del usuario	Ubicación inadecuada de la estación de trabajo
308	Secretaria de hacienda distrital.	15	[A.15] Modificación de información	Copias no restringidas de datos o software
309	Secretaria de hacienda distrital.	15	[A.15] Modificación de información	Falta de controles de acceso lógico
310	Secretaria de hacienda distrital.	15	[E.18] Destrucción de la información	Copias no restringidas de datos o software

311	Firma digital certicámara	25	[A.11] Acceso no autorizado	Préstamo de usuarios y contraseñas
312	Firma digital certicámara	25	[E.1] Errores de los usuarios	Segregación inadecuada de funciones
313	Firma digital Dian	25	[A.11] Acceso no autorizado	Préstamo de usuarios y contraseñas
314	Firma digital Dian	25	[E.1] Errores de los usuarios	Segregación inadecuada de funciones
315	Firma Escaneadas Directores	25	[A.11] Acceso no autorizado	Préstamo de usuarios y contraseñas
316	Firma Escaneadas Directores	25	[E.1] Errores de los usuarios	Segregación inadecuada de funciones
317	Documentos de soporte de contratos de Interventoría a concesiones	15	[A.11] Acceso no autorizado	Segregación inadecuada de funciones

318	Documentos de soporte de contratos de Interventoría a concesiones	15	[A.15] Modificación de información	Falta de controles de acceso lógico
319	Documentos de soporte de contratos de Interventoría a concesiones	15	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los archivos
320	Documentos de soporte de contratos de Interventoría a concesiones	15	[A.15] Modificación de información	Préstamo de usuarios y contraseñas
321	Documentos de soporte de contratos de Interventoría a concesiones	15	[E.19] Divulgación de la información	Falta de controles de almacenamiento y resguardo sobre los archivos

322	Documentos de soporte de contratos de Interventoría a concesiones	15	[A.4] Manipulación de la configuración	Falta de controles en el traslado de los dispositivos
323	Capitulo de Autoridades de Tránsito	15	[A.15] Modificación de información	Clasificación de la información de manera inadecuada (en términos de confidencialidad, integridad y disponibilidad)
324	Capitulo de Autoridades de Tránsito	15	[E.18] Destrucción de la información	Falta de controles de almacenamiento y resguardo sobre los documentos
325	Capitulo de Autoridades de Tránsito	15	[E.19] Divulgación de la información	Falta de controles de almacenamiento y resguardo sobre los documentos
326	Capitulo de Autoridades de Tránsito	15	[A.15] Modificación de información	Falta de controles de acceso físico
327	Capitulo de Autoridades de Tránsito	15	[E.18] Destrucción de la información	Clasificación de la información de manera inadecuada (en términos de confidencialidad, integridad y disponibilidad)

328	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	20	[A.5] Suplantación de la identidad del usuario	Falta de comunicación entre talento humano y la Dirección de Sistemas con respecto a la salida de personal de la Federación
329	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	20	[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de controles sobre la gestión del cambio
330	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	20	[A.5] Suplantación de la identidad del usuario	Falta de controles de acceso lógico

331	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	20	[A.5] Suplantación de la identidad del usuario	Préstamo de usuarios y contraseñas
332	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	20	[E.1] Errores de los usuarios	Errores de digitación
333	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	20	[A.5] Suplantación de la identidad del usuario	Segregación inadecuada de funciones

334	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	20	[E.15] Alteración de la información	Acceso no autorizado a utilidades del sistema de información
335	Directorio de Autoridades de Tránsito	20	[A.11] Acceso no autorizado	Debilidad en las contraseñas del sistema
336	Directorio de Autoridades de Tránsito	20	[A.5] Suplantación de la identidad del usuario	Falta de auditoría a la actividad sobre el sistema de información
337	Directorio de Autoridades de Tránsito	20	[A.5] Suplantación de la identidad del usuario	Préstamo de usuarios y contraseñas
338	Directorio de Autoridades de Tránsito	20	[E.15] Alteración de la información	Falta de controles de acceso lógico
339	Directorio de Autoridades de Tránsito	20	[E.4] Errores de configuración	Falta de auditoría a la actividad sobre el sistema de información

340	Directorio de Autoridades de Tránsito	20	[E.4] Errores de configuración	Falta de controles sobre la gestión del cambio
341	Directorio de Autoridades de Tránsito	20	[E.17] Degradación de la información	Errores de digitación
342	Soporte a Capacitación	16	[E.19] Divulgación de la información	Falta de controles de acceso físico
343	Soporte a Capacitación	16	[E.19] Divulgación de la información	Segregación inadecuada de funciones
344	Soporte a Capacitación	16	[E.19] Divulgación de la información	Clasificación de la información de manera inadecuada (en términos de confidencialidad, integridad y disponibilidad)
345	Soporte a Capacitación	16	[A.15] Modificación de información	Falta de controles de integridad a los documentos
346	Soporte a Capacitación	16	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los documentos
347	Soporte a Capacitación	16	[I.7] Condiciones inadecuadas de temperatura o humedad	Monitoreo inadecuado de las condiciones ambientales
348	Carpeta de servicios simit.	22	[A.11] Acceso no autorizado	Acceso no autorizado a la informacion.

349	Carpeta de servicios simit.	22	[A.11] Acceso no autorizado	Debilidad en las contraseñas de la Red
350	Carpeta de servicios simit.	22	[A.11] Acceso no autorizado	Falta de auditoría a la actividad de los usuarios en acceso a la informacion.
351	Carpeta de servicios simit.	22	[A.11] Acceso no autorizado	Falta de comunicación entre la Dirección Administrativa y Sistemas con respecto a la salida de personal de la Federación
352	Carpeta de servicios simit.	22	[A.11] Acceso no autorizado	Falta de controles de acceso lógico
353	Carpeta de servicios simit.	22	[A.11] Acceso no autorizado	Préstamo de usuarios y contraseñas
354	Carpeta de servicios simit.	22	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
355	Carpeta de servicios simit.	22	[E.15] Alteración de la información	Acceso no autorizado a la informacion.
356	Carpeta de servicios simit.	22	[E.15] Alteración de la información	Falta de controles de acceso lógico
357	Carpeta de servicios simit.	22	[A.11] Acceso no autorizado	Acceso no autorizado a la informacion.
358	Carpeta de servicios simit.	22	[A.11] Acceso no autorizado	Debilidad en las contraseñas de la Red

359	Carpeta de servicios simit.	22	[A.11] Acceso no autorizado	Falta de auditoría a la actividad de los usuarios en acceso a la informacion.
360	Carpeta de servicios simit.	22	[A.11] Acceso no autorizado	Falta de comunicación entre la Dirección Administrativa y Sistemas con respecto a la salida de personal de la Federación
361	Banco de Proyectos (Proyectos)	20	[A.11] Acceso no autorizado	Falta de controles de acceso lógico
362	Política pública.	16	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
363	Pagos especiales.	23	[E.15] Alteración de la información	Acceso no autorizado a la informacion.
364	Manuales de operación no concesionada.	18	[E.15] Alteración de la información	Falta de controles de acceso lógico
365	Soportes de pago (transferencias).	20	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
366	Soportes de pago (transferencias).	20	[A.15] Modificación de información	Falta de controles de acceso lógico
367	Soportes de pago (transferencias).	20	[A.15] Modificación de información	Falta de controles de almacenamiento y resguardo sobre los archivos
368	Soportes de pago (transferencias).	20	[A.15] Modificación de información	Préstamo de usuarios y contraseñas

369	Soportes de pago (transferencias).	20	[E.19] Divulgación de la información	Falta de controles de almacenamiento y resguardo sobre los archivos
370	Soportes de pago (transferencias).	20	[A.4] Manipulación de la configuración	Falta de controles en el traslado de los dispositivos
371	Soportes de pago (transferencias).	20	[A.11] Acceso no autorizado	Segregación inadecuada de funciones
372	Logística de eventos (FCM - SIMIT).	15	[A.7] Uso no previsto	Falta de controles en el reclutamiento
373	Logística de eventos (FCM - SIMIT).	15	[A.5] Suplantación de la identidad del usuario	Falta de controles en el reclutamiento
374	Logística de eventos (FCM - SIMIT).	15	[A.7] Uso no previsto	Segregación inadecuada de funciones
375	Logística de eventos (FCM - SIMIT).	15	[E.1] Errores de los usuarios	Segregación inadecuada de funciones
376	Bases de datos logística y proveedores.	15	[A.5] Suplantación de la identidad del usuario	Falta de controles de acceso lógico

377	Bases de datos logística y proveedores.	15	[A.5] Suplantación de la identidad del usuario	Segregación inadecuada de funciones
378	Bases de datos logística y proveedores.	15	[A.6] Abuso de privilegios de acceso	Acceso de los desarrolladores a ambientes productivos
379	Bases de datos logística y proveedores.	15	[E.15] Alteración de la información	Segregación inadecuada de funciones
380	Bases de datos logística y proveedores.	15	[E.1] Errores de los usuarios	Segregación inadecuada de funciones
381	Bases de datos logística y proveedores.	15	[E.28] Indisponibilidad del personal	Falta de conocimiento del soporte de la aplicación
382	Canal de comunicaciones.	25	[A.5] Suplantación de la identidad del usuario	Falta de controles en el traslado de los dispositivos
383	Canal de comunicaciones.	25	[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de planes de contingencia o procedimientos de recuperación
384	Canal de comunicaciones.	25	[I.7] Condiciones inadecuadas de temperatura o humedad	Ubicación en áreas susceptibles a temperaturas y humedad extremas

385	Canal de comunicaciones.	25	[E.28] Indisponibilidad del personal	Falta de documentación
386	Canal de comunicaciones.	25	[E.18] Destrucción de la información	Falta de tratamiento de incidentes de seguridad de la información
387	Base de datos de desarrollo.	23	[E.18] Destrucción de la información	Falta de controles de acceso lógico
388	Base de datos de desarrollo.	23	[E.28] Indisponibilidad del personal	Falta de contingencias de respaldo de personal crítico
389	Base de datos de desarrollo.	23	[E.18] Destrucción de la información	Préstamo de usuarios y contraseñas
390	Base de datos de desarrollo.	23	[E.18] Destrucción de la información	Falta de tratamiento de incidentes de seguridad de la información
391	Base de datos de desarrollo.	23	[A.11] Acceso no autorizado	Falta de auditoría a la actividad de los usuarios en acceso a la informacion.
392	Base de datos de pruebas.	23	[E.18] Destrucción de la información	Falta de controles de acceso lógico
393	Base de datos de pruebas.	23	[E.28] Indisponibilidad del personal	Falta de contingencias de respaldo de personal crítico

394	Base de datos de pruebas.	23	[E.18] Destrucción de la información	Préstamo de usuarios y contraseñas
395	Base de datos de pruebas.	23	[E.18] Destrucción de la información	Falta de tratamiento de incidentes de seguridad de la información
396	Base de datos de pruebas.	23	[A.11] Acceso no autorizado	Falta de auditoría a la actividad de los usuarios en acceso a la informacion.
397	Base de datos producción.	25	[E.18] Destrucción de la información	Falta de controles de acceso lógico
398	Base de datos producción.	25	[E.28] Indisponibilidad del personal	Falta de contingencias de respaldo de personal crítico
399	Base de datos producción.	25	[E.18] Destrucción de la información	Préstamo de usuarios y contraseñas
400	Base de datos producción.	25	[E.18] Destrucción de la información	Falta de tratamiento de incidentes de seguridad de la información
401	Base de datos producción.	25	[A.11] Acceso no autorizado	Falta de auditoría a la actividad de los usuarios en acceso a la informacion.
402	Backups base de datos simit.	25	[I.10] Degradación de los soportes de almacenamiento de la información	Falta de controles de acceso físico
403	Backups base de datos simit.	25	[E.4] Errores de configuración	Falta de controles de almacenamiento y resguardo sobre los medios de almacenamiento
404	Backups base de datos simit.	25	[E.4] Errores de configuración	Falta de controles de almacenamiento y resguardo sobre los medios de almacenamiento

405	Backups base de datos simit.	25	[E.18] Destrucción de la información	Clasificación de la información de manera inadecuada (en términos de confidencialidad, integridad y disponibilidad)
406	Backups base de datos simit.	25	[E.18] Destrucción de la información	Falta de controles de acceso físico
407	Backups base de datos simit.	25	[E.18] Destrucción de la información	Falta de controles en el préstamo de los medios de almacenamiento
408	Servidores store wise.	22	[A.4] Manipulación de la configuración	Falta de tratamiento de incidentes de seguridad de la información
409	Servidores store wise.	22	[A.6] Abuso de privilegios de acceso	Falta de políticas de manejo de contraseñas críticas
410	Servidores store wise.	22	[A.4] Manipulación de la configuración	Falta de tratamiento de incidentes de seguridad de la información
411	Servidores store wise.	22	[E.2] Errores del administrador	Falta de auditoría a la actividad sobre el servidor
412	Servidores store wise.	22	[E.2] Errores del administrador	Falta de controles de acceso lógico
413	Servidores store wise.	22	[E.2] Errores del administrador	Insuficiencia de archivos de backup
414	Servidores store wise.	22	[E.1] Errores de los usuarios	Falta de documentación

415	Servidores store wise.	22	[N.*]Desastres naturales	Falta de planes de contingencia o procedimientos de recuperación
416	Firewall.	22	[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de planes de contingencia o procedimientos de recuperación
417	Firewall.	22	[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de controles sobre la gestión del cambio
418	Firewall.	22	[I.8] Fallo de servicios de comunicaciones	Administración inadecuada de la red
419	Firewall.	22	[A.14] Interceptación de información (escucha)	Falta de seguridad física sobre los armarios o hubs de comunicaciones de datos
420	Firewall.	22	[E.18] Destrucción de la información	Copias no restringidas de datos o software
421	Firewall.	22	[E.18] Destrucción de la información	Falta de controles de acceso lógico
422	Firewall.	22	[E.28] Indisponibilidad del personal	Falta de contingencias de respaldo de personal crítico
423	Datacenter.	25	[A.6] Abuso de privilegios de acceso	Falta de políticas de manejo de contraseñas críticas
424	Datacenter.	25	[A.4] Manipulación de la configuración	Falta de tratamiento de incidentes de seguridad de la información
425	Datacenter.	25	[E.2] Errores del administrador	Falta de auditoría a la actividad sobre el servidor
426	Datacenter.	25	[E.2] Errores del administrador	Falta de controles de acceso lógico
427	Datacenter.	25	[E.2] Errores del administrador	Insuficiencia de archivos de backup

428	Datacenter.	25	[E.1] Errores de los usuarios	Falta de documentación
429	Datacenter.	25	[N.*]Desastres naturales	Falta de planes de contingencia o procedimientos de recuperación
430	UPS.	13	[A.5] Suplantación de la identidad del usuario	Ubicación inadecuada de la estación de trabajo
431	UPS.	13	[A.4] Manipulación de la configuración	Falta de controles en el traslado de los dispositivos
432	VPN site to site.	25	[A.5] Suplantación de la identidad del usuario	Falta de controles en el traslado de los dispositivos
433	VPN site to site.	25	[E.21] Errores de mantenimiento / actualización de programas (software)	Falta de planes de contingencia o procedimientos de recuperación
434	VPN site to site.	25	[I.7] Condiciones inadecuadas de temperatura o humedad	Ubicación en áreas susceptibles a temperaturas y humedad extremas
435	VPN site to site.	25	[E.28] Indisponibilidad del personal	Falta de documentación
436	VPN site to site.	25	[E.18] Destrucción de la información	Falta de tratamiento de incidentes de seguridad de la información
437	Switch core.	20	[E.28] Indisponibilidad del personal	Falta de documentación

438	Switch core.	20	[E.1] Errores de los usuarios	Falta de documentación
439	Switch core.	20	[N.*]Desastres naturales	Falta de planes de contingencia o procedimientos de recuperación
440	Bodega de Datos	25	[E.18] Destrucción de la información	Falta de controles de acceso lógico

A continuación los controles de seguridad que se deben aplicar junto con el plan de tratamiento de los riesgos:

Tabla 18.

GESTION DE RIESGOS: ANALISIS DE RIESGOS Y TRATAMIENTO DE LOS RIESGOS				
No. De Amenazas y Vulnerabilidades	**Nombre del activo de información**	**VALORACIÓN DEL RIESGO DE LOS ACTIVOS**	**CONTROLES QUE SE DEBEN APLICAR SEGÚN EL ANEXO A DE LA NORMA ISO 27001:2013**	**PLAN DE TRATAMIENTO DE RIESGOS SUGERIDOS**
1	Tutelas	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. Implementar permisos a nivel de uso de las aplicaciones del sistema. Extender las restricciones en el dominio para todos los usuarios finales. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
2	Tutelas	15	A.9.1.1 Política de control de acceso	1. Realizar el plan de concientización y entrenamiento formal debido a la

			A.9.3.1 Uso de información secreta de autenticación	importancia del tema del uso de las contraseñas.
3	Tutelas	15	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Realizar revisiones periódicas a los registros y determinar un política de almacenamiento que detalle los términos y responsabilidades, así como los mecanismos de seguridad para tales registros. 2. Los registros de los sistemas de monitoreo deben ser revisados periódicamente en busca de mejoras en su implementación y uso. 3. El acceso a los registros debe ser exclusivo para los auditores, administradores de la plataforma y oficial de seguridad. Estos registros deben estar asegurados en un sistema de archivos protegido.
4	Tutelas	15	A.7.3.1 Terminación o cambio de responsabilidades de empleo A.9.2.6 Retiro o ajuste de los derechos de acceso	1. Incluír el proceso en el SGSI cuando haya sido implementado en la terminación de contratos. 2. Debe establecerse un procedimiento formal y consistente dentro del SGSI para la eliminación de los derechos de acceso cuando las personas se retiren.
5	Tutelas	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
6	Tutelas	15	A.9.3.1 Uso de información secreta de autenticación	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
7	Tutelas	15	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
8	Tutelas	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Implementar permisos a nivel de uso de las aplicaciones del sistema. Extender las restricciones en el dominio para todos los usuarios finales. 2. Definir periodicidad y

			A.9.4.4 Uso de programas utilitarios privilegiados	detalle del procedimiento al controlar la revisión de privilegios.
9	Tutelas	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
10	Tutelas	15	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro	1. Los registros de los sistemas de monitoreo deben ser revisados periódicamente en busca de mejoras en su implementación y uso. 2. El acceso a los registros debe ser exclusivo para los auditores, administradores de la plataforma y oficial de seguridad. Estos registros deben estar asegurados en un sistema de archivos protegidos.
11	Tutelas	15	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
12	Tutelas	15	A.12.1.1 Procedimientos de operación documentados	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI
13	Tutelas	15	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
14	Tutelas	15	A.12.1.1 Procedimientos de operación documentados A.12.1.2 Gestión de cambios	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI

15	Tutelas	15	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
16	Tutelas	15	A.6.1.2 Separación de deberes	1. La información de contingencias de respaldo de personal crítico debe mantener un esquema estructural, para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
17	Tutelas	15	A.12.1.1 Procedimientos de operación documentados	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI
18	Tutelas	15	A.18.1.2 Derechos de propiedad intelectual	1. Mantener el esquema de control de licenciamiento implementado. Generar una política de cumplimiento sobre la propiedad intelectual.
19	Tutelas	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
20	Tutelas	15	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro	1. Los registros de los sistemas de monitoreo deben ser revisados periódicamente en busca de mejoras en su implementación y uso. 2. El acceso a los registros debe ser exclusivo para los auditores, administradores de la plataforma y oficial de seguridad. Estos registros deben estar asegurados en un sistema de archivos protegidos.

21	Tutelas	15	A.9.3.1 Uso de información secreta de autenticación	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
22	Tutelas	15	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
23	Modulo Proyectos SAP	25	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
24	Modulo Proyectos SAP	25	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
25	Modulo Proyectos SAP	25	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
26	Modulo Proyectos SAP	25	A.15.1.2 Tratamiento la seguridad dentro de los acuerdos con los proveedores A.15.2.1 Seguimiento y revisión de los servicios de los proveedores	1. Alinear Acuerdos de Niveles de Servicio con el Proveedor con la implementación del SGSI, todos los análisis de riesgo externos e internos sobre los activos de información. Esto permitirá incluírlos en los indicadores de seguridad. 2. Se debe aprender de las auditorías realizadas a los contratos de los terceros y revisar los controles implementados para cada contrato con el fin de mejorar en el siguiente ciclo del SGSI.

27	Modulo Proyectos SAP	25	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
28	Modulo Proyectos SAP	25	A.6.1.2 Separación de deberes	1. La información de contingencias de respaldo de personal crítico debe mantener un esquema estructural, para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
29	Archivo de planes de acción (últimos 5 años)	17	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
30	Archivo de planes de acción (últimos 5 años)	17	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
31	Archivo de planes de acción (últimos 5 años)	17	A.12.1.1 Procedimientos de operación documentados	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI

32	Archivo de planes de acción (últimos 5 años)	17	A.18.1.2 Derechos de propiedad intelectual	1. Mantener el esquema de control de licenciamiento implementado. Generar una política de cumplimiento sobre la propiedad intelectual.
33	Archivo de planes de acción (últimos 5 años)	17	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	1. Desarrollar la politica al SGSI de contraseñas para ser divulgada en la organización. 2. Realizar el plan de concientización y entrenamiento formal debido a la importancia del tema.
34	Archivo de planes de acción (últimos 5 años)	17	A.7.3.1 Terminación o cambio de responsabilidades de empleo A.8.1.4 Devolución de activos A.9.2.6 Retiro o ajuste de los derechos de acceso	1. Debe establecerse un procedimiento formal y consistente dentro del SGSI. 2. Incluír el proceso en el SGSI cuando haya sido implementado en la terminación de contratos.
35	Archivo de planes de acción (últimos 5 años)	17	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado. 2. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso.
36	Archivo de planes de acción (últimos 5 años)	17	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
37	Archivo de planes de acción (últimos 5 años)	17	A.8.2.3 Manejo de activos	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.

38	Archivo de planes de acción (últimos 5 años)	17		1. Debe mantenerse la guía con lineamientos claros, alineada al SGSI, que exija unos mínimos lineamientos en el desarrollo y puesta en marcha de nuevos sistemas de información. 2. Implementar un Mecanismos oficiales para la validación de datos.
39	Archivo de planes de acción (últimos 5 años)	17	A.9.3.1 Uso de información secreta de autenticación	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
40	Archivo de planes de acción (últimos 5 años)	17	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
41	Archivo de planes de acción (últimos 5 años)	17	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
42	Archivo de planes de acción (últimos 5 años)	17	A.8.2.3 Manejo de activos	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
43	Archivo de planes de acción (últimos 5 años)	17	A.9.3.1 Uso de información secreta de autenticación	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
44	Archivo de planes de acción (últimos 5 años)	17	A.11.2.5 Retiro de activos	1. los controles en el translado de los dispositivos debe revisarse y monitorearse constantemente para corregir posibles fallas en los controles.

45	Portafolio de sevicios SIMIT	15	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.3 Seguridad de oficinas, recintos e instalaciones	1. Mantener un esquema para luego ser monitoreado por el responsable. 2. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior.
46	Portafolio de sevicios SIMIT	15	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado. 2. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso.
47	Portafolio de sevicios SIMIT	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
48	Portafolio de sevicios SIMIT	15	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado. 2. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso.
49	Actas de Seguimiento a la gestón procesal	22	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	1. Realizar el plan de concientización y entrenamiento formal debido a la importancia del tema relacionado con las contraseñas del sistema.

50	Actas de Seguimiento a la gestón procesal	22	A.9.3.1 Uso de información secreta de autenticación	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
51	Actas de Seguimiento a la gestón procesal	22	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
52	Actas de Seguimiento a la gestón procesal	22	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
53	Aplicativo SIMIT	25	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1 el Procedimiento de documentación de fallas reportadas por usuarios o por programas del sistema relacionadas con los sistemas de comunicación de procesamiento de la información. Política de manejo de fallas reportadas aprobada y divulgada.
54	Aplicativo SIMIT	25	A.9.3.1 Uso de información secreta de autenticación	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
55	Aplicativo SIMIT	25	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Realizar las revisiones periódicas de auditoria el el sistemas de informción, definir el procedimieto de monitoreo y su relación con el de reacción a incidentes. Logs de auditoría de la actividad de administradores y operadores habilitados. 2. Procedimiento de documentación de fallas reportadas por usuarios o por programas del sistema relacionadas con los sistemas de comunicación de procesamiento de la información. Política de manejo de fallas reportadas aprobada y divulgada.
56	Aplicativo SIMIT	25	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.

57	Aplicativo SIMIT	25	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
58	Aplicativo SIMIT	25	A.12.1.2 Gestión de cambios A.6.1.2 Separación de deberes A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Los controles y protección de los datos deben ser iguales tanto para producción como para desarrollo y pruebas dado que son los mismos. El SGSI debería incluír lineamientos de manejo de los datos en Desarrollo y Pruebas con respecto a la confidencialidad de la información. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
59	Aplicativo SIMIT	25	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
60	Aplicativo SIMIT	25	A.15.1.2 Tratamiento la seguridad dentro de los acuerdos con los proveedores A.15.2.1 Seguimiento y revisión de los servicios de los proveedores	1. Alinear Acuerdos de Niveles de Servicio con el Proveedor con la implementación del SGSI, todos los análisis de riesgo externos e internos sobre los activos de información. Esto permitirá incluírlos en los indicadores de seguridad. 2. Se debe aprender de las auditorías realizadas a los contratos de los terceros y revisar los controles implementados para cada contrato con el fin de mejorar en el siguiente ciclo del SGSI.
61	Aplicativo SIMIT	25	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
62	Servicios de Impresión	11	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de	1. Definir los controles de acceso lógico periodicidad y detalle del procedimiento al controlar la revisión de privilegios.

			autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	
63	Estadísticas contraloría	13	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
64	Procedimientos Y Consultas PL/SQL	23	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	1. Desarrollar la politica del uso de contraseñas alineadas con el SGSI para ser divulgada en la organización.
65	Procedimientos Y Consultas PL/SQL	23	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
66	Procedimientos Y Consultas PL/SQL	23	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. Implementar permisos a nivel de uso de las aplicaciones del sistema. Extender las restricciones en el dominio para todos los usuarios finales. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
67	Procedimientos Y Consultas PL/SQL	23	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. Implementar permisos a nivel de uso de las aplicaciones del sistema. Extender las restricciones en el dominio para todos los usuarios finales. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
68	Bitacora de Casos SIMIT	22	A.12.1.1 Procedimientos de operación documentados	1. Los manuales deben incluír procedimientos contingentes del área, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI.
69	Bitacora de Casos SIMIT	22	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Implementar permisos a nivel de uso de las aplicaciones del sistema. Extender las restricciones en el dominio para todos los usuarios finales. 2. Definir periodicidad y

			A.9.4.4 Uso de programas utilitarios privilegiados	detalle del procedimiento al controlar la revisión de privilegios.
70	Bitacora de Casos SIMIT	22	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro	1. Los registros de los sistemas de monitoreo deben ser revisados periódicamente en busca de mejoras en su implementación y uso. 2. El acceso a los registros debe ser exclusivo para los auditores, administradores de la plataforma y oficial de seguridad. Estos registros deben estar asegurados en un sistema de archivos protegidos.
71	Reportes y Estadisticas SIMIT	20	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
72	Reportes y Estadisticas SIMIT	20	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
73	Reportes y Estadisticas SIMIT	20	A.9.3.1 Uso de información secreta de autenticación	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
74	Software gestor de transito (Reporte data nueva)	25	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado.

75	Software gestor de transito (Reporte data nueva)	25	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
76	Software gestor de transito (Reporte data nueva)	25	A.12.1.1 Procedimientos de operación documentados A.12.1.2 Gestión de cambios A.14.2.2 Procedimientos de control de cambios en sistemas	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
77	Software gestor de transito (Reporte data nueva)	25	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado.
78	Software gestor de transito (Reporte data nueva)	25	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
79	Sistema de información SAP	25	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.

80	Sistema de información SAP	25	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado.
81	Sistema de información SAP	25	A.12.1.1 Procedimientos de operación documentados A.12.1.2 Gestión de cambios A.14.2.2 Procedimientos de control de cambios en sistemas	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
82	Sistema de información SAP	25	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
83	Sistema de información SAP	25	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
84	Archivos Contabilidad SDF	22	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado.
85	Archivos Contabilidad SDF	22	A.8.2.3 Manejo de activos	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma

				adecuada del manejo de la información.
86	Archivos Contabilidad SDF	22	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
87	Documentos de Nomina	17	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
88	Documentos de Nomina	17	A.8.2.3 Manejo de activos	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado.
89	Documentos de Nomina	17	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
90	Archivos Información Contratos Gremiales	22	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
91	Archivos Información Contratos Gremiales	22	A.8.2.3 Manejo de activos	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.

92	Archivos Información Contratos Gremiales	22	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Desarrollar la politica al SGSI para ser divulgada en la organización.
93	Archivos Información Contratos Gremiales	22	A.8.2.3 Manejo de activos	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
94	Base de datos de los colaboradores	25	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
95	Base de datos de los colaboradores	25	A.8.2.3 Manejo de activos	1. Los controles y protección de los datos deben ser iguales tanto para producción como para desarrollo y pruebas dado que son los mismos. El SGSI debería incluír lineamientos de manejo de los datos en Desarrollo y Pruebas con respecto a la confidencialidad de la información. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
96	Base de datos de los colaboradores	25	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
97	Base de datos de los colaboradores	25	A.8.2.3 Manejo de activos	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
98	Historia Laboral	11	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información	1. Implementar auditorías a todos los procesos solicitándo la información de responsabilidades a los recién contratados.

99	Historia Laboral	11	A.8.2.3 Manejo de activos	1. Desarrollar la politica al SGSI para ser divulgada en la organización.
100	Historia Laboral	11	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
101	Historia Laboral	11	A.8.2.3 Manejo de activos	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
102	Base de Datos Municipios Colombianos	23	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	1. Los controles y protección de los datos deben ser iguales tanto para producción como para desarrollo y pruebas dado que son los mismos. El SGSI debería incluír lineamientos de manejo de los datos en Desarrollo y Pruebas con respecto a la confidencialidad de la información. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
103	Base de Datos Municipios Colombianos	23	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
104	Base de Datos Municipios Colombianos	23	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.

105	Base de Datos Municipios Colombianos	23	A.12.1.2 Gestión de cambios A.6.1.2 Separación de deberes A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Implementar auditorías a todos los procesos solicitándo la información de responsabilidades a los recién contratados.
106	Base de Datos Municipios Colombianos	23	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Mantener un esquema para luego ser monitoreado por el responsable. 2. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior.
107	Base de Datos Municipios Colombianos	23	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Una vez establecida e implementada la política de seguridad, realizar los controles al cumplimiento de la misma.
108	Base de Datos Municipios Colombianos	23	A.7.1.2 Términos y condiciones de empleo A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
109	Base de datos alcaldes	22	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	1. Se debe mantener el esquema de contratos de mantenimiento constantes sobre los equipos tecnológicos. 2. Este esquema debe revisarse y monitorearse constantemente para corregir posibles fallas en los controles.
110	Base de datos alcaldes	22	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado. 2. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso.

111	Base de datos alcaldes	22	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Mantener un esquema para luego ser monitoreado por el responsable. 2. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior.
112	Base de datos alcaldes	22	A.12.1.2 Gestión de cambios A.6.1.2 Separación de deberes A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Una vez establecida e implementada la política de seguridad, realizar los controles al cumplimiento de la misma.
113	Base de datos alcaldes	22	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
114	Base de datos alcaldes	22	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Se debe mantener el esquema de contratos de mantenimiento constantes sobre los equipos tecnológicos. 2. Este esquema debe revisarse y monitorearse constantemente para corregir posibles fallas en los controles.
115	Base de datos alcaldes	22	A.7.1.2 Términos y condiciones de empleo A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información	1. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado. 2. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso.

116	Borrador de resoluciones relacionadas a la planta de personal y cambios de estructura	20	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.3 Seguridad de oficinas, recintos e instalaciones A.11.1.6 Áreas de despacho y carga	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
117	Borrador de resoluciones relacionadas a la planta de personal y cambios de estructura	20	A.18.2.2 Cumplimiento de las políticas y normas de seguridad	1. Realizar revisiones periódicas a los registros y determinar un política de almacenamiento que detalle los términos y responsabilidades, así como los mecanismos de seguridad para tales registros. 2. Los registros de los sistemas de monitoreo deben ser revisados periódicamente en busca de mejoras en su implementación y uso. 3. El acceso a los registros debe ser exclusivo para los auditores, administradores de la plataforma y oficial de seguridad. Estos registros deben estar asegurados en un sistema de archivos protegido.
118	Borrador de resoluciones relacionadas a la planta de personal y cambios de estructura	20	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
119	Borrador de resoluciones relacionadas a la planta de personal y cambios de estructura	20	A.11.2.4 Mantenimiento de los equipos A.11.2.5 Retiro de activos	1. Implementar permisos a nivel de uso de las aplicaciones del sistema. Extender las restricciones en el dominio para todos los usuarios finales. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.

120	Borrador de resoluciones relacionadas a la planta de personal y cambios de estructura	20	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
121	Certificaciones permanencia de alcaldes	17	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.3 Seguridad de oficinas, recintos e instalaciones A.11.1.6 Áreas de despacho y carga	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
122	Certificaciones permanencia de alcaldes	17	A.18.2.2 Cumplimiento de las políticas y normas de seguridad	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
123	Certificaciones permanencia de alcaldes	17	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. La información de contingencias de respaldo de personal crítico debe mantener un esquema estructural, para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
124	Certificaciones permanencia de alcaldes	17	A.11.2.4 Mantenimiento de los equipos A.11.2.5 Retiro de activos	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
125	Certificaciones permanencia de alcaldes	17	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.

126	Facturación Clientes.	17	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
127	Facturación Clientes.	17	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
128	Facturación Clientes.	17	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
129	Facturación Clientes.	17	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
130	Cuentas por pagar Proveedores.	16	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
131	Cuentas por pagar Proveedores.	16	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
132	Cuentas por pagar Proveedores.	16	A.9.3.1 Uso de información secreta de autenticación	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.

133	Cuentas por pagar Proveedores.	16	A.6.1.2 Separación de deberes	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
134	Informes contraloría.	17	A.8.2.3 Manejo de activos	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
135	Informes contraloría.	17	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
136	Carpeta daf tesorería	15	A.8.2.3 Manejo de activos	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
137	Carpeta daf tesorería	15	A.8.2.3 Manejo de activos	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
138	Carpeta daf tesorería	15	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
139	Carpeta DIR	15	A.8.2.3 Manejo de activos	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
140	Carpeta DIR	15	A.8.2.3 Manejo de activos	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
141	Carpeta DIR	15	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
142	Carpeta Presupuesto	16	A.8.2.3 Manejo de activos	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2.

				Mantener un esquema para luego ser monitoreado por el responsable.
143	Carpeta Presupuesto	16	A.8.2.3 Manejo de activos	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
144	Carpeta Presupuesto	16	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
145	Carpeta Corrrespondencia DAF	20	A.8.2.3 Manejo de activos	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
146	Carpeta Corrrespondencia DAF	20	A.8.2.3 Manejo de activos	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
147	Carpeta Corrrespondencia DAF	20	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
148	Procesos Contractuales	15	A.8.2.3 Manejo de activos	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
149	Procesos Contractuales	15	A.8.2.3 Manejo de activos	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
150	Procesos Contractuales	15	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
151	Procesos Judiciales	15	A.8.2.3 Manejo de activos	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.

152	Procesos Judiciales	15	A.8.2.3 Manejo de activos	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
153	Procesos Judiciales	15	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1. Mantener el esquema de acceso no autorizado implementado. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
154	Reportes Dane	20	A.8.2.3 Manejo de activos	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
155	Reportes Dane	20	A.8.2.3 Manejo de activos	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
156	Reportes Dane	20	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas.
157	Seguimiento a Polizas	15	A.8.2.3 Manejo de activos	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
158	Seguimiento a Polizas	15	A.8.2.3 Manejo de activos	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
159	Seguimiento a Polizas	15	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas.

160	Solicitud de Pedido y Contrato marco Dígital	15	A.8.2.3 Manejo de activos	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
161	Solicitud de Pedido y Contrato marco Dígital	15	A.8.2.3 Manejo de activos	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
162	Solicitud de Pedido y Contrato marco Dígital	15	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas.
163	Derechos de petición.	13	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
164	Estados financieros.	20	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI
165	Estados financieros.	20	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
166	Estados financieros.	20	A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.3.1 Uso de información secreta de autenticación	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar

				acciones para las cuales está autorizado.
167	Comodato	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
168	Comodato	15	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Implementar permisos a nivel de uso de las aplicaciones del sistema. Extender las restricciones en el dominio para todos los usuarios finales. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
169	Comodato	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. Definir los controles de acceso lógico periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
170	Consultas y conceptos	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
171	Consultas y conceptos	15	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
172	Consultas y conceptos	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.

			A.9.4.4 Uso de programas utilitarios privilegiados	
173	Contratos Interadministrativo	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
174	Contratos Interadministrativo	15	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
175	Contratos Interadministrativo	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
176	Estudios previos contractuales Y Fichas Técnicas.	20	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
177	Estudios previos contractuales Y Fichas Técnicas.	20	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.

178	Estudios previos contractuales Y Fichas Técnicas.	20	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado. 2. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso.
179	Control de Ingreso al edificio de alcaldes y funcionarios públicos (SUPERACCES)	18	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1 el Procedimiento de documentación de fallas reportadas por usuarios o por programas del sistema relacionadas con los sistemas de comunicación de procesamiento de la información. Política de manejo de fallas reportadas aprobada y divulgada.
180	Control de Ingreso al edificio de alcaldes y funcionarios públicos (SUPERACCES)	18	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
181	Control de Ingreso al edificio de alcaldes y funcionarios públicos (SUPERACCES)	18	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.

182	Control de Ingreso al edificio de alcaldes y funcionarios públicos (SUPERACCES)	18	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
183	Informes de Alcaldías	16	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Realizar el plan de concientización, el entrenamiento adecuado a los usuarios y la campaña completa de divulgación del SGSI.
184	Informes de Alcaldías	16	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Realizar el plan de concientización, el entrenamiento adecuado a los usuarios y la campaña completa de divulgación del SGSI.
185	Carpetas de Gestión documental	16	A.7.2.1 Responsabilidades de la Dirección A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información A.7.2.3 Proceso disciplinario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
186	Carpetas de Gestión documental	16	A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información	1.incluír el detalle de procesos disciplinarios y descargos, dentro del manual de funciones y en el SGSI
187	Carpetas de Gestión documental	16	A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información	1.incluír el detalle de procesos disciplinarios y descargos, dentro del manual de funciones y en el SGSI

188	Carpetas de Gestión documental	16	A.7.2.1 Responsabilidades de la Dirección A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información A.7.2.3 Proceso disciplinario	1. Incluír el proceso en el SGSI cuando haya sido implementado en la terminación de contratos.
189	Carpetas de Gestión documental	16	A.7.2.1 Responsabilidades de la Dirección A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información A.7.2.3 Proceso disciplinario	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
190	Carpetas de Gestión documental	16	A.7.2.1 Responsabilidades de la Dirección A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información A.7.2.3 Proceso disciplinario	1. Realizar el plan de concientización, el entrenamiento adecuado a los usuarios y la campaña completa de divulgación del SGSI.
191	Carpetas de Gestión documental	16	A.7.3.1 Terminación o cambio de responsabilidades de empleo	1. Realizar el plan de concientización, el entrenamiento adecuado a los usuarios y la campaña completa de divulgación del SGSI.
192	Consolidados de transferencias.	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. Implementar un estándar de desarrollo seguro de aplicaciones que cumpla con las políticas específicas de seguridad, en la revisión de entradas, procesamiento y salidas de información.
193	Consolidados de transferencias.	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Realizar el plan de concientización y entrenamiento formal debido a la importancia del tema relacionado con las contraseñas del sistema.
194	Consolidados de transferencias.	15	A.9.3.1 Uso de información secreta de autenticación	1. Realizar las revisiones periódicas de auditoria el el sistemas de informción, definir el procedimieto de monitoreo y su relación con el de reacción a incidentes. Logs de auditoría de la actividad de administradores y operadores habilitados. 2. Procedimiento de documentación de fallas reportadas por usuarios o por programas del sistema relacionadas con los

				sistemas de comunicación de procesamiento de la información. Política de manejo de fallas reportadas aprobada y divulgada.
195	Consolidados de transferencias.	15	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
196	Bases de datos (sistema de distribución de transferencias)	25	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
197	Bases de datos (sistema de distribución de transferencias)	25	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Realizar las revisiones periódicas de auditoria el el sistemas de informción, definir el procedimieto de monitoreo y su relación con el de reacción a incidentes. Logs de auditoría de la actividad de administradores y operadores habilitados. 2. Procedimiento de documentación de fallas reportadas por usuarios o por programas del sistema relacionadas con los sistemas de comunicación de procesamiento de la información. Política de manejo de fallas reportadas aprobada y divulgada.
198	Bases de datos (sistema de distribución de transferencias)	25	A.9.3.1 Uso de información secreta de autenticación	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI

199	Bases de datos (sistema de distribución de transferencias)	25	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Implementar un estándar de desarrollo seguro de aplicaciones que cumpla con las políticas específicas de seguridad, en la revisión de entradas, procesamiento y salidas de información.
200	Bases de datos (sistema de distribución de transferencias)	25	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Realizar el plan de concientización y entrenamiento formal debido a la importancia del tema relacionado con las contraseñas del sistema.
201	Bases de datos (sistema de distribución de transferencias)	25	A.12.1.1 Procedimientos de operación documentados A.12.1.2 Gestión de cambios A.14.2.2 Procedimientos de control de cambios en sistemas	1. Realizar las revisiones periódicas de auditoria el el sistemas de informción, definir el procedimieto de monitoreo y su relación con el de reacción a incidentes. Logs de auditoría de la actividad de administradores y operadores habilitados. 2. Procedimiento de documentación de fallas reportadas por usuarios o por programas del sistema relacionadas con los sistemas de comunicación de procesamiento de la información. Política de manejo de fallas reportadas aprobada y divulgada.
202	Bases de datos (sistema de distribución de transferencias)	25		1. Realizar las revisiones periódicas de auditoria el el sistemas de informción, definir el procedimieto de monitoreo y su relación con el de reacción a incidentes. Logs de auditoría de la actividad de administradores y operadores habilitados. 2. Procedimiento de documentación de fallas reportadas por usuarios o por programas del sistema relacionadas con los sistemas de comunicación de procesamiento de la información. Política de manejo de fallas reportadas aprobada y divulgada.

203	Software de deuda.	25	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
204	Software de deuda.	25	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Los controles y protección de los datos deben ser iguales tanto para producción como para desarrollo y pruebas dado que son los mismos. El SGSI debería incluír lineamientos de manejo de los datos en Desarrollo y Pruebas con respecto a la confidencialidad de la información. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
205	Software de deuda.	25	A.9.3.1 Uso de información secreta de autenticación	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
206	Software de deuda.	25	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
207	Software de deuda.	25	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
208	Software de deuda.	25	A.12.1.1 Procedimientos de operación documentados A.12.1.2 Gestión de cambios A.14.2.2 Procedimientos de	1. Realizar el plan de concientización y entrenamiento formal debido a la importancia del tema relacionado con las contraseñas del sistema.

209	Software de deuda.	25	control de cambios en sistemas	1. Realizar las revisiones periódicas de auditoria el el sistemas de informción, definir el procedimieto de monitoreo y su relación con el de reacción a incidentes. Logs de auditoría de la actividad de administradores y operadores habilitados. 2. Procedimiento de documentación de fallas reportadas por usuarios o por programas del sistema relacionadas con los sistemas de comunicación de procesamiento de la información. Política de manejo de fallas reportadas aprobada y divulgada.
210	SIGECCOM	25	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	1. Realizar las revisiones periódicas de auditoria el el sistemas de informción, definir el procedimieto de monitoreo y su relación con el de reacción a incidentes. Logs de auditoría de la actividad de administradores y operadores habilitados. 2. Procedimiento de documentación de fallas reportadas por usuarios o por programas del sistema relacionadas con los sistemas de comunicación de procesamiento de la información. Política de manejo de fallas reportadas aprobada y divulgada.
211	SIGECCOM	25	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
212	SIGECCOM	25	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Los controles y protección de los datos deben ser iguales tanto para producción como para desarrollo y pruebas dado que son los mismos. El SGSI debería incluír lineamientos de manejo de los datos en Desarrollo y Pruebas con respecto a la confidencialidad de la información. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
213	SIGECCOM	25	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar

			A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	acciones para las cuales está autorizado.
214	SIGECCOM	25	A.12.1.2 Gestión de cambios A.6.1.2 Separación de deberes A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
215	SIGECCOM	25	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
216	SIGECCOM	25	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	#N/A
217	SIGECCOM	25	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado.
218	Software de Distribucion Financiera (SDF).	25	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.

219	Software de Distribucion Financiera (SDF).	25	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Desarrollar la politica del uso de contraseñas alineadas con el SGSI para ser divulgada en la organización.
220	Software de Distribucion Financiera (SDF).	25	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
221	Software de Distribucion Financiera (SDF).	25	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Implementar permisos a nivel de uso de las aplicaciones del sistema. Extender las restricciones en el dominio para todos los usuarios finales. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
222	Software de Distribucion Financiera (SDF).	25	A.12.1.2 Gestión de cambios A.6.1.2 Separación de deberes A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Realizar el plan de concientización y entrenamiento formal debido a la importancia del tema del uso de las contraseñas.
223	Software de Distribucion Financiera (SDF).	25	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Realizar revisiones periódicas a los registros y determinar un política de almacenamiento que detalle los términos y responsabilidades, así como los mecanismos de seguridad para tales registros. 2. Los registros de los sistemas de monitoreo deben ser revisados periódicamente en busca de mejoras en su implementación y uso. 3. El acceso a los registros debe ser exclusivo para los auditores, administradores de la plataforma y oficial de seguridad. Estos registros deben estar asegurados en un sistema de archivos protegido.

224	Software de Distribucion Financiera (SDF).	25	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. Incluír el proceso en el SGSI cuando haya sido implementado en la terminación de contratos. 2. Debe establecerse un procedimiento formal y consistente dentro del SGSI para la eliminación de los derechos de acceso cuando las personas se retiren.
225	Software de Distribucion Financiera (SDF).	25	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
226	Conciliaciones.	16	A.11.2.1 Ubicación y protección del equipo	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
227	Conciliaciones.	16	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
228	Conciliaciones.	16	A.8.2.3 Manejo de activos	1. Implementar permisos a nivel de uso de las aplicaciones del sistema. Extender las restricciones en el dominio para todos los usuarios finales. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
229	Archivos de Recaudo Externo	20	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
230	Archivos de Recaudo Externo	20	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Implementar permisos a nivel de uso de las aplicaciones del sistema. Extender las restricciones en el dominio para todos los usuarios finales. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
231	Actualizaciones SDF	20	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los	1. Realizar el plan de concientización y entrenamiento formal debido a la

			derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	importancia del tema del uso de las contraseñas.
232	Actualizaciones SDF	20	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	1. Realizar revisiones periódicas a los registros y determinar un política de almacenamiento que detalle los términos y responsabilidades, así como los mecanismos de seguridad para tales registros. 2. Los registros de los sistemas de monitoreo deben ser revisados periódicamente en busca de mejoras en su implementación y uso. 3. El acceso a los registros debe ser exclusivo para los auditores, administradores de la plataforma y oficial de seguridad. Estos registros deben estar asegurados en un sistema de archivos protegido.
233	Actualizaciones SDF	20	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Incluír el proceso en el SGSI cuando haya sido implementado en la terminación de contratos. 2. Debe establecerse un procedimiento formal y consistente dentro del SGSI para la eliminación de los derechos de acceso cuando las personas se retiren.
234	Actualizaciones SDF	20	A.7.3.1 Terminación o cambio de responsabilidades de empleo A.9.2.6 Retiro o ajuste de los derechos de acceso	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
235	Actualizaciones SDF	20	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
236	Actualizaciones SDF	20	A.9.3.1 Uso de información secreta de autenticación	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar

				acciones para las cuales está autorizado.
237	Actualizaciones SDF	20	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Implementar permisos a nivel de uso de las aplicaciones del sistema. Extender las restricciones en el dominio para todos los usuarios finales. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
238	Actualizaciones SDF	20	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
239	Actualizaciones SDF	20	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria.
240	Actualizaciones SDF	20	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. La información de contingencias de respaldo de personal crítico debe mantener un esquema estructural, para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
241	Actualizaciones SDF	20	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.

242	Actualizaciones SDF	20	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado. 2. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso.
243	Actualizaciones SDF	20	A.7.3.1 Terminación o cambio de responsabilidades de empleo A.9.2.6 Retiro o ajuste de los derechos de acceso	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
244	Actualizaciones SDF	20	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Mantener un esquema para luego ser monitoreado por el responsable. 2. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior.
245	Actualizaciones SDF	20	A.9.3.1 Uso de información secreta de autenticación	1. Una vez establecida e implementada la política de seguridad, realizar los controles al cumplimiento de la misma.
246	Actualizaciones SDF	20	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
247	Actualizaciones SDF	20	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. Se debe mantener el esquema de contratos de mantenimiento constantes sobre los equipos tecnológicos. 2. Este esquema debe revisarse y monitorearse constantemente para corregir posibles fallas en los controles.

248	Actualizaciones SDF	20	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado. 2. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso.
249	Bases de datos (sistema de distribución de transferencias)	25	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. Mantener un esquema para luego ser monitoreado por el responsable. 2. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior.
250	Bases de datos (sistema de distribución de transferencias)	25	A.6.1.2 Separación de deberes	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
251	Bases de datos (sistema de distribución de transferencias)	25	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado.
252	Bases de datos (sistema de distribución de transferencias)	25	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Establecer procedimientos especiales de seguridad para los registros organizacionales de clasificación ultra-secreta.

253	Bases de datos (sistema de distribución de transferencias)	25	A.9.3.1 Uso de información secreta de autenticación	1. Mantener un esquema para luego ser monitoreado por el responsable. 2. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior.
254	Certificaciones.	13	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.3 Seguridad de oficinas, recintos e instalaciones A.11.1.6 Áreas de despacho y carga	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
255	Certificaciones.	13	A.18.2.2 Cumplimiento de las políticas y normas de seguridad	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado.
256	Certificaciones.	13	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. Establecer procedimientos especiales de seguridad para los registros organizacionales de clasificación ultra-secreta.
257	Certificaciones.	13	A.11.2.4 Mantenimiento de los equipos A.11.2.5 Retiro de activos	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
258	Certificaciones.	13	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Documentar todos los controles de protección contra amenazas externas, juntar los del edificio con los que tiene definidos TI para el centro de datos y periféricos.

259	Gastos de personal	16	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
260	Gastos de personal	16	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Los manuales deben incluír procedimientos contingentes del área, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI.
261	Gastos de personal	16	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información	1. Los manuales deben incluír procedimientos contingentes del área, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI.
262	Gastos de personal	16	A.18.1.3 Protección de registros	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
263	Planes de acción.	15	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI
264	Planes de acción.	15	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
265	Planes de acción.	15	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información	1. Los manuales deben incluír procedimientos contingentes del área, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI.
266	Planes de acción.	15	A.18.1.3 Protección de registros	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma

				adecuada del manejo de la información.
267	Planes de acción.	15	A.18.1.3 Protección de registros	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI
268	Planes de acción.	15	A.11.1.4 Protección contra amenazas externas y ambientales.	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
269	Planes de acción.	15	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. Los manuales deben incluír procedimientos contingentes del área, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI.
270	Planes de acción.	15	A.12.1.1 Procedimientos de operación documentados	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
271	Seguimiento de Contratos Gremial	25	A.12.1.1 Procedimientos de operación documentados	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI
272	Seguimiento de Contratos Gremial	25	A.8.2.3 Manejo de activos	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.

273	Seguimiento de Contratos Gremial	25	A.12.1.1 Procedimientos de operación documentados	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado.
274	Seguimiento de Contratos Gremial	25	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
275	Inventario y movimientos de Almacén	20	A.12.1.1 Procedimientos de operación documentados	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
276	Inventario y movimientos de Almacén	20	A.8.2.3 Manejo de activos	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado.
277	Inventario y movimientos de Almacén	20	A.12.1.1 Procedimientos de operación documentados	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.

278	Inventario y movimientos de Almacén	20	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
279	Listas de asistencia de los procesos relacionados a gestión humana (inducciòn, socializaciones, actividades, capacitaciones) FÍSICOS	15	A.12.1.1 Procedimientos de operación documentados	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
280	Listas de asistencia de los procesos relacionados a gestión humana (inducciòn, socializaciones, actividades, capacitaciones) FÍSICOS	15	A.8.2.3 Manejo de activos	1. Realizar el plan de concientización, el entrenamiento adecuado a los usuarios y la campaña completa de divulgación del SGSI.

281	Listas de asistencia de los procesos relacionados a gestión humana (inducciòn, socializaciones, actividades, capacitaciones) FÍSICOS	15	A.12.1.1 Procedimientos de operación documentados	1. Realizar el plan de concientización, el entrenamiento adecuado a los usuarios y la campaña completa de divulgación del SGSI.
282	Listas de asistencia de los procesos relacionados a gestión humana (inducciòn, socializaciones, actividades, capacitaciones) FÍSICOS	15	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
283	Chip (consolidado de información de la contaduría general de la nación)	17	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información	1.incluír el detalle de procesos disciplinarios y descargos, dentro del manual de funciones y en el SGSI

284	Chip (consolidado de información de la contaduría general de la nación)	17	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1.incluír el detalle de procesos disciplinarios y descargos, dentro del manual de funciones y en el SGSI
285	Chip (consolidado de información de la contaduría general de la nación)	17	A.8.2.3 Manejo de activos	1. Incluír el proceso en el SGSI cuando haya sido implementado en la terminación de contratos.
286	Chip (consolidado de información de la contaduría general de la nación)	17	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
287	Chip (consolidado de información de la contaduría general de la nación)	17	A.8.2.3 Manejo de activos	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado. 2. Se debe aprender de las auditorías realizadas a los contratos de los terceros y revisar los controles implementados para cada contrato con el fin de mejorar en el siguiente ciclo del SGSI.
288	Chip (consolidado de información de la contaduría general de la nación)	17	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.

289	Mesa de ayuda.	18	A.7.2.1 Responsabilidades de la Dirección A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información A.7.2.3 Proceso disciplinario	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
290	Mesa de ayuda.	18	A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
291	Mesa de ayuda.	18	A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información	1. Este esquema de controles en el traslado de dispositivos debe revisarse y monitorearse constantemente para corregir posibles fallas en los controles establecidos.
292	Mesa de ayuda.	18	A.7.2.1 Responsabilidades de la Dirección A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información A.7.2.3 Proceso disciplinario	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
293	Mesa de ayuda.	18	A.7.2.1 Responsabilidades de la Dirección A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información A.7.2.3 Proceso disciplinario	1. Mantener un esquema para luego ser monitoreado por el responsable. 2. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior.
294	Mesa de ayuda.	18	A.7.2.1 Responsabilidades de la Dirección A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información A.7.2.3 Proceso disciplinario	1. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado. 2. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso.
295	Mesa de ayuda.	18	A.7.3.1 Terminación o cambio de responsabilidades de empleo	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.

296	Mesa de ayuda.	18	A.7.2.1 Responsabilidades de la Dirección A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información A.7.2.3 Proceso disciplinario	1. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado. 2. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso.
297	Tesorería.	23	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Mantener un esquema para luego ser monitoreado por el responsable. 2. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior.
298	Tesorería.	23	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado. 2. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso.
299	Tesorería.	23	A.8.2.3 Manejo de activos	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
300	Tesorería.	23	A.9.3.1 Uso de información secreta de autenticación	1. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado. 2. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso.

301	Tesorería.	23	A.11.2.5 Retiro de activos	1. Realizar el plan de concientización y entrenamiento formal debido a la importancia del tema.
302	Tesorería.	23	A.8.2.3 Manejo de activos	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
303	Informes a Dian	18	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.3 Seguridad de oficinas, recintos e instalaciones	1. Realizar el plan de concientización y entrenamiento formal debido a la importancia del tema.
304	Informes a Dian	18	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
305	Informes a Dian	18	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Realizar el plan de concientización y entrenamiento formal debido a la importancia del tema.
306	Informes a Dian	18	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
307	Secretaria de hacienda distrital.	15	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.3 Seguridad de oficinas, recintos e instalaciones	1. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria.

308	Secretaria de hacienda distrital.	15	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Documentar todos los controles de protección contra amenazas externas, juntar los del edificio con los que tiene definidos TI para el centro de datos y periféricos.
309	Secretaria de hacienda distrital.	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
310	Secretaria de hacienda distrital.	15	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
311	Firma digital certicámara	25	A.9.3.1 Uso de información secreta de autenticación	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
312	Firma digital certicámara	25	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Este esquema de controles en el traslado de dispositivos debe revisarse y monitorearse constantemente para corregir posibles fallas en los controles establecidos.
313	Firma digital Dian	25	A.9.3.1 Uso de información secreta de autenticación	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado. 2. Se debe aprender de las auditorías realizadas a los contratos de los terceros y revisar los controles implementados para

				cada contrato con el fin de mejorar en el siguiente ciclo del SGSI.
314	Firma digital Dian	25	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
315	Firma Escaneadas Directores	25	A.9.3.1 Uso de información secreta de autenticación	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
316	Firma Escaneadas Directores	25	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
317	Documentos de soporte de contratos de Interventoría a concesiones	15	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado.
318	Documentos de soporte de contratos de Interventoría a concesiones	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Incluír el proceso de comunicación entre talento humano y la Dirección de Sistemas con respecto a la salida de personal o termino de contrato en el SGSI.

319	Documentos de soporte de contratos de Interventoría a concesiones	15	A.8.2.3 Manejo de activos	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI
320	Documentos de soporte de contratos de Interventoría a concesiones	15	A.9.3.1 Uso de información secreta de autenticación	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
321	Documentos de soporte de contratos de Interventoría a concesiones	15	A.8.2.3 Manejo de activos	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
322	Documentos de soporte de contratos de Interventoría a concesiones	15	A.11.2.5 Retiro de activos	1. Implementar un estándar de desarrollo seguro de aplicaciones que cumpla con las políticas específicas de seguridad, en la revisión de entradas, procesamiento y salidas de información.
323	Capitulo de Autoridades de Tránsito	15	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar

				acciones para las cuales está autorizado.
324	Capitulo de Autoridades de Tránsito	15	A.8.2.3 Manejo de activos	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
325	Capitulo de Autoridades de Tránsito	15	A.8.2.3 Manejo de activos	1. Realizar el plan de concientización y entrenamiento formal debido a la importancia del tema relacionado con las contraseñas del sistema.
326	Capitulo de Autoridades de Tránsito	15	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1. Realizar las revisiones periódicas de auditoria el el sistemas de informción, definir el procedimieto de monitoreo y su relación con el de reacción a incidentes. Logs de auditoría de la actividad de administradores y operadores habilitados. 2. Procedimiento de documentación de fallas reportadas por usuarios o por programas del sistema relacionadas con los sistemas de comunicación de procesamiento de la información. Política de manejo de fallas reportadas aprobada y divulgada.
327	Capitulo de Autoridades de Tránsito	15	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
328	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	20	A.7.3.1 Terminación o cambio de responsabilidades de empleo A.9.2.6 Retiro o ajuste de los derechos de acceso	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.

329	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	20	A.12.1.1 Procedimientos de operación documentados A.12.1.2 Gestión de cambios A.14.2.2 Procedimientos de control de cambios en sistemas	1. Realizar las revisiones periódicas de auditoria el el sistemas de informción, definir el procedimieto de monitoreo y su relación con el de reacción a incidentes. Logs de auditoría de la actividad de administradores y operadores habilitados. 2. Procedimiento de documentación de fallas reportadas por usuarios o por programas del sistema relacionadas con los sistemas de comunicación de procesamiento de la información. Política de manejo de fallas reportadas aprobada y divulgada.
330	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	20	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI
331	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	20	A.9.3.1 Uso de información secreta de autenticación	1. Implementar un estándar de desarrollo seguro de aplicaciones que cumpla con las políticas específicas de seguridad, en la revisión de entradas, procesamiento y salidas de información.

332	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	20	A.18.1.3 Protección de registros	1. Mantener un esquema para luego ser monitoreado por el responsable. 2. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior.
333	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	20	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
334	Contratos de concesiones (Documentos de soporte de contratos de Interventoría a concesiones)	20	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado.

335	Directorio de Autoridades de Tránsito	20	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	1. Establecer procedimientos especiales de seguridad para los registros organizacionales de clasificación ultra-secreta.
336	Directorio de Autoridades de Tránsito	20	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
337	Directorio de Autoridades de Tránsito	20	A.9.3.1 Uso de información secreta de autenticación	1. Documentar todos los controles de protección contra amenazas externas, juntar los del edificio con los que tiene definidos TI para el centro de datos y periféricos.
338	Directorio de Autoridades de Tránsito	20	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Implementar permisos a nivel de uso de las aplicaciones del sistema. Extender las restricciones en el dominio para todos los usuarios finales. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
339	Directorio de Autoridades de Tránsito	20	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Realizar el plan de concientización y entrenamiento formal debido a la importancia del tema del uso de las contraseñas.
340	Directorio de Autoridades de Tránsito	20	A.12.1.1 Procedimientos de operación documentados A.12.1.2 Gestión de cambios A.14.2.2 Procedimientos de control de cambios en sistemas	1. Realizar revisiones periódicas a los registros y determinar un política de almacenamiento que detalle los términos y responsabilidades, así como los mecanismos de seguridad para tales registros. 2. Los registros de los sistemas de monitoreo deben ser revisados periódicamente en busca de mejoras en su implementación y uso. 3. El acceso a los registros debe ser exclusivo para los auditores, administradores de la plataforma y oficial de seguridad. Estos registros deben estar asegurados en un sistema de archivos protegido.

341	Directorio de Autoridades de Tránsito	20	A.12.1.1 Procedimientos de operación documentados A.12.1.2 Gestión de cambios A.14.2.2 Procedimientos de control de cambios en sistemas	1. Incluír el proceso en el SGSI cuando haya sido implementado en la terminación de contratos. 2. Debe establecerse un procedimiento formal y consistente dentro del SGSI para la eliminación de los derechos de acceso cuando las personas se retiren.
342	Soporte a Capacitación	16	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
343	Soporte a Capacitación	16	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
344	Soporte a Capacitación	16	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
345	Soporte a Capacitación	16	A.18.1.3 Protección de registros	1. Implementar permisos a nivel de uso de las aplicaciones del sistema. Extender las restricciones en el dominio para todos los usuarios finales. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
346	Soporte a Capacitación	16	A.18.1.3 Protección de registros	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
347	Soporte a Capacitación	16	A.11.1.4 Protección contra amenazas externas y ambientales.	1. Implementar permisos a nivel de uso de las aplicaciones del sistema. Extender las restricciones en el dominio para todos los usuarios finales. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.

348	Carpeta de servicios simit.	22	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. Realizar el plan de concientización y entrenamiento formal debido a la importancia del tema del uso de las contraseñas.
349	Carpeta de servicios simit.	22	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	1. Realizar revisiones periódicas a los registros y determinar un política de almacenamiento que detalle los términos y responsabilidades, así como los mecanismos de seguridad para tales registros. 2. Los registros de los sistemas de monitoreo deben ser revisados periódicamente en busca de mejoras en su implementación y uso. 3. El acceso a los registros debe ser exclusivo para los auditores, administradores de la plataforma y oficial de seguridad. Estos registros deben estar asegurados en un sistema de archivos protegido.
350	Carpeta de servicios simit.	22	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Incluír el proceso en el SGSI cuando haya sido implementado en la terminación de contratos. 2. Debe establecerse un procedimiento formal y consistente dentro del SGSI para la eliminación de los derechos de acceso cuando las personas se retiren.
351	Carpeta de servicios simit.	22	A.7.3.1 Terminación o cambio de responsabilidades de empleo A.9.2.6 Retiro o ajuste de los derechos de acceso	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
352	Carpeta de servicios simit.	22	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
353	Carpeta de servicios simit.	22	A.9.3.1 Uso de información secreta de autenticación	1. Implementar permisos a nivel de uso de las aplicaciones del sistema. Extender las restricciones en el dominio para todos los usuarios

				finales. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
354	Carpeta de servicios simit.	22	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
355	Carpeta de servicios simit.	22	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado. 2. Se debe aprender de las auditorías realizadas a los contratos de los terceros y revisar los controles implementados para cada contrato con el fin de mejorar en el siguiente ciclo del SGSI.
356	Carpeta de servicios simit.	22	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
357	Carpeta de servicios simit.	22	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
358	Carpeta de servicios simit.	22	A.9.1.1 Política de control de acceso A.9.3.1 Uso de información secreta de autenticación	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
359	Carpeta de servicios simit.	22	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.

			actividades de los administradores y operadores	
360	Carpeta de servicios simit.	22	A.7.3.1 Terminación o cambio de responsabilidades de empleo A.9.2.6 Retiro o ajuste de los derechos de acceso	1. Este esquema de controles en el traslado de dispositivos debe revisarse y monitorearse constantemente para corregir posibles fallas en los controles establecidos.
361	Banco de Proyectos (Proyectos)	20	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado. 2. Se debe aprender de las auditorías realizadas a los contratos de los terceros y revisar los controles implementados para cada contrato con el fin de mejorar en el siguiente ciclo del SGSI.
362	Política pública.	16	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Implementar auditorías a todos los procesos solicitándo la información de responsabilidades a los recién contratados.
363	Pagos especiales.	23	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario A.9.4.4 Uso de programas utilitarios privilegiados	#N/A
364	Manuales de operación no concesionada.	18	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
365	Soportes de pago (transferencias).	20	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar

				acciones para las cuales está autorizado.
366	Soportes de pago (transferencias).	20	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
367	Soportes de pago (transferencias).	20	A.8.2.3 Manejo de activos	1. La información debe mantener un esquema estructural para que los sistemas de información funcionen segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
368	Soportes de pago (transferencias).	20	A.9.3.1 Uso de información secreta de autenticación	1. Los controles y protección de los datos deben ser iguales tanto para producción como para desarrollo y pruebas dado que son los mismos. El SGSI debería incluír lineamientos de manejo de los datos en Desarrollo y Pruebas con respecto a la confidencialidad de la información. 2. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios.
369	Soportes de pago (transferencias).	20	A.8.2.3 Manejo de activos	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
370	Soportes de pago (transferencias).	20	A.11.2.5 Retiro de activos	1. La información del rol debe mantener un esquema estructural para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.

371	Soportes de pago (transferencias).	20	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Implementar auditorías a todos los procesos solicitándo la información de responsabilidades a los recién contratados.
372	Logística de eventos (FCM - SIMIT).	15	A.7.1.2 Términos y condiciones de empleo A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información	1. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado. 2. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso.
373	Logística de eventos (FCM - SIMIT).	15	A.7.1.2 Términos y condiciones de empleo A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información	1. Mantener un esquema para luego ser monitoreado por el responsable. 2. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior.
374	Logística de eventos (FCM - SIMIT).	15	A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información	1. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado. 2. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso.
375	Logística de eventos (FCM - SIMIT).	15	A.7.2.1 Responsabilidades de la Dirección A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información A.7.2.3 Proceso disciplinario	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
376	Bases de datos logística y proveedores.	15	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario	1. Este esquema de controles en el traslado de dispositivos debe revisarse y monitorearse constantemente para corregir posibles fallas en los controles establecidos.

			A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	
377	Bases de datos logística y proveedores.	15	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
378	Bases de datos logística y proveedores.	15	A.12.1.2 Gestión de cambios A.6.1.2 Separación de deberes A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Documentar todos los controles de protección contra amenazas externas, juntar los del edificio con los que tiene definidos TI para el centro de datos y periféricos.
379	Bases de datos logística y proveedores.	15	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI
380	Bases de datos logística y proveedores.	15	A.6.1.2 Separación de deberes A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Diseñar e implemetnar el procedimiento detallado de recolección de evidencia que permita de forma efectiva obtener toda la información necesaria y conscientizar a los usuarios del impacto que puede tener un incidente y las demoras que representaría en su trabajo para la toma de evidencias.
381	Bases de datos logística y proveedores.	15	A.7.1.2 Términos y condiciones de empleo A.7.2.2 Toma de conciencia, educación y formacion en la seguridad de la información	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.

382	Canal de comunicaciones.	25	A.13.2.1 Políticas y procedimientos para la transferencia de información. A.13.2.2 Acuerdos sobre transferencia de información A.8.3.3 Transporte de medios físicos	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
383	Canal de comunicaciones.	25	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. La información de contingencias de respaldo de personal crítico debe mantener un esquema estructural, para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
384	Canal de comunicaciones.	25	A.11.1.4 Protección contra amenazas externas y ambientales.	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
385	Canal de comunicaciones.	25	A.12.1.1 Procedimientos de operación documentados	1. Diseñar e implemetnar el procedimiento detallado de recolección de evidencia que permita de forma efectiva obtener toda la información necesaria y conscientizar a los usuarios del impacto que puede tener un incidente y las demoras que representaría en su trabajo para la toma de evidencias.
386	Canal de comunicaciones.	25	A.16.1.1 Responsabilidades y procedimientos A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información A.16.1.7 Recolección de evidencia	1. Realizar revisiones periódicas a los registros y determinar un política de almacenamiento que detalle los términos y responsabilidades, así como los mecanismos de seguridad para tales registros. 2. Los registros de los sistemas de monitoreo deben ser revisados periódicamente en busca de mejoras en su implementación y uso. 3. El acceso a los registros debe ser exclusivo para los auditores, administradores de la plataforma y oficial de seguridad. Estos registros deben estar asegurados en un sistema de archivos protegido.
387	Base de datos de desarrollo.	23	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y

			usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
388	Base de datos de desarrollo.	23	A.6.1.2 Separación de deberes	1. La información de contingencias de respaldo de personal crítico debe mantener un esquema estructural, para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
389	Base de datos de desarrollo.	23	A.9.3.1 Uso de información secreta de autenticación	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
390	Base de datos de desarrollo.	23	A.16.1.1 Responsabilidades y procedimientos A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información A.16.1.7 Recolección de evidencia	1. Diseñar e implemetnar el procedimiento detallado de recolección de evidencia que permita de forma efectiva obtener toda la información necesaria y conscientizar a los usuarios del impacto que puede tener un incidente y las demoras que representaría en su trabajo para la toma de evidencias.
391	Base de datos de desarrollo.	23	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Realizar revisiones periódicas a los registros y determinar un política de almacenamiento que detalle los términos y responsabilidades, así como los mecanismos de seguridad para tales registros. 2. Los registros de los sistemas de monitoreo deben ser revisados periódicamente en busca de mejoras en su implementación y uso. 3. El acceso a los registros debe ser exclusivo para los auditores, administradores de la plataforma y oficial de seguridad. Estos registros deben estar asegurados en un sistema de archivos protegido.
392	Base de datos de pruebas.	23	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido	1. Mantener un esquema para luego ser monitoreado por el responsable. 2. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior.

			A.11.2.9 Política escritorio limpio y pantalla limpia	
393	Base de datos de pruebas.	23	A.6.1.2 Separación de deberes	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
394	Base de datos de pruebas.	23	A.9.3.1 Uso de información secreta de autenticación	1. Se debe fortalecer el esquema de manejo de tipos de información, estableciendo dentro del SGSI y en una política formal, la forma adecuada del manejo de la información.
395	Base de datos de pruebas.	23	A.16.1.1 Responsabilidades y procedimientos A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información A.16.1.7 Recolección de evidencia	1. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso. 2. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado.
396	Base de datos de pruebas.	23	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior. 2. Mantener un esquema para luego ser monitoreado por el responsable.
397	Base de datos producción.	25	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Incluír en el SGSI una política y procedimientos claros del intercambio seguro de información 2. El manejo de información y su intercambio con terceros debería incluír acuerdos sobre su transporte y almacenamiento seguros al tratar y manipular la información (por ejemplo comprimir y cifrar la información).
398	Base de datos producción.	25	A.6.1.2 Separación de deberes	1. Además de tipificar esta labor como parte de las actividades de un oficial de seguridad, definir el procedimiento adecuado en el SGSI y realizar la revisión a todos los repotes de incidentes e incluírlos en el plan de mejoramiento.

399	Base de datos producción.	25	A.9.3.1 Uso de información secreta de autenticación	1. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas.
400	Base de datos producción.	25	A.16.1.1 Responsabilidades y procedimientos A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información A.16.1.7 Recolección de evidencia	1. Diseñar e implemetnar el procedimiento detallado de recolección de evidencia que permita de forma efectiva obtener toda la información necesaria y conscientizar a los usuarios del impacto que puede tener un incidente y las demoras que representaría en su trabajo para la toma de evidencias.
401	Base de datos producción.	25	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Realizar las revisiones periódicas, definir el procedimieto de monitoreo y su relación con el de reacción a incidentes. Logs de auditoría de la actividad de administradores y operadores habilitados.
402	Backups base de datos simit.	25	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
403	Backups base de datos simit.	25	A.8.2.3 Manejo de activos	1. Mantiener esta politica y sociabilizarla al grupo de usuarios.
404	Backups base de datos simit.	25	A.18.1.3 Protección de registros	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI
405	Backups base de datos simit.	25	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
406	Backups base de datos simit.	25	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico	1. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria.

			A.11.1.6 Áreas de despacho y carga	
407	Backups base de datos simit.	25	A.13.2.1 Políticas y procedimientos para la transferencia de información. A.13.2.2 Acuerdos sobre transferencia de información A.8.3.3 Transporte de medios físicos	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI
408	Servidores store wise.	22	A.16.1.1 Responsabilidades y procedimientos A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información A.16.1.7 Recolección de evidencia	1. Se debe replantear la arquitectura de seguridad en la red LAN (desde el punto de vista de correlación de eventos y monitoreo de seguridad), para ubicar y configurar correctamente todos los elementos de seguridad y monitoreo en la red. Esto debe estar acompañado de una política de seguridad en el SGSI
409	Servidores store wise.	22	A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.3.1 Uso de información secreta de autenticación	1. Debe reforzarse el esquema estableciendo una directiva explicita o una política dentro del SGSI que requiera la protección y ubicación de los equipos tecnológicos en areas protegidas.
410	Servidores store wise.	22	A.16.1.1 Responsabilidades y procedimientos A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información A.16.1.7 Recolección de evidencia	1. El esquema de manejo de la información debe estar apoyado por un SGSI consistente a lo largo de toda la organización y respetarse de esta manera las normas de manejo de la información usando el etiquetado. 2. Las normas de clasificación son claramente inexistentes. Se debe madurar el etiquetado y manejo de las clasificaciones de acuerdo a características y patrones en la información manejada por cada proceso.
411	Servidores store wise.	22	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
412	Servidores store wise.	22	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información	1. La información de contingencias de respaldo de personal crítico debe mantener un esquema estructural, para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar

			secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	acciones para las cuales está autorizado.
413	Servidores store wise.	22	A.12.3.1 Respaldo de la información	1. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas.
414	Servidores store wise.	22	A.12.1.1 Procedimientos de operación documentados	1. Diseñar e implemetnar el procedimiento detallado de recolección de evidencia que permita de forma efectiva obtener toda la información necesaria y conscientizar a los usuarios del impacto que puede tener un incidente y las demoras que representaría en su trabajo para la toma de evidencias.
415	Servidores store wise.	22	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. Realizar las revisiones periódicas, definir el procedimieto de monitoreo y su relación con el de reacción a incidentes. Logs de auditoría de la actividad de administradores y operadores habilitados.
416	Firewall.	22	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
417	Firewall.	22	A.12.1.1 Procedimientos de operación documentados A.12.1.2 Gestión de cambios	1. Mantiener esta politica y sociabilizarla al grupo de usuarios.
418	Firewall.	22	A.13.1.1 Controles de red	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI

419	Firewall.	22	A.11.2.1 Ubicación y protección del equipo A.11.2.3 Seguridad del cableado	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
420	Firewall.	22	A.8.2.1 Clasificación de la información A.8.2.2 Etiquetado de la información A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.5 Revisión de los derechos de acceso de usuario	1. Mantener un esquema para luego ser monitoreado por el responsable. 2. Incluír la descripción de las precauciones de seguridad en oficinas en el SGSI. Algunas áreas son visibles desde el exterior.
421	Firewall.	22	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Este esquema de controles en el traslado de dispositivos debe revisarse y monitorearse constantemente para corregir posibles fallas en los controles establecidos.
422	Firewall.	22	A.6.1.2 Separación de deberes	1. Este esquema de controles en el traslado de dispositivos debe revisarse y monitorearse constantemente para corregir posibles fallas en los controles establecidos.
423	Datacenter.	25	A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.3.1 Uso de información secreta de autenticación	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
424	Datacenter.	25	A.16.1.1 Responsabilidades y procedimientos A.16.1.6 Aprendizaje obtenido de los incidentes de	1. Documentar todos los controles de protección contra amenazas externas, juntar los del edificio con

			seguridad de la información A.16.1.7 Recolección de evidencia	los que tiene definidos TI para el centro de datos y periféricos.
425	Datacenter.	25	A.12.4.1 Registro de evento A.12.4.2 Protección de la información de registro A.12.4.3 Registro de las actividades de los administradores y operadores	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI
426	Datacenter.	25	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Diseñar e implemetnar el procedimiento detallado de recolección de evidencia que permita de forma efectiva obtener toda la información necesaria y conscientizar a los usuarios del impacto que puede tener un incidente y las demoras que representaría en su trabajo para la toma de evidencias.
427	Datacenter.	25	A.12.3.1 Respaldo de la información	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI
428	Datacenter.	25	A.12.1.1 Procedimientos de operación documentados	1. Los manuales deben incluír procedimientos contingentes del áera, así como las actividades en casos de emergencia. Todo debe estar alineado o incluído en el SGSI
429	Datacenter.	25	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. Diseñar un simulacro de recuperación de un sistema de información que haya impactado la integridad o confidencialidad de la información. 2. Una vez afinados y probados los planes de continuidad, realizar la divulgación e implementación respectiva y obligatoria. 3. Realizar el seguimiento y revisión apropiados a los planes de continuidad una vez hayan sido implementados, puestos a prueba o en simulacro.
430	UPS.	13	A.11.1.1 Perímetro de seguridad física A.11.1.2 Controles de acceso físico A.11.1.3 Seguridad de oficinas, recintos e instalaciones A.11.1.6 Áreas de despacho y carga	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.

431	UPS.	13	A.11.2.5 Retiro de activos	1. La información de contingencias de respaldo de personal crítico debe mantener un esquema estructural, para que los sistemas de información funcionen de manera segura y coordinadamente. Se requiere al menos un control técnico especial que impida a un rol ejecutar acciones para las cuales está autorizado.
432	VPN site to site.	25	A.13.2.1 Políticas y procedimientos para la transferencia de información. A.13.2.2 Acuerdos sobre transferencia de información A.8.3.3 Transporte de medios físicos	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
433	VPN site to site.	25	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. Diseñar e implemetnar el procedimiento detallado de recolección de evidencia que permita de forma efectiva obtener toda la información necesaria y conscientizar a los usuarios del impacto que puede tener un incidente y las demoras que representaría en su trabajo para la toma de evidencias.
434	VPN site to site.	25	A.11.1.4 Protección contra amenazas externas y ambientales.	1. Realizar revisiones periódicas a los registros y determinar un política de almacenamiento que detalle los términos y responsabilidades, así como los mecanismos de seguridad para tales registros. 2. Los registros de los sistemas de monitoreo deben ser revisados periódicamente en busca de mejoras en su implementación y uso. 3. El acceso a los registros debe ser exclusivo para los auditores, administradores de la plataforma y oficial de seguridad. Estos registros deben estar asegurados en un sistema de archivos protegido.
435	VPN site to site.	25	A.12.1.1 Procedimientos de operación documentados	1. Realizar el plan de concientización y entrenamiento formal debido a la importancia del tema relacionado con las contraseñas del sistema.
436	VPN site to site.	25	A.16.1.1 Responsabilidades y procedimientos A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información A.16.1.7 Recolección de evidencia	1. Realizar las revisiones periódicas de auditoria el el sistemas de informción, definir el procedimieto de monitoreo y su relación con el de reacción a incidentes. Logs de auditoría de la actividad de administradores y operadores habilitados. 2. Procedimiento de documentación de fallas reportadas por usuarios o por programas del

				sistema relacionadas con los sistemas de comunicación de procesamiento de la información. Política de manejo de fallas reportadas aprobada y divulgada.
437	Switch core.	20	A.12.1.1 Procedimientos de operación documentados	Realizar el plan de concientización y entrenamiento formal debido a la importancia del prestamo de usuarios y contraseñas.
438	Switch core.	20	A.12.1.1 Procedimientos de operación documentados	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.
439	Switch core.	20	A.17.1.2 Implementación de la continuidad de seguridad de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	1. Implementar auditorías a todos los procesos solicitándo la información de responsabilidades a los recién contratados.
440	Bodega de Datos	25	A.9.2.3 Gestión de derechos de acceso privilegiados A.9.2.4 Gestión de información secreta de autenticación de usuarios A.9.2.5 Revisión de los derechos de acceso de usuario A.9.3.1 Uso de información secreta de autenticación A.11.2.8 Equipo de usuario desatendido A.11.2.9 Política escritorio limpio y pantalla limpia	1. Definir periodicidad y detalle del procedimiento al controlar la revisión de privilegios. 2. Documentar dentro del SGSI una política de administración de contraseñas formal que incluya manejo, almacenamiento, cambio y construcción de contraseñas. 3. Realizar el plan de concientización y entrenamiento encaminados al tema.

9. ENTREGABLES ETAPA 2

9.1 Alineacion del SGSI de la FCM al Modelo de Seguridad y Privacidad de la Información de Mintic.

El Profesional Oficial de Seguridad Informática; es el Oficial de Seguridad de la Información de la entidad, encargado de dirigir, coordinar y definir la estrategia e implementación de la Seguridad y Privacidad de la Información, con base a los lineamientos, instrumentos, artefactos y guías que dispone el programa de la Estrategia de Gobierno en Línea.

Por lo tanto, el proyecto de Inversión y Presupuesto para el Modelo de Seguridad y Privacidad de la Información, será realizado con los recursos propios de la Dirección de Tecnologías de la Información y las Comunicaciones, y demás actores de la entidad que se involucren en el desarrollo de actividades para la Implementación del Modelo de Seguridad y Privacidad de la Información en la Federación Colombiana de Municipios – Dirección Nacional Simit.

En la proactividad y eficiencia administrativa de la entidad, en el año 2017 se logran avances significativos en la implementación del Modelo de Seguridad y Privacidad de la Información que dispuso el Ministerio de las Tecnologías de la Información y las Comunicaciones, para las entidades de la administración pública; esto conforme a los lineamientos de la Estrategia de Gobierno en Línea.

Por lo anterior, se resume en alto nivel; el estado actual del Modelo de Seguridad y Privacidad de la Información en la entidad para conocer la alineación que posee actualmente el SGSI con el MSPI:

Figura 18. Alineacion SGSI al MSPI

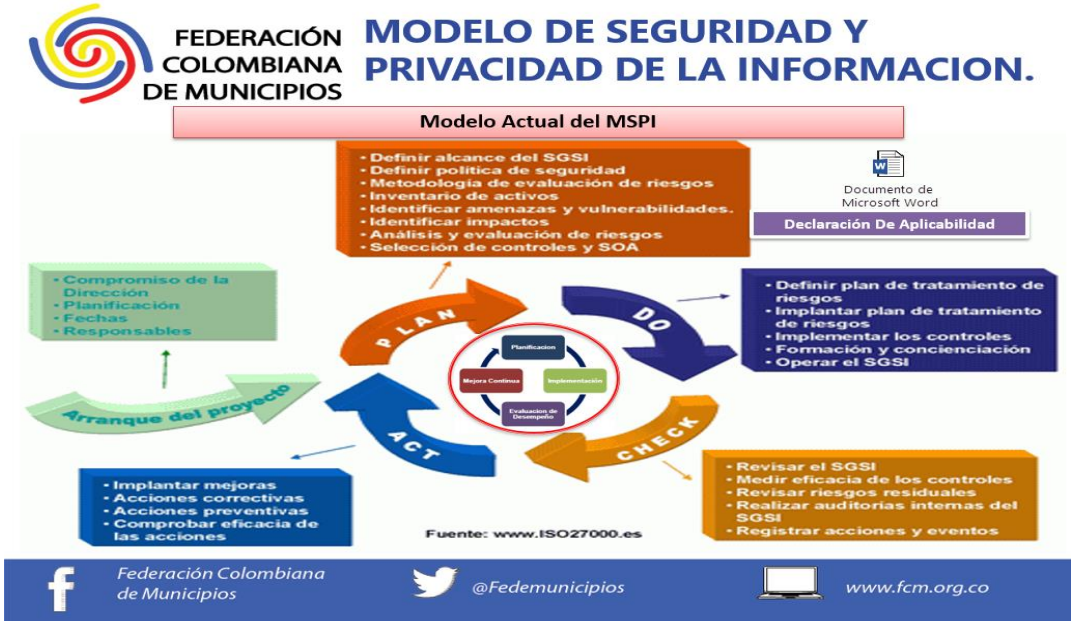
Fuente: Activos de Informacion FCM.

Como estamos y como nos proyectamos:

Figura 19. Nivel del MSPI

Fuente: Activos de Informacion FCM.

Figura 20. Modelo actual del MSPI



Fuente: Activos de Informacion FCM.

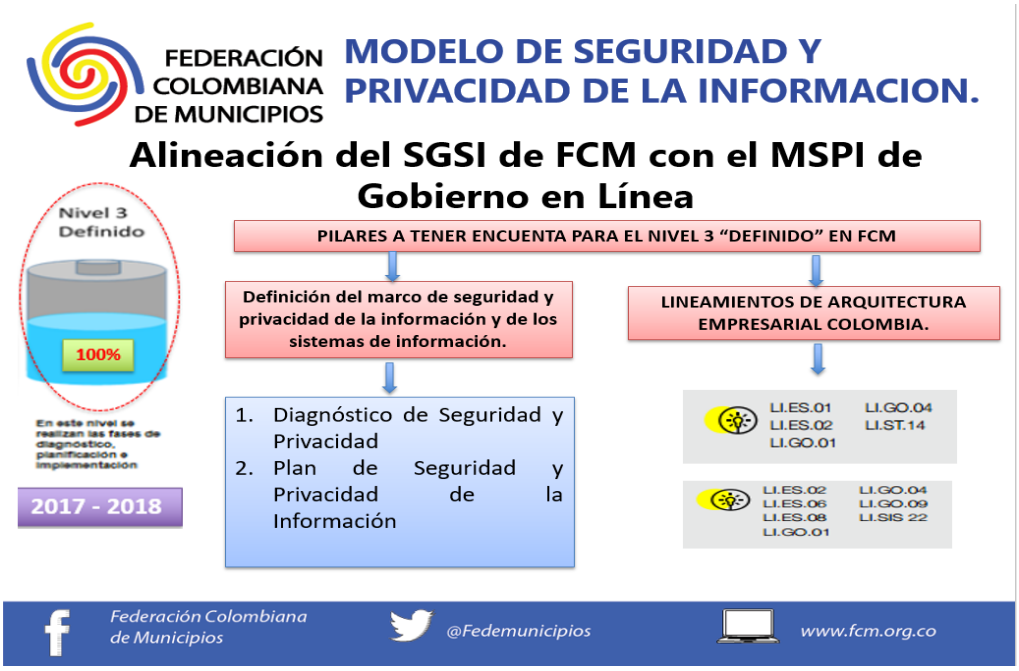
Figura 21. Modelo de Gestion de Seguridad y Privacidad de la Información.

Fuente: Activos de Informacion FCM.

Figura 22. Proyeccion del MSPI en FCM

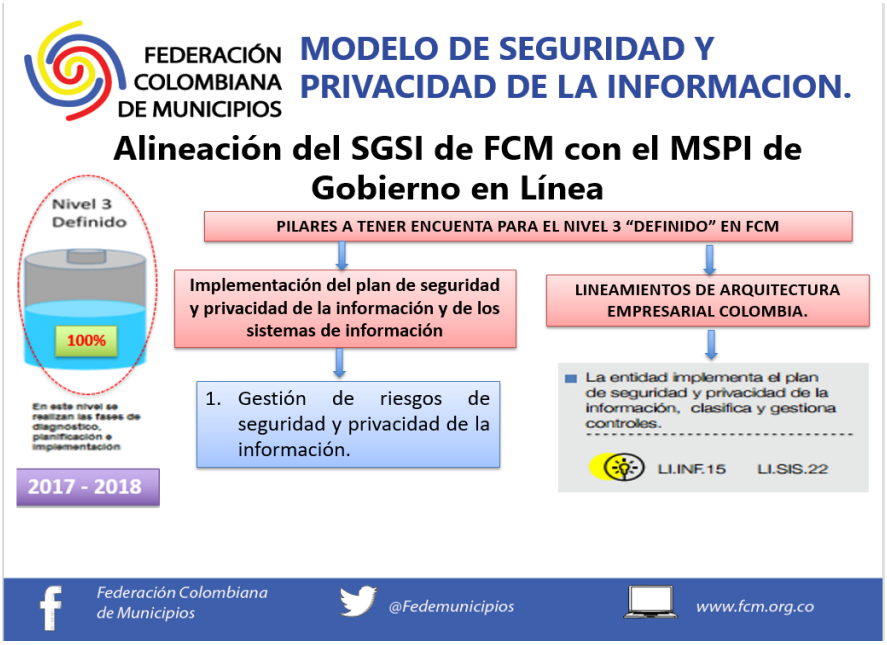
Fuente: Activos de Informacion FCM.

Figura 23. Alineacion del SGSI al MSPI de GEL



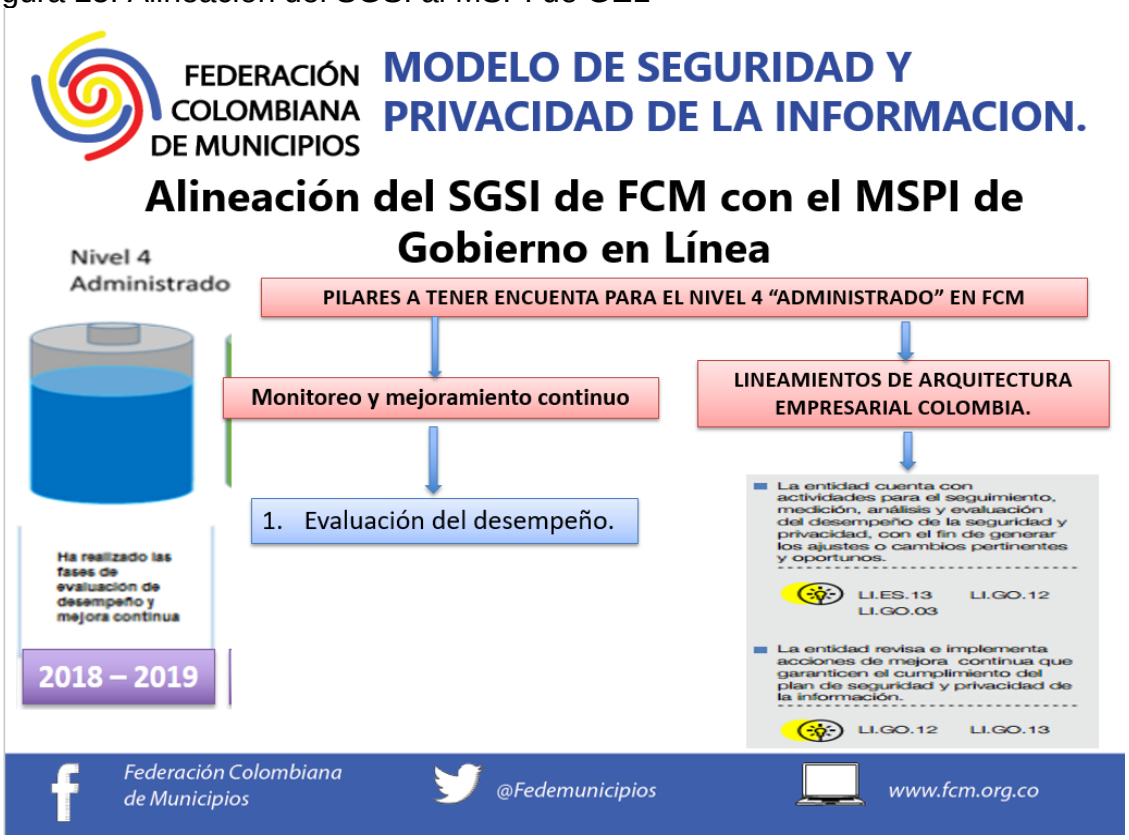
Fuente: Activos de Informacion FCM.

Figura 24. Alineacion del SGSI al MSPI de GEL



Fuente: Activos de Informacion FCM.

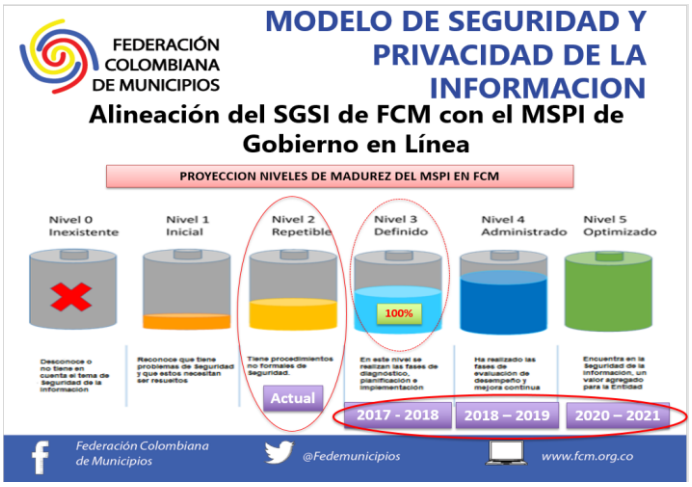
Figura 25. Alineacion del SGSI al MSPI de GEL



Fuente: Activos de Informacion FCM.

Estado Actual del Modelo de Seguridad y Privacidad de la Información, teniendo en cuenta el ejercicio y resultados obtenidos en el diseño del Sistema de Gestión de Seguridad de la Informacion según Norma ISO27001: 2013.

Figura 26. Estado Actual del SGSI al MSPI de GEL



Estado Actual: Nivel 2 (Repetible)

9.2 Plan de Implementacion para el Modelo de Seguridad y Privacidad de la Informacion

Plan de Impementacion del MSPI

En cumplimiento de lo señalado en el decreto 1078 de 2015 de la Estrategia de Gobierno en Línea.

Figura 27. Logros de Segurida y Privacidad de la Información.

Fuente: Activos de Informacion FCM.

Figura 28. Niveles de Interes.

Fuente: Activos de Informacion FCM.

COLABORADORES DEL PLAN ESTRATEGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – PESI.

Dr. Gilberto Toro Giraldo
Director Ejecutivo

Ing. Alejandro Murillo Pedroza
Director de Tecnologías de la Información y las Comunicaciones

Ing. Ronald Mauricio Cely Espitia
Profesional Oficial de Seguridad Informática

Sandra Milena Tapias Mena
Directora Dirección Nacional Simit

Juan Carlos Sepúlveda Martínez
Asesor de la Oficina de Planeación y Calidad (E)

Giomar Tatiana Forero Torres
Jefe de Control Interno de Gestión

COMITE DE GOBIERNO EN LINEA Y ANTITRAMITES

En cumplimiento de lo establecido en la resolución No. 68 de 2013 de la Federación Colombiana de Municipios; los integrantes del Comité, son:

Dr. Gilberto Toro Giraldo
Director Ejecutivo

Ing. Alejandro Murillo Pedroza
Director de Tecnologías de la Información y las Comunicaciones

Dr. Julio Cesar Freyre Sánchez
Director Jurídico

Marcela Jaramillo Suarez
Directora de Gestión Técnica

Sandra Milena Tapias Mena
Directora Dirección Nacional Simit

Dinorah Patricia Abadía Murillo
Directora Administrativa y Financiera

Giomar Tatiana Forero Torres
Jefe de Control Interno de Gestión

Giselle María Castro Vásquez
Jefe de Administración del Sistema Simit

Juan Carlos Sepúlveda Martínez
Asesor de la Oficina de Planeación y Calidad (E)

Kelly Elizabeth García Vargas
Asesor de Comunicaciones Simit (E)

COMITE DE SEGURIDAD DE LA INFORMACIÓN

En cumplimiento de lo establecido en la resolución No. 50 de 2017 de la Federación Colombiana de Municipios; los integrantes del Comité, son:

Dr. Gilberto Toro Giraldo
Director Ejecutivo

Ing. Alejandro Murillo Pedroza
Director de Tecnologías de la Información y las Comunicaciones

Ing. Ronald Mauricio Cely Espitia
Profesional Oficial de Seguridad Informática

Dr. Julio Cesar Freyre Sánchez
Director Jurídico

Marcela Jaramillo Suarez
Directora de Gestión Técnica

Sandra Milena Tapias Mena
Directora Dirección Nacional Simit,

Dinorah Patricia Abadía Murillo
Directora Administrativa y Financiera

Jiclit Edgardo Montañez Ortiz
Asesor de Servicio al Asociado y al Cliente

Sandra Milena Castro Torres
Asesor de Políticas Públicas

Giomar Tatiana Forero Torres
Jefe de Control Interno de Gestión

Juan Carlos Sepúlveda Martínez
Asesor de la Oficina de Planeación y Calidad (E)

Javier Hernando Cuesta Godoy
Asesor de Comunicaciones Estratégicas (E)

Rosa Yadira Mosquera Guerrero
Jefe de Control Interno Disciplinario

Contexto del Plan para la Implementacion del MSPI:

El Plan de Implementacion de Seguridad y Privacidad de la Información, se elaboró con la recopilación de las guías de seguridad y privacidad de la información del programa de la Estrategia de Gobierno en Línea, mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL.

La Estrategia de Gobierno en Línea, liderada por la Dirección de Tecnologías de la Información y las Comunicaciones de la Federación Colombiana de Municipios – Dirección Nacional Simit, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de ofrecer servicios de tecnología con altos estándares de seguridad y privacidad de la información, de tal manera que contribuye con la construcción de un Estado más participativo, más eficiente y más transparente, hacia las autoridades de tránsito y municipios del País.

La planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Federación Colombiana de Municipios – Dirección Nacional Simit, está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos estratégicos, misionales, apoyo, control y evaluación; y el tamaño y estructura de la Entidad.

El Modelo de Seguridad y Privacidad de la Información – MSPI, en la Federación Colombiana de Municipios – Dirección Nacional Simit, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

El Modelo de Seguridad y Privacidad de la Información, en la Federación Colombiana de Municipios – Dirección Nacional Simit, se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

El Modelo de Seguridad y Privacidad de la Información, pretende facilitar la comprensión del proceso de construcción de una política de privacidad por parte de la Federación Colombiana de Municipios – Dirección Nacional Simit, que permita

fijar los criterios que seguirán para proteger la privacidad de la información y los datos, así como de los procesos y las personas vinculadas con dicha información.

MARCO NORMATIVO

Figura 29. Marco Normativo.

Figura 30. Cumplrimiento del Modelo segun Decreto 2573 de 2014.

Figura 31.Piramide de Ciberseguridad.

Figura 32. Linea Historica de la Seguridad de la Información en Colombia.

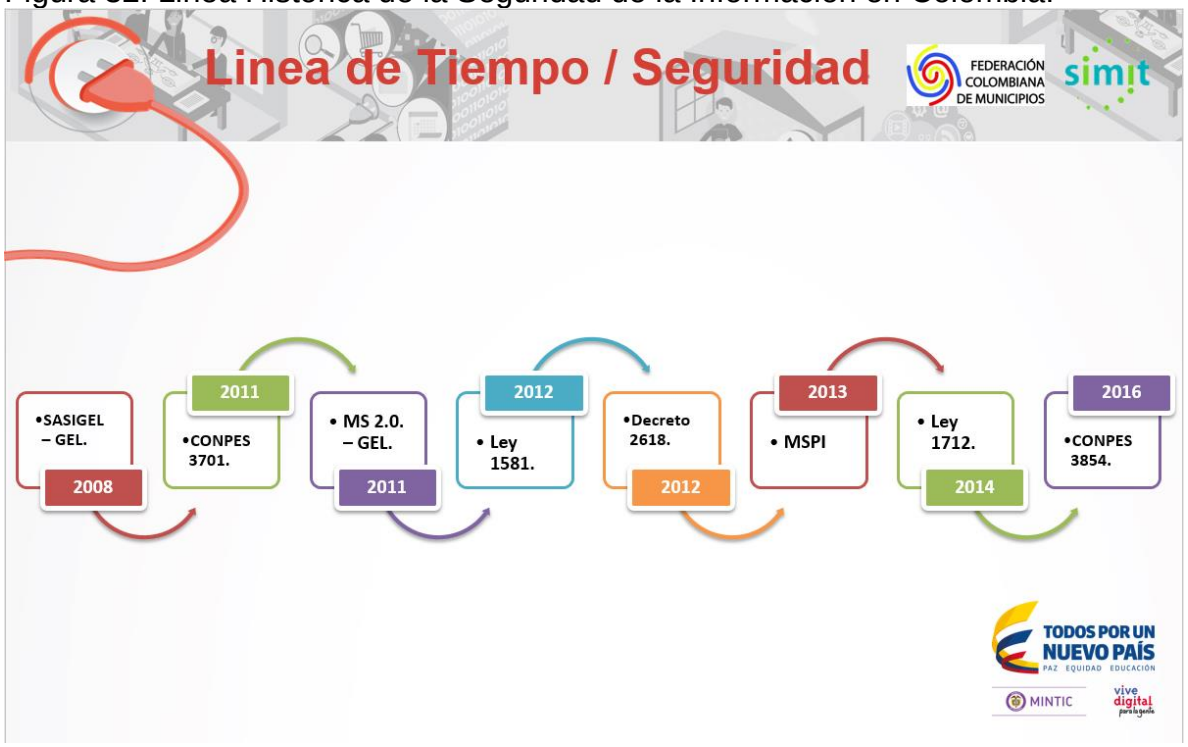
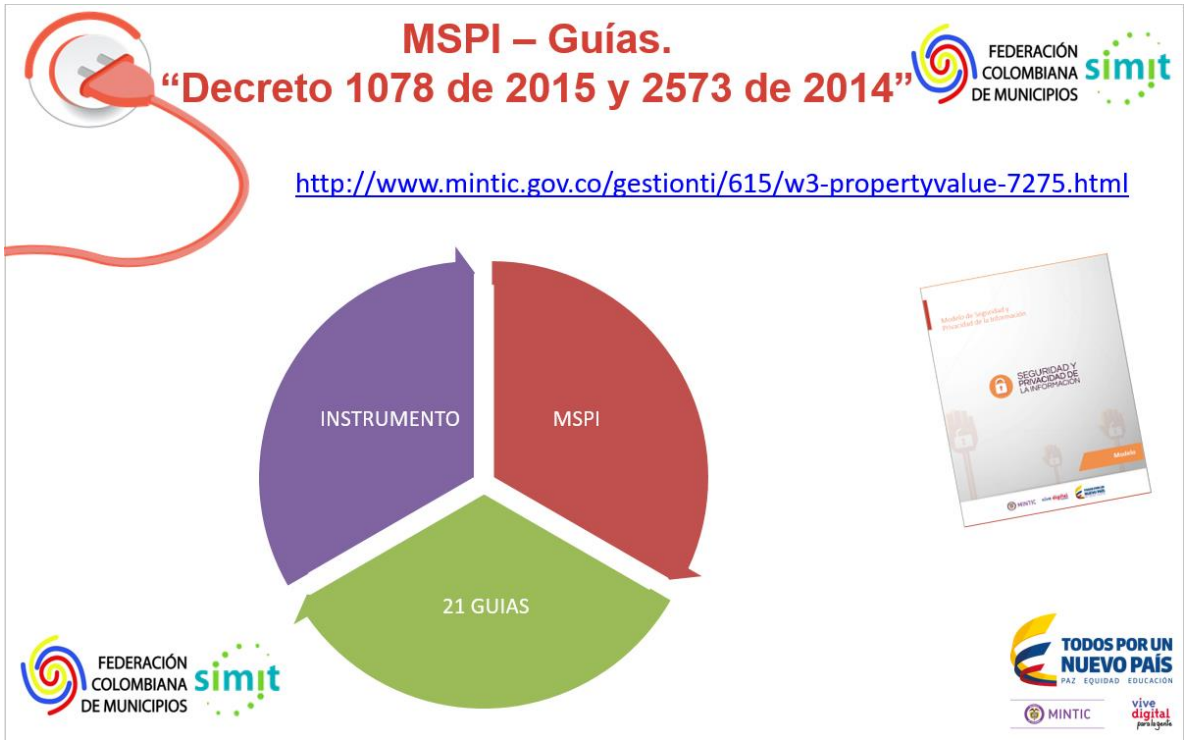


Figura 33. Ciclo de Implementacion y Gestion del MSPI.

Figura 34. Guia del Modelo de Seguridad y Privacidad de la Información.

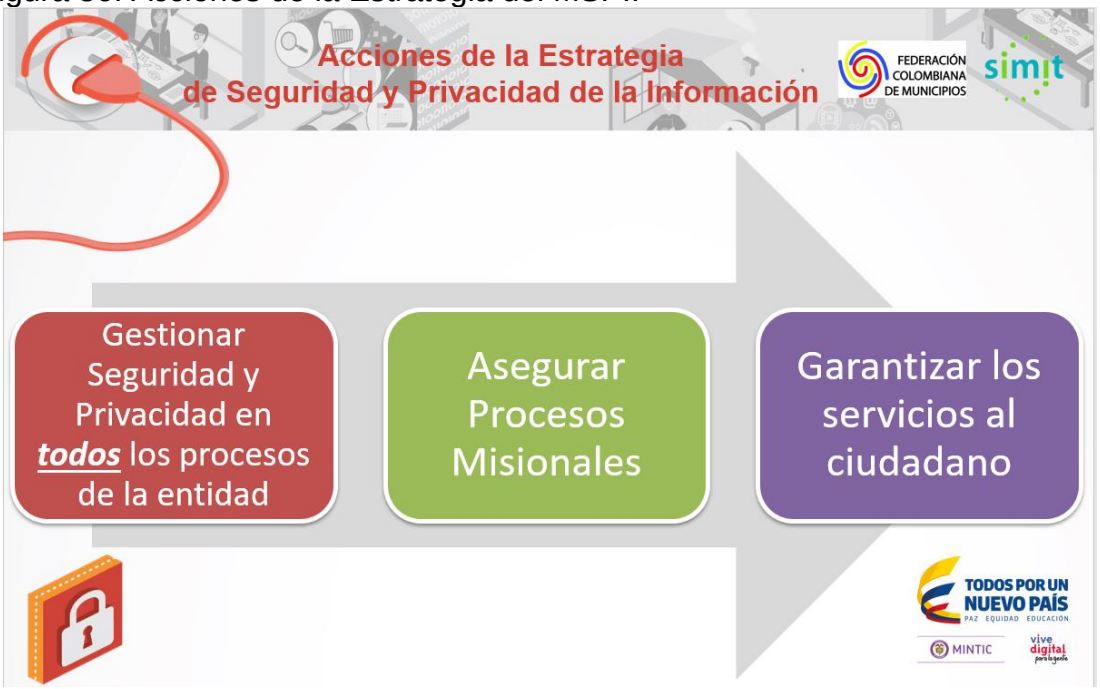


ALCANCE DEL (MSPI) PLAN DE IMPLEMENTACION SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÒN:

Figura 35. Alcance del MSPI.

ACCIONES DE LA ESTRATEGIA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA FEDERACION COLOMBIANA DE MUNICIPIOS – DIRECCIÓN NACIONAL SIMIT.

Figura 36. Acciones de la Estrategia del MSPI.



Aspectos Generales de la Organización

La Federación Colombiana de Municipios es una persona jurídica de carácter privado, sin ánimo de lucro, creada mediante el concurso y consenso de los entes territoriales en ejercicio del derecho constitucional de asociación. A ella pertenecen por derecho propio todos los municipios, distritos y asociaciones de municipios del país y tiene como finalidad la defensa de sus intereses. En este sentido, la Federación Colombiana de Municipios se rige por el derecho privado, salvo en lo que concierne a la función pública asignada según los artículos 10 y 11 de la Ley 769 de 2002, cuyo fundamento constitucional se esgrime en el artículo 209 de la Constitución Política.

Luego, si bien es cierto que la Federación Colombiana de Municipios se rige por las normas del derecho privado, en lo concerniente a la función pública delegada por disposición legal, se encuentra sometida a las normas propias del derecho público, siendo aplicable entonces para el presente proceso de contratación, los procedimientos contemplados en la Ley 80 de 1993, modificada por la Ley 1150 de 2007, Ley 1474 de 2011 y el Decreto Reglamentario 1082 de 2015.

La Federación Colombiana de Municipios por expreso mandato legal, ha requerido desde sus inicios, contar con una infraestructura tecnológica suficiente que garantice un adecuado y permanente funcionamiento, y que sea susceptible de perfeccionamiento a través de la implementación de nuevas tecnologías aplicadas siempre al logro del fin perseguido, con métodos de control y calidad de la información.

En el marco del cumplimiento de dicha función pública delegada y teniendo en cuenta que la Dirección Nacional Simit, administra un sistema de información que está disponible en internet y a pesar de las implementaciones en seguridad puede llegar a ser objeto de intentos de sabotaje o ataques cibernéticos, se hace necesario para la entidad prepararse en la protección del sistema y de sus activos de información contra posibles ataques y amenazas, la protección debe estar alineada al MSPI (Modelo de Seguridad y Privacidad de la Información) que dispuso el Ministerio de las Tecnologías de la Información y las Comunicaciones en el marco de la estrategia de Gobierno en Línea y en cumplimiento de lo señalado en el artículo 5 del decreto 2573 del 2014 y lo expresado en el Decreto 1078 de 2015*.***

Así mismo la Federación Colombiana de Municipios dentro de la administración y actualización del sistema Integrado de Información sobre Multas y Sanciones por Infracciones de Tránsito debe garantizar la integridad de la información almacenada en el Sistema y blindar la infraestructura asegurando su disponibilidad para la consulta del estado de cuenta, cargue de información de las autoridades de tránsito a nivel nacional y por supuesto, la generación de paz y salvos que permitan, a los ciudadanos, realizar los trámites de tránsito.

Dado esto se hace necesario buscar un apoyo que le permita a la Federación Colombiana de Municipios tomar las decisiones correctas, apropiadas y oportunas en cuanto a la seguridad de la información, acordes a la rápida evolución de los sistemas de información a nivel mundial y por lo tanto volviéndose un insumo indispensable para proteger el sistema y los procesos, basándose en las mejores prácticas existentes en la actualidad. Para suplir esta necesidad la Federación Colombiana de Municipios requiere contar con asesorías sobre los modelos de seguridad informática, las cuales deben incluir las revisiones y mejoras de políticas, normas, procedimientos y estándares, así como divulgaciones y capacitaciones para todos los usuarios de la entidad.

Atendiendo a que las actividades propias de seguridad y privacidad de la información demandan conocimientos especializados en donde predomina el factor intelectual, se asigna al Profesional Oficial de Seguridad Informática, quien, a través de su conocimiento y experiencia en implementación de soluciones de tecnología, experiencia en la Gerencia de Proyectos de TI, consultoría y auditoría en la norma ISO 27001 y en la Interventoría de Proyectos, se encuentran enfocados y especializados en la Seguridad de la Información.

El Profesional Oficial de Seguridad Informática, como responsable Oficial en Seguridad de la Información para la Federación Colombiana de Municipios – Dirección Nacional Simit, busca mantener vigentes los requerimientos de la entidad en los procesos que serán analizados para posteriormente complementar, ajustar e implementar la seguridad y privacidad de la información con las mejores prácticas, para administrar y mitigar razonablemente los riesgos informáticos relacionados con pérdida de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Por estas razones, dada la necesidad de acceder a la información cualificada en el marco de las funciones encomendadas por expreso mandato legal; se hace necesario dirigir, coordinar y gestionar a través del Profesional Oficial de Seguridad Informática, el logro de objetivos estratégicos y tácticos en materia de confidencialidad, integridad y disponibilidad de los sistemas y activos de información con los que cuenta la Federación Colombiana de Municipios – Dirección Nacional Simit.

Descripción de la Entidad con Función Pública Delegada

Razón social: Federación Colombiana de Municipios
Dirección: Kra 7a, No. 74-56 Bogotá D.C
Teléfono: (57+1) 593 40 20
Responsable: Dr. Gilberto Toro Giraldo
Teléfono Responsable: (57+1) 593 40 20
Cargo: Director Ejecutivo.

Descripción y Actividad Comercial: La (FCM) Federación Colombiana de Municipios, es una entidad privada sin ánimo de lucro, mediante el cual; el congreso de la república mediante un acto administrativo de estado, le delego un órgano de gobierno para su administración pública, con el fin de fortalecer la gestión y necesidades estratégicas de los municipios de Colombia y el sistema de información sobre multas y sanciones por infracciones de tránsito del País, el órgano de gobierno que le fue delegado es la Dirección Nacional Simit.

Como actividad comercial, realiza convenios y contrataciones a nivel nacional e internacional, con el fin de apoyar las necesidades estratégicas y tácticas que poseen las alcaldías y las autoridades de transito del país, de tal manera que materializa la estrategia hacia una operación de negocio a nivel nacional en varios ámbitos, como: político, tecnológico, gestión social, infraestructura, entre otros.

Misión de la Función Publica

Contribuir al mejoramiento de los ingresos de los municipios con la operación y permanente actualización del sistema integrado de información sobre multas y sanciones por infracciones de tránsito a nivel nacional; permitiendo el acceso a la información que impida la realización de trámites de tránsito a los ciudadanos que no se encuentren a Paz y Salvo.

Visión de la Función Publica

Para el año 2020 el Sistema Integrado de Información sobre Multas y Sanciones por Infracciones de Tránsito - SIMIT será el referente en Latinoamérica con los más altos estándares de innovación, calidad y confiabilidad.

Seremos la mejor experiencia de gobierno en línea y la principal fuente de información para las políticas públicas de seguridad vial, garantizando la nivelación tecnológica de los organismos territoriales de tránsito, y consolidándonos como un sistema invulnerable que asegure la satisfacción del usuario y la rentabilidad social**.**

Objetivos Estratégicos de la Función Publica:

PERSPECTIVA SOCIAL
- Objetivo: Responsabilidad Social
- Objetivo: Creación de Valor

PERSPECTIVA CLIENTE
- Objetivo: Confiabilidad

PERSPECTIVA PROCESO INTERNO
- Objetivo: Información Valiosa

PERSPECTIVA INNOVACIÓN
- Objetivo: Posicionamiento

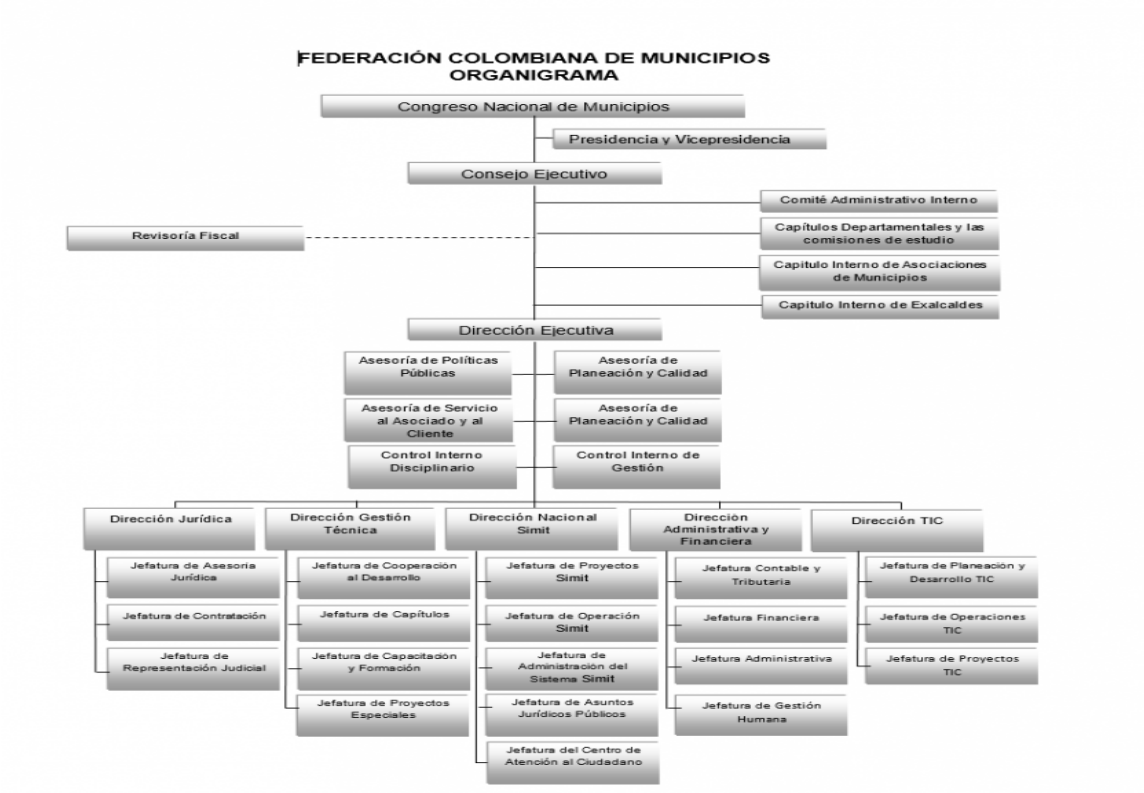
Mapa Estratégico Dirección Nacional Simit

Figura 37. Mapa Estrategico Direccion Nacional Simit.

Fuente: Activos de Información FCM.

Organigrama Federación Colombiana de Municipios

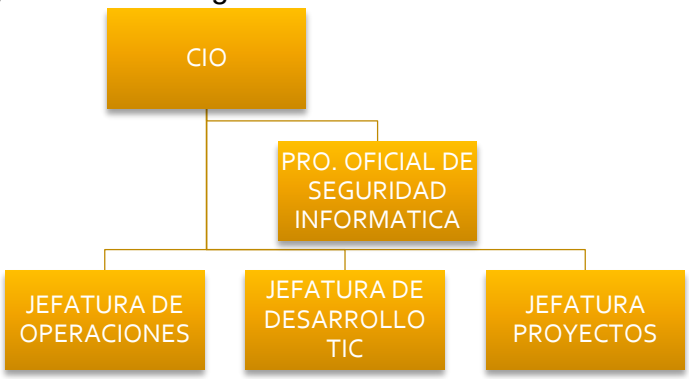
Figura 38. Organigrama de Federacion Colombiana de Municipios.



Organigrama Federación Colombiana de Municipios

Estructura Organizacional de la Dirección TIC

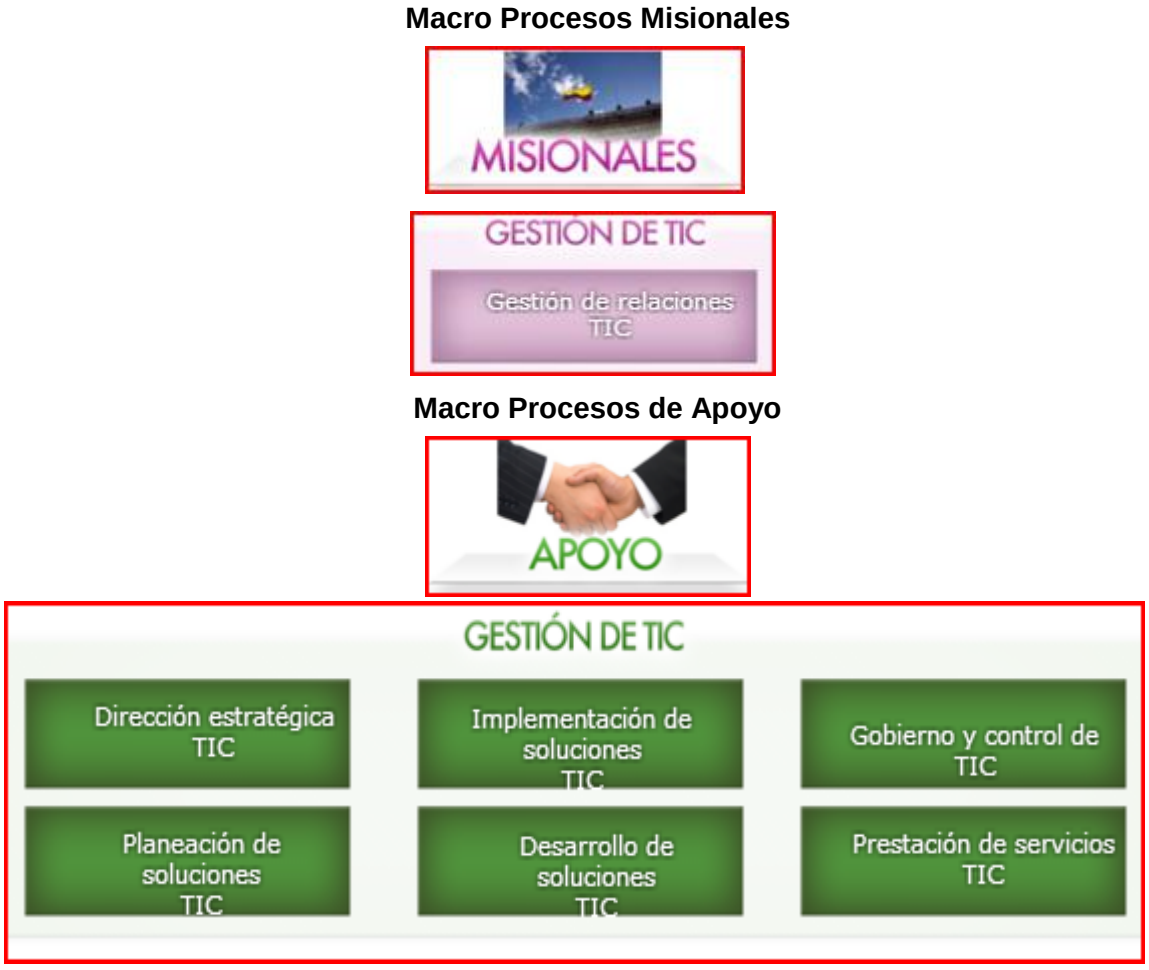
Figura 39. Estructura Organizacional Seguridad Informatica.



Fuente: Activos de Información de la Dirección de Tecnologías de la Información y las Comunicaciones.

Procesos y Servicios de la Dirección TIC

Figura 40. Procesos y Servicio de la Direccion TIC.



Fuente: https://www.fcm.org.co/mapa-de-procesos/

Caracterización de los Procesos de la Dirección TIC que presta a la Federación Colombiana de Municipios – Dirección Nacional Simit:

En los siguientes vínculos pueden visualizar la caracterización de los procesos que la Dirección de Tecnologías de la Información y las Comunicaciones, gestiona en la entidad.

Macro Proceso Misional:
https://www.fcm.org.co/wp-content/uploads/2017/01/GestiondeRelacionesTIC.pdf

Macro Procesos de Apoyo:

Dirección Estratégica:
https://www.fcm.org.co/wp-content/uploads/2017/01/DireccionestrategicadeTIC.pdf

Implementación de Soluciones TIC:
https://www.fcm.org.co/wp-content/uploads/2017/01/ImplementaciondeSolucionesTIC.pdf

Gobierno y Control TIC:
https://www.fcm.org.co/wp-content/uploads/2017/01/GobiernoycontroldeTIC.pdf

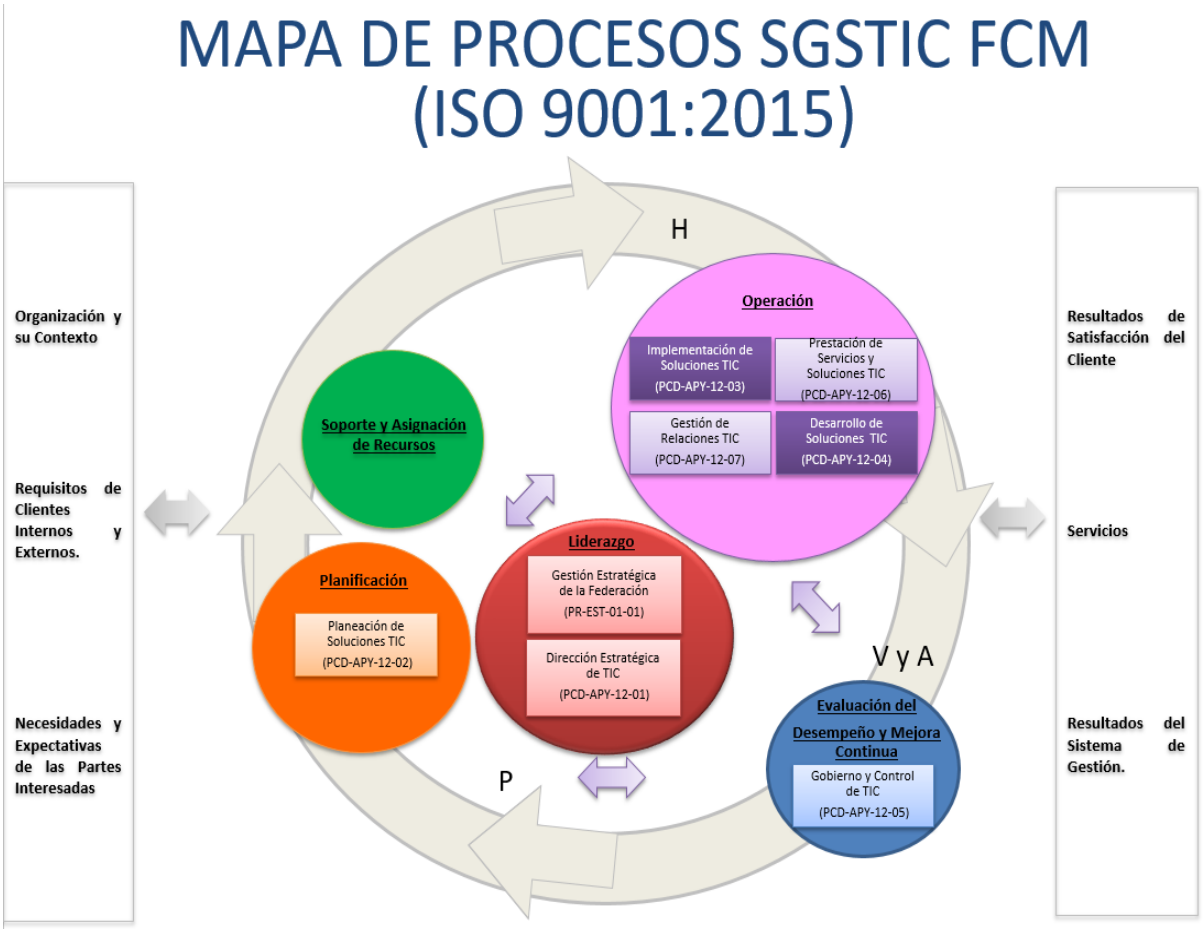
Planeación de Soluciones TIC:
https://www.fcm.org.co/wp-content/uploads/2017/01/PlaneaciondesolucionesTIC.pdf

Desarrollo de Soluciones TIC:
https://www.fcm.org.co/wp-content/uploads/2017/01/DesarrollodesolucionesTIC.pdf

Prestación de Servicios TIC:
https://www.fcm.org.co/wp-content/uploads/2017/01/PrestaciondeServiciosTIC.pdf

Mapa de Procesos Estratégicos, Misionales y Apoyo, de la Dirección de Tecnologías de la Información y las Comunicaciones, alineado a la Norma ISO 9001:2015.

Figura 41. Mapa de Procesos ISO 9001:2015.



Fuente: Activos de Información de la Dirección TIC

A continuación, se estructura el ponderado de los avances de actividades del MSPI – Modeo de Seguridad y Privacividad de la Información que se han realizado a la fecha, como también identificando como brecha la ejecución de actividades que no están al 100%, de los cuales se tiene que desarrollar para los años 2.018 al 2.021, esto alineado conforme a las fases del proyecto del MSPI que definió el Ministerio de las Tecnologias de la Información y las Comunicaciones, las cuales son: Diagnóstico, Planificación, Implementación, Mejoramiento continuo y la Evaluación de desempeño.

Tabla 22. Plan de Actividades para la Implementacion del Modelo de Seguridad y Privacidad de la Informacion de Mintic.

DIRECCIÓN DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES								
PROYECTO DE IMPLEMENTACIÓN PARA EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, EN LA FEDERACIÓN COLOMBIANA DE MUNICIPIOS - DIRECCION NACIONAL SIMIT, SEGÚN LINEAMIENTOS Y GUIAS DE LA ESTRATEGIA DE GOBIERNO EN LINEA.								
DECRETO 1078 DE 2015								
PLANIFICACIÓN DE ACTIVIDADES								
No.	ACTIVIDADES	RECURSOS HUMANOS	ESTADO ACTUAL EN FCM					
1	DIAGNOSTICO (ACTIVIDADES DE INICIO)		0%	20%	40%	60%	80%	100%
1.1	Manifestar la intención de incluir el MSPI en el Sistema de Gestión de la Calidad y la caracterización de procesos en FCM-DNS, por parte de la Alta Dirección.	Profesional Oficial de Seguridad Informática / DIRECCION TIC / DIR. EJECUTIVA / PLANEACION Y CALIDAD				60		
1.2	Definir la conformación del Comité de Seguridad de la Información	Profesional Oficial de Seguridad Informática					80	
1.3	Aprobar conformación del Comité de Seguridad de la Información	DIRECCION EJECUTIVA			40			
1.4	Aplicar el autodiagnóstico de Seguridad de la Información	Profesional Oficial de Seguridad Informática				60		
1.5	Desarrollar Plan de Proyecto para implementar el MSPI	Profesional Oficial de Seguridad Informática					80	
1.6	Aprobar el plan de proyecto para iniciar el proyecto MSPI	COMITÉ MSPI			50			
1.7	Divulgar el plan de Trabajo para estandarizar el MSPI con los procesos construidos, manifestar las auditorias que se planearan con el propósito de la mejora continua al MSPI.	Profesional Oficial de Seguridad Informática			50			
1.8	Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad	Profesional Oficial de Seguridad Informática				60		
1.9	Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Profesional Oficial de Seguridad Informática			50			
1.10	Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Profesional Oficial de Seguridad Informática						100

1.11	Hito de Entregables Fase Diagnostico	Profesional Oficial de Seguridad Informática						
2	PLANIFICACIÓN DEL MSPI							
2.1	Definir el alcance del MSPI (contexto, liderazgo, planeación, interesados, limites, aplicabilidad, soporte)	Profesional Oficial de Seguridad Informática / COMITÉ MSPI						
2.2	Aprobar alcance del MSPI, límites de acuerdo a la estructura de la organización	COMITÉ MSPI						
2.3	Definir roles y responsabilidades de seguridad de la información	Profesional Oficial de Seguridad Informática / COMITÉ MSPI		20				
2.4	Aprobar roles y responsabilidades de seguridad de la información	COMITÉ MSPI		20				
2.5	Definir la política general, manual de políticas y política por documento, teniendo en cuenta los objetivos.	Profesional Oficial de Seguridad Informática						
2.6	Aprobar la políticas y objetivos del MSPI	Profesional Oficial de Seguridad Informática / COMITÉ MSPI						
2.7	Definir los instrumentos para la identificación y clasificación de activos de información	Profesional Oficial de Seguridad Informática		20				
2.8	Aprobar los instrumentos para la identificación y clasificación de activos de información (documento y formato)	Profesional Oficial de Seguridad Informática						
2.9	Identificar y clasificar los activos de información por proceso de acuerdo con el alcance del MSPI definido.	Profesional Oficial de Seguridad Informática					80	
2.10	Aplicar la metodología de gestión de riesgos alineada al SGC y/o control interno o DAF	Profesional Oficial de Seguridad Informática / CONTROL INTERNO DE GESTION						
2.11	Aprobar la metodología de gestión de riesgos	Profesional Oficial de Seguridad Informática / COMITÉ MSPI					80	
2.12	Realizar la identificación, valoración y evaluación de riesgos de seguridad de la información por proceso según la metodología aprobada.	Profesional Oficial de Seguridad Informática					80	

2.13	Aprobar matriz de evaluación de riesgos del MSPI	Profesional Oficial de Seguridad Informática					80
2.14	Establecer el plan de tratamiento de riesgos	Profesional Oficial de Seguridad Informática					80
2.15	Aprobar plan de tratamiento de riesgos	Profesional Oficial de Seguridad Informática / COMITÉ MSPI					
2.16	Definir documento de declaración de aplicabilidad	Profesional Oficial de Seguridad Informática					
2.17	Aprobar documento de declaración de aplicabilidad	Profesional Oficial de Seguridad Informática / COMITÉ MSPI					
2.18	Elaborar Procedimiento del MSPI	Profesional Oficial de Seguridad Informática					
2.19	Socializar Procedimientos a los miembros del Comité MSPI y (Ajustar si Aplica)	Profesional Oficial de Seguridad Informática / COMITÉ MSPI					
2.20	Entregar copia de los Procedimientos a Planeación y Calidad para su integración al sistema de gestión institucional	Profesional Oficial de Seguridad Informática					
2.21	Integrar los documentos de seguridad de la información al Manual SGC	Profesional Oficial de Seguridad Informática / PLANEACION Y CALIDAD					
2.22	Aprobar el Manual SGC con la integración del MSPI	Profesional Oficial de Seguridad Informática / PLANEACION Y CALIDAD					
2.23	Definir la estrategia y adoptar la Integración del MSPI con el Sistema de Gestión Documental de la entidad	Profesional Oficial de Seguridad Informática / COORD. GESTION DOCUMENTAL					
2.24	Aprobar la estrategia y adopción de la Integración del MSPI con el Sistema de gestión documental	Profesional Oficial de Seguridad Informática / COORD. GESTION DOCUMENTAL					
2.25	Implementación de la Integración del MSPI con el sistema de gestión documental	Profesional Oficial de Seguridad Informática / COORD. GESTION DOCUMENTAL					
2.26	Plan de Diagnostico de IPV4 a IPV6	Profesional Oficial de Seguridad Informática					

2.27	Incluir dentro de los planes de concienciación y sensibilización, capacitación y entrenamiento del SGC de la entidad, los aspectos de seguridad de la información.	Profesional Oficial de Seguridad Informática / PLANEACION Y CALIDAD / RECURSOS HUMANOS					
2.28	Definir mecanismos (qué, quién, cuándo) para la evaluación del cumplimiento de las políticas declaradas.	Profesional Oficial de Seguridad Informática					
2.29	Ajustar y/o definir y planificar el programa de auditorías internas incluyendo aspectos de seguridad de la información.	Profesional Oficial de Seguridad Informática / CONTROL INTERNO DE GESTION					
2.30	Aprobar el programa de auditorías internas incluyendo aspectos de seguridad de la información.	Profesional Oficial de Seguridad Informática / CONTROL INTERNO DE GESTION / COMITÉ MSPI					
2.31	Establecer indicadores de eficacia para el MSPI en general.	Profesional Oficial de Seguridad Informática					
2.32	Aprobar indicadores de eficacia para el MSPI en general.	Profesional Oficial de Seguridad Informática					
2.33	Hitos de Entregables de Planificación y Plan de Seguridad y Privacidad de la Información Actualizado.	Profesional Oficial de Seguridad Informática					
3	IMPLEMENTACIÓN DEL MSPI						
3,1	Desarrollar las actividades incluidas en los planes de concienciación y sensibilización, entrenamiento y capacitación a la entidad que hacen referencia al MSPI.	Profesional Oficial de Seguridad Informática					
3,2	Implementar controles del plan de tratamiento de riesgos de acuerdo a los riesgos encontrados	Profesional Oficial de Seguridad Informática					
3.3	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Profesional Oficial de Seguridad Informática					

3.4	Planificación y Control Operacional: Actualizar la declaración de aplicabilidad	Profesional Oficial de Seguridad Informática					
3.5	Describir en documento la Evaluación del MSPI conforme a los Indicadores de Gestión definidos	Profesional Oficial de Seguridad Informática					
3.6	Plan de Transición de IPv4 a IPv6	Profesional Oficial de Seguridad Informática / JEFATURA DE OPERACIONES TIC					
3.7	Aprobación del plan con la estrategia de implementación de IPv6 en la entidad, aprobado por la Dirección de TI.	Profesional Oficial de Seguridad Informática / DIRECCION TIC					
4	EVALUACIÓN DEL DESEMPEÑO DEL MSPI						
4.1	Evaluar el cumplimiento de las políticas/procedimientos implementados y Plan de revisión y seguimiento a la Implementación del MSPI	Profesional Oficial de Seguridad Informática					
4.2	Ejecutar el programa de auditorías internas.	AUDITORES CONTROL INTERNO DE GESTION / Profesional Oficial de Seguridad nformática					
4.3	Revisar y analizar el nivel del riesgo residual, implementación del plan de riesgos, revisión y aprobación de la declaración de aplicabilidad actualizada e indicadores	Profesional Oficial de Seguridad Informática					
4.4	Realizar la revisión por la dirección de la Entidad dentro del marco del SGC	COMITÉ MSPI					
5	MEJORAMIENTO CONTINUO DEL MSPI						
5.1	Generar el plan de mejoramiento del MSPI y auditorias (acciones correctivas y mejora continua) de acuerdo con los resultados de las revisiones dadas.	Profesional Oficial de Seguridad Informática / CONTROL INTERNO DE GESTION / DEMAS AREAS DE LA ENTIDAD		20			
5.2	Aprobar el plan de mejoramiento del MSPI y de las auditorias (acciones correctivas y mejora continua) de acuerdo con los resultados de las revisiones dadas.	Profesional Oficial de Seguridad Informática / CONTROL INTERNO DE GESTION					

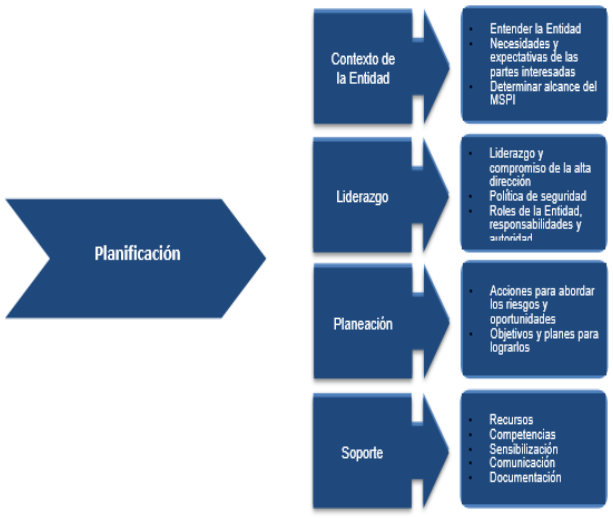
5.3	Ejecutar el plan de mejoramiento del MSPI.	Profesional Oficial de Seguridad Informática / CONTROL INTERNO DE GESTION / DEMAS AREAS DE LA ENTIDAD		20			

DESCRIPCIÓN Y ENTREGABLES DE LAS FASES DEL PROYECTO DE INVERSION Y PRESUPUESTO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Tabla 23. Entregables Fase Diagnostico.

FASE DIAGNOSTICO	
GESTION A REALIZAR	**ENTREGABLES**
En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas: 1. Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad. 2. Determinar el nivel de madurez de los controles de seguridad de la información. 3. Identificar el avance de la implementación del ciclo de operación al interior de la entidad. 4. Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales. 5.Identificación del uso de buenas prácticas en ciberseguridad. Para ello se recomienda utilizar los siguientes instrumentos: 1. Herramienta de diagnóstico 2. Instructivo para el diligenciamiento de la herramienta 3. Guía No 1 - Metodología de Pruebas de Efectividad Para realizar dicha fase las entidades deben efectuar la recolección de la información con la ayuda de la herramienta de diagnóstico y la metodología de pruebas de efectividad. Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la entidad se procede al desarrollo de la fase de Planificación. Los resultados asociados a la fase de Diagnostico previas a la implementación deben ser revisados y socializados por las partes interesadas.	Documento de identificación del nivel de madurez de la entidad. Herramienta de diagnóstico Diligenciada. Documento con los hallazgos encontrados en las pruebas de vulnerabilidad Macroprocesos de Gestión de la Seguridad y Privacidad de la Información y la Caracterización de Procesos, integrado al SGC - Sistema de Gestión de Calidad.

Tabla 24.Entregables fase Planificación

FASE PLANIFICACIÓN	
GESTION A REALIZAR	**ENTREGABLES**
Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo. El alcance del MSPI permite a la Entidad definir los límites sobre los cuales se implementará la seguridad y privacidad en la Entidad. Este enfoque es por procesos y debe extenderse a toda la Entidad. Para desarrollar el alcance y los límites del Modelo se deben tener en cuenta las siguientes recomendaciones: Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.  Figura 3 - Fase de planificación[1]	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad. Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad. Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional. Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad. Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales Inventario de activos de IPv6. Integración del MSPI, con el sistema de gestión documental de la entidad. Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección. Documento con el plan de comunicación, sensibilización y

	capacitación para la entidad. Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.

Tabla 25. Entregables Fase Implementación

FASE IMPLEMENTACION	
GESTION A REALIZAR	**ENTREGABLES**
Esta fase le permitirá a la Entidad, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI.  Figura 4 - Fase de implementación[2] Plan de Transición de IPv4 a IPv6 | Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI. | Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6. Guía No 20 - Transición de IPv4 a IPv6 para Colombia. Guía No 19 – Aseguramiento del Protocolo IPv6.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso. Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información. Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI. Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.

Tabla 26. Entregables Fase Evaluación

FASE EVALUACIÓN	
GESTION A REALIZAR	**ENTREGABLES**
El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.  Figura 5 - Fase de Evaluación de desempeño[3]	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección. Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.

Tabla 27. Entregables Fase Mejora Continua

FASE MEJORA CONTINUA	
GESTION A REALIZAR	**ENTREGABLES**
En esta fase la Entidad debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.  Figura 6 - Fase de mejoramiento continúo[4] En esta fase es importante que la entidad defina y ejecute el plan de mejora continua con base en los resultados de la fase de evaluación del desempeño. Este plan incluye: · Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI. · Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI. Utilizando los insumos anteriores, la entidad puede efectuar los ajustes a los entregables, controles y procedimientos dentro del MSPI. Estos insumos tendrán como resultado un plan de mejoramiento y un plan de comunicaciones de mejora continua, revisados y aprobados por la Alta Dirección de la entidad. La revisión por la Alta Dirección hace referencia a las decisiones, cambios, prioridades etc. tomadas en sus comités y que impacten el MSPI.	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados. Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.

9.3 Plan de Sensibilizacion de Seguridad y Privacidad de la Información

Objetivos específicos de la divulgación y sensibilización:

Los siguientes son los objetivos a alcanzar luego de la ejecución de las estrategias de sensibilización:

a. Mejorar el nivel de conocimiento de los colaboradores de la FCM en temas de seguridad de la información.

b. Dar a conocer y entender a los colaboradores las Políticas, Procesos y Procedimientos de Seguridad de la Información.

c. Mejorar el nivel de conciencia en temas de seguridad de la información y promover el reporte de eventos e incidentes.

d. Desarrollar una campaña de computador seguro que permita generar una cultura organizacional al interior de la Federación Nacional de Municipios frente a temas de seguridad de la información.

Estrategias de sensibilización y divulgación propuestas:

Las estrategias propuestas por parte de la FEDERACION COLOMBIANA DE MUNICIPIOS, buscan promover la Seguridad de la Información y están alienadas con el Pliego de Condiciones, el contrato y la propuesta técnica así.

Es muy importante generar una cultura organizacional al interior de la FEDERACION NACIONAL DE MUNICIPIOS frente a temas de seguridad de la información, para ello se proponen actividades asertivas que propicien el entendimiento de lo que significa el aseguramiento de los datos y las posibles consecuencias frente a descuidos, usualmente culposos, con ocasión de malos manejos de la información.

Plan de sensibilización

El plan para la campaña de computador seguro busca cubrir los siguientes temas:

Modificar actitudes: Generar conciencia en los Funcionarios de la Organización, sobre la importancia del adecuado manejo de la información; demostrando que todas las personas que integran la Entidad, son responsables de la seguridad de la información.

Entrenamiento: Capacitar a los Funcionarios seleccionados por la organización en el uso de buenas prácticas, respecto a las políticas y procedimientos internos de seguridad de la información; que permita contribuir activamente hacia el eficiente aseguramiento de la información dentro del SGSI.

Educar al personal: Una vez culminadas las etapas anteriores, se fomentarán hábitos en los Funcionarios capacitados para que estén a la vanguardia en temas relacionados con seguridad de la información y mejores prácticas; lo cual a su vez permitirá contribuir activamente con las políticas de calidad, mejoramiento continuo y el adecuado manejo del sistema de gestión de seguridad de la información.

Legislación: FEDERACION COLOMBIANA DE MUNICIPIOS capacitará a los funcionarios seleccionados por la organización, en aspectos legales y técnicos relacionados con la seguridad de la información, para que estas puedan ser usadas en diferentes procesos, tales como laborales, penales o civiles.

Inventario de música, videos y borrado de contenidos ilegales: Se harán inspecciones sobre los equipos de cómputo, utilizando para ello software portable que permita encontrar todo tipo de archivos como imágenes, videos, música, etc., que no sea permitido por la organización o que atente contra la vulneración de cualquier derecho.

Borrado de información personal: Notificar a las personas que deben suprimir la información personal que no es admitida por la organización y enseñarles que no ingresen a páginas de redes sociales, tales como Facebook, twitter, MSN y demás. Tampoco deberán acceder a programas de mensajería instantánea, a no ser que su contenido este legalmente pactado con fines y objetivos corporativos.

Navegación segura por internet: Incentivar a las personas a que hagan un buen uso del internet, especialmente con fines laborales; lo cual generaría un mejor desempeño en cuanto a velocidad, navegación y seguridad de la red.

Uso del correo electrónico: Indicar a los participantes de la Campaña, que el correo de la Entidad, es para uso exclusivo de la misma; ya que un manejo no adecuado, puede causar fugas de información.

Nota. El diseño de la campaña será entregado con los derechos de uso para su posterior actualización y aplicación para Federación Colombiana de Municipios.

Etapa de campaña de sensibilización.

LA FEDERACION COLOMBIANA DE MUNICIPIOS desarrollara una campaña denominada por nuestra organización -COMPUTADOR SEGURO-, la cual tiene como propósito sensibilizar a los funcionarios de la Federación Nacional de Municipios en todos los temas relacionados con seguridad de la información orientado a la adecuada implementación del Sistema de Gestión de Seguridad de la Información.

El desarrollo de esta campaña se ejecutará en cuatro (4) fases, así:

FASE DE EXPECTATIVA

Existirá un lanzamiento global de la Campaña, basada en el concepto de *Back to the future*, la cual estará dirigida a los funcionarios de la Federación Nacional de Municipios, con duración aproximada de tres (3) horas. entre otros, que permitan captar la atención de los participantes a fin de propiciar la receptividad de los mensajes emitidos y de los medios utilizados; para ellos se hará uso y entrega de:

- Cuatro (4) pendones, en material de lona y/o tela plástica, impreso digitalmente a tintas con los colores y logos Institucionales, que emitan mensajes relativos a la seguridad de la información.
- Diseño de cuatro (4) salvapantallas (protectores de pantalla), para el estudio y escogencia por parte de la Federación Nacional de Municipios.
- Uso de la imagen de segurito para que los funcionarios identifiquen la campaña.

- Un (1) Slogan de la campaña.
- Cuatro (4) Fondos de Pantalla. (Alusivo a la campaña de seguridad de la información).
- Diseño de dos (2) mensajes de correo electrónico, para ser enviados a todos los Funcionarios comprometidos en la campaña.
- Retroalimentación interactiva de cultura en seguridad de la información, con premios entre los participantes los cuales van desde una cena para dos (2) personas con botella de vino, dos entradas para obra de teatro de temporada y/o el sorteo de una tableta electrónica.
- Se propone un photobooth (como elemento publicitario alusivo) para que las personas se tomen una foto, la tengan en sus puestos de trabajo y generen recordación, sentimientos positivos que refuercen, y finalicen en la apropiación de la campaña y de la seguridad de la información.

Se diseñarán diez (10) mensajes alusivos al tema de Seguridad de la información, los cuales serán escogidos por los funcionarios responsables de la Federación; éstos tendrán temas de tipo racional, emocionales y morales, buscando generar conciencia y mayor efectividad en las personas que los lean.

Los mensajes tendrán los siguientes propósitos:

- **Mensajes Racionales:** Conducta esperada para beneficios de la Seguridad de la Información.
- **Mensaje Emocionales:** Provocar emociones positivas con el fin de estimular la conducta deseada.
- **Mensajes Morales:** Comportamientos que se consideran seguros y los inseguros respecto a la gestión de la información y la infraestructura tecnológica.

FASE DE EJECUCIÓN.

Dentro de la fase de ejecución, FEDERACION COLOMBIANA DE MUNICIPIOS realizara dos (2) campañas de divulgación, las cuales corresponden a:

- Una primera campaña de sensibilización, será la realización de ***MICROOBRAS DE TEATRO****,* en donde se traten temas relacionados con seguridad de la información frente a los errores más comunes que los usuarios cometen en temas de seguridad de la información. Cada Micro obra será de quince (15) minutos por cada 20 usuarios hasta completar como mínimo el 50% de la población objetivo. Es importante resaltar que las obras de teatro se desarrollaran en las áreas de trabajo de los funcionarios, esto con la finalidad de evitar el traslado a otros lugares, y con ello, la inasistencia de los funcionarios.

- La segunda campaña de divulgación, será un juego concurso, en donde los funcionarios la Federación Nacional de Municipios podrán participar y ganar premios (dos (2) Tablet). Lo que se busca con esta actividad es lograr evaluar los conocimientos que en temas de seguridad de la información poseen los funcionarios de la entidad y poder hacer una evaluación que termine con una retroalimentación que podrá darse en la etapa de transmisión del conocimiento. El juego consistirá en responder preguntas de manera periódica, para lo cual los funcionarios estarán acumulando puntos que les permitirá tener un score, y con ello, poder determinar los mayores puntajes conseguidos en el desarrollo de la actividad, premiando a los dos (2) puntajes más altos.

En esta segunda fase, se está cumpliendo con lo solicitado en el alcance, es decir, dos (2) campañas de divulgación.

- FEDERACION COLOMBIANA DE MUNICIPIOS brindará una solución que permita practicar una evaluación teórica de los conceptos adquiridos durante la capacitación a los Funcionarios participantes; a su vez dicha solución permitirá realizar la retroalimentación de la actividad.
- Así mismo, FEDERACION COLOMBIANA DE MUNICIPIOS diseñará y hará entrega de una cartilla digital, donde se muestren temas relacionados con la seguridad de la información, elemento que será desarrollado por medio de una herramienta grafica que permita una fácil interacción con los usuarios y actualización de la misma.

FASE DE TRANSFERENCIA DEL CONOCIMIENTO

Como complemento de estas actividades lúdicas asociadas a la campaña de computador seguro, y con la finalidad de no tener que desarrollar un documento adicional, nos permitimos exponer a continuación nuestra propuesta para la transmisión del conocimiento, la cual está completamente contextualizada, por ende, proponemos lo siguiente:

- Capacitación a través de conferencias, donde se socializarán temas relacionados con Seguridad de la Información, Sistemas de Gestión de Seguridad de la Información, políticas internas, delitos informáticos, protección de datos personales, aspectos laborales y legales en seguridad de la información, manejo de incidentes informáticos, entre otras. Estas conferencias serán definidas y coordinadas entre la Federación y FEDERACION COLOMBIANA DE MUNICIPIOS, en donde se deberán definir los temas a tratar, basados en los que anteriormente se plantearon, así como las fechas de su realización.

- Dentro del diseño de la campaña, se creará un módulo de sensibilización y formación orientado al nivel Directivo y Asesor de la Federación, con una intensidad aproximada de dos (2) horas, dicha capacitación se llevará a cabo en las instalaciones del Club de Abogados de la Ciudad de Bogotá, previa aprobación logística y de contenidos por partes de la entidad.

a. Conferencia dirigida a los colaboradores de la FCM. 100 personas. (entrenamiento, navegación segura, uso del correo electrónico, legislación)

b. Conferencia dirigida al personal responsable de la operación, mantenimiento y mejora del SGSI. 30 personas (educar al personal, legislación)
    a. Comité de seguridad de la información
    b. Comité Directivo

FASE DE CIERRE

FEDERACION COLOMBIANA DE MUNICIPIOS, en desarrollo del cronograma establecido, programará una actividad de tipo lúdico, para el cierre de la campaña, llevando un registro de asistencia. Esta etapa estará enfocada a los funcionarios de la Federación Nacional de Municipios; y para motivar la participación, se podrá sortear entre los asistentes premios, los cuales serán definidos por las partes.
Nota: El escenario, así como la logística serán responsabilidad de la Federación.

DETALLES DESARROLLO ACTIVIDADES.

MICRO-OBRAS DE TEATRO

Definición

Consiste en una actividad lúdica cultural con actores expertos, quienes a través de Micro representaciones teatrales difundirán los mensajes de concientización.

Datos de la obra teatral

Lugar: Federación colombiana de Municipios.
Fecha: 4 de diciembre de 2015
Hora: Medio día.

Características principales

a. Seis (6) representaciones teatrales que abarquen toda la FCM
b. Disponibilidad de 1 guion.
c. Cada presentación tiene una duración de 20 minutos.

JUEGO CONCURSO - TRIVIA

Definición

Consiste en una actividad lúdica y de concurso, en donde a través de la utilización de los canales de comunicaciones de la Federación Nacional de Municipios, se enviarán preguntas relacionadas con temas de seguridad de la información, las cuales se han desarrollado en las diferentes conferencias, logrando de esta manera la atención de los funcionarios, y con ello, premiar a las personas que tengan más preguntas acertadas.

Datos del concurso

Lugar: Federación colombiana de Municipios.
Fecha: 3 al 10 de diciembre. Entrega de premios el día del cierre.

Características principales

a. Se realizarán preguntas asociadas a temas de seguridad de la información.
b. Se emplearán los canales de comunicación de la Federación Nacional de Municipios.
c. Se llevará un score de los funcionarios que participen.

d. Se entregará una (1) tableta al mejores puntaje.
e. Se rifará una (1) tableta entre los asistentes a la conferencia.

CONFERENCIA DIRIGIDA A LOS COLABORADORES DE LA FCM

Conferencista

Consultores en Seguridad de la Información

Datos de la conferencia

Lugar: Sala de reunión - Federación colombiana de Municipios
Fecha: 9 de diciembre de 2015
Hora: 4 conferencias de 1 hora cada una en 2 salones simultáneos.

Nota: A cada charla podrá asistir un máximo de 20 personas.

Temáticas

a. ¿Qué es la seguridad de la información?

b. Estadísticas y casos reales de incidentes de seguridad de la información:

- A nivel internacional
- A nivel nacional
- Sector gobierno

c. ¿Por qué proteger la información?

- Beneficios de la Seguridad de la información.
- Política de Seguridad de la Información.

d. Marco legal Colombiano para la seguridad de la información.

- Ley 1712 de 2014 (Transparencias y Acceso a la Información Pública)
- Decisión 351 de la Comunidad Andina de Naciones (CAN) y la Ley 23 de 1982 (Protección de Propiedad Intelectual)
- Ley 1581 de 2012
- Ley 1273 de 2009 (Delitos Informáticos)

e. ¿Cómo participar en la seguridad de la información?

- Tips de seguridad de la información.
- Reporte de eventos e incidentes de seguridad de la información.

Registros

Se tomarán registros fotográficos de la actividad y listas de asistencia.

Hitos

Entrega de la presentación para revisión: 4 de diciembre de 2015.
Recepción de observaciones: 7 de diciembre de 2015

CONFERENCIA DIRIGIDA AL COMITÉ DIRECTIVO (PERSONAL RESPONSABLE DE LA OPERACIÓN, MANTENIMIENTO Y MEJORA DEL SGSI)

Conferencista

Ingeniero Experto en SGSI
CISM, CISA, CIA, CRISC, ITILF, CBCP, BCMMA
Experto en Consultoría en Seguridad de la Información y Continuidad del Negocio

Datos de la conferencia

Comité Directivo
Lugar: Sala de reunión – Club de Abogados
Fecha: 14 de diciembre de 2015
Hora: 10 a.m. – 12 p.m.

Temáticas

a. Compromiso de la Dirección

b. Ciclo PHVA del Sistema de Gestión de Seguridad de la información.

c. Organización de la Seguridad de la Información.

d. Propósito de la documentación del SGSI e integración con otros sistemas de gestión.

- Inventario de activos de información
- Políticas específicas requeridas por la ISO 27001:2013
- Procedimientos requeridos por la ISO 27001:2013
- Matriz de riesgos y plan de tratamiento
- Declaración de aplicabilidad

f. Gestión de Incidentes de Seguridad de la Información.

g. Articulando y Dirigiendo el SGSI

h. Ideas para campañas de sensibilización futuras.

i. Gestión de Continudad del Negocio.

j. Preguntas y respuestas

Registros

Se tomarán registros fotográficos de la actividad y listas de asistencia.

Hitos

Entrega de la presentación para revisión: 9 de diciembre de 2015.
Recepción de observaciones: 11 de diciembre de 2015

CONFERENCIA DIRIGIDA A COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (PERSONAL RESPONSABLE DE LA OPERACIÓN, MANTENIMIENTO Y MEJORA DEL SGSI)

Conferencista

Ingeniero Experto en SGSI
CISM, CISA, CIA, CRISC, ITILF, CBCP, BCMMA
Experto en Consultoría en Seguridad de la Información y Continuidad del Negocio

Datos de la conferencia

Comité de Seguridad de la Información
Lugar: Sala de reunión - Federación colombiana de Municipios
Fecha: 15 de diciembre de 2015
Hora: 9 – 10 a.m.

Temáticas

a. Diferencia entre seguridad informática y seguridad de la información.
b. Ciclo PHVA del Sistema de Gestión de Seguridad de la información.
c. Organización de la Seguridad de la Información.
d. Propósito de la documentación del SGSI.

- Inventario de activos de información
- Políticas específicas requeridas por la ISO 27001:2013
- Procedimientos requeridos por la ISO 27001:2013
- Matriz de riesgos y plan de tratamiento
- Declaración de aplicabilidad

k. Gestión de Incidentes de Seguridad de la Información.

l. Ideas para campañas de sensibilización futuras.

m. Preguntas y respuestas

Registros

Se tomarán registros fotográficos de la actividad y listas de asistencia.

Hitos

Entrega de la presentación para revisión: 9 de diciembre de 2015.
Recepción de observaciones: 11 de diciembre de 2015

ACTIVIDAD DE SENSIBILIZACIÓN Y CIERRE (MICRO OBRA 2 – SEGURITO Y LOLA SEGURA).

Definición

Consiste en una actividad lúdica cultural con actores expertos, quienes a través de una obra teatral difundirán los mensajes de concientización frente a seguridad de la información.

Datos de la obra teatral

Lugar: Federación colombiana de Municipios. Sala de reunión
Fecha: 11 de diciembre de 2015
Hora: 8 – 12 m.

Características principales

a. Seis (6) representaciones teatrales que abarquen toda la FCM
b. Disponibilidad de 1 guion.
d. Caracterización de "Segurito" y Lola Segura.

Montaje en escena

El montaje tendrá sonido, contará con dos actores caracterizados, uno como “Segurito” y otro como la villana, para hacer sentir un ambiente más familiar entre los colaboradores de la FCM y los actores del evento.

Los actores llevarán dulces, juguetes, confetis, globos y juegos para hacer más dinámica las presentaciones.

Hitos

Recepción de observaciones sobre el guion: hasta 3 de diciembre de 2015.

Anexos

Guion obra teatral

VIDEO DE INDUCCIÓN Y RE INDUCCIÓN AL SGSI

Temáticas

a. Generalidades del Sistema de Gestión de Seguridad de la Información.
b. Política de Seguridad de la Información.
c. Procedimientos de Seguridad de la Información.
d. Buenas prácticas en Seguridad de la Información
e. Sanciones ante el incumplimiento.

Propuesta de duración del video.

a. 1 video de 5 minutos.
b. 5 videos de 1 minuto.
c. 3 videos de 1.5 minutos.

Nota: Incluye voz en off y sonorización.

Requisitos

a. Comunicación fluida y constante. Toda información suministrada por parte del cliente debe estar digital y completamente editada.
b. Manual de identidad visual de la FCM o documento que haga sus veces, donde se indique las características del logo, colores y demás parámetros visuales de la FCM.
c. Imagen sectorizada de segurito (si lo tienen)

CURSO ESPECIALIZADOS:

Adicional a lo comprendido dentro de la campaña de computador seguro, FEDERACION COLOMBIANA DE MUNICIPIOS se compromete a dictar dos (2) cursos para treinta (30) colaboradores de la Federación Colombiana de Municipios, certificable por una universidad acreditada del país. Dentro de los cursos propuestos se encuentran:

CURSO DE PROTECCIÓN DE DATOS PERSONALES:

La protección de datos personales es un asunto que actualmente ninguna persona, empresa o entidad puede ignorar ya que la información de una persona y/o de una organización representa uno de sus bienes más importantes, situando el tema de seguridad de la información en una posición primordial y protagónica sobre otros temas. Progresivamente hemos pasado de los datos en textos escritos y archivadores físicos a textos digitales y archivos electrónicos, así, con la proliferación de nuevas tecnologías de comunicación y el incremento de la complejidad en los sistemas de información y de los riesgos asociados, por tal motivo se hace necesario capacitar a los encargados del manejo de los mismos para el correcto tratamiento y protección de los Datos de Carácter Personal.

Las autoridades nacionales, con la adopción de ley 1581 de 2012, que entró en vigencia en octubre de 2012, obligó a las personas, Entidades Públicas y Empresas a que cumplan con las normas vigentes en materia de protección de datos, en este sentido, es primordial conocer la regulación que se refiere a la protección de datos personales, asegurarse que la organización esté en total conformidad con el marco legal y que los encargados de la protección de datos personales tengan claro cuál es al ámbito de aplicación, las obligaciones de las organizaciones y las sanciones a imponer, por la no adecuación de la norma, que van desde penalidades disciplinarias a los funcionarios hasta millonarias multas.

Es por eso que FEDERACION COLOMBIANA DE MUNICIPIOS, previendo la importancia del tema en el contexto organizacional, propone el desarrollo del curso de protección de datos personales para que los funcionarios de la entidad desarrollen competencias en la clasificación, administración y registro de las bases de datos, y su adecuada protección mediante la aprehensión de los principios fundamentales de la Ley de Datos Personales 1581 de 2012.

El curso estará comprendido por siente (7) módulos que permiten llevar a cabo el desarrollo de los temas de forma teórico-prácticos y su aplicación en las

organizaciones teniendo en cuenta el contexto tanto nacional como internacional. Dentro de los módulos se encuentran:

- MÓDULO I. Fundamentos
- MÓDULO II. Marco Colombiano
- MÓDULO III. Marco Internacional
- MÓDULO IV. Protección de los Activos de la Información
- MÓDULO V. Gestión y Respuesta Antes Incidentes
- MÓDULO VI. Control y Auditoría de los Sistemas de Información

CURSO DE PRIMEROS RESPONDIENTES:

Efectivamente, la información hoy en día es el mayor activo para la sociedad, la cual se encuentra bajo extremo riesgo. La seguridad de la información es un problema complejo, y por lo tanto es necesario preparar a profundidad profesionales de diferentes perfiles que no solo conozcan y sepan aplicar adecuadamente los elementos tecnológicos, sino que también estén totalmente formados para garantizar la continuidad del negocio, manejando los incidentes informáticos, realizando la respectiva auditoría, levantando servicios e información perdida, recaudando las evidencias digitales e incluso salvaguardando la integridad de éstas en aras de buscar los responsables. Estos profesionales deberán ser capaces de aplicar su conocimiento a la organización para asegurar los sistemas de información.

El Curso de Primeros Respondientes de Incidentes Informáticos (CPRI) fue diseñado para que en cada empresa y entidad del País se prepare a un “Primer Respondiente de Incidentes Informáticos”, entendiendo por éste a un experto en el manejo de casos informáticos y recaudo de evidencias digitales que sean válidos en procesos judiciales. Este curso dará a los participantes las competencias y técnicas para convertirse en un experto en la atención como primer respondiente de incidentes informáticos, por medio de competencias en: la recuperación de la información luego de que un medio de almacenamiento ha sido borrado, análisis y realización del seguimiento post-incidente para la recuperación de información y asegurar la continuidad de las actividades de la organización luego de que ha presentado un fraude y/o delito informático, investigación de fraudes informáticos y recolectar, manejar, preparar, valorar, explicar e interpretar, con una concepción crítica y fundamentada, evidencias en formatos digitales como, pruebas digitales, grabaciones digitales, correos electrónicos firmas electrónicas, información contenida en sim cards, teléfonos celulares y computadores, mensajes de texto, páginas de internet, videos multimedia y en general pruebas técnicas, conocimiento y manejo de los criterios de la inspección judicial como prueba, dentro de los diferentes tipos de procesos judiciales, entre otras.

El curso estará comprendido por cuatro (4) módulos que permiten llevar a cabo el desarrollo de los temas de forma teórico-prácticos y su aplicación en las organizaciones para la atención de un incidente informático como primer respondiente. Dentro de los módulos se encuentran:

- MÓDULO I. Conceptos básicos
- MÓDULO II. Técnicas de Ingeniería Social
- MÓDULO III. Gestión de la Seguridad Informática
- MÓDULO IV. Respuesta ante incidentes de seguridad de la información.

ANEXO - GUION OBRA TEATRAL

SEGURITO: PERIODISTA SEGURITO QUE SIEMPRE QUIERE LLEGAR A LA VERDAD DE UNA MANERA SOBRADA Y MUY INTELIGENTE.

LOLA SEGURA: PERSONAJE IMPERTINENTE Y MUY DESCUIDADA.

TEMA: CONDUCTA ESPERADA PARA BENEFICIOS DE LA SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información son nuestro medio de protección.

Llegan los actores al lugar de trabajo invitando a los colaboradores a una nueva emisión de su noticiero (s.m.s: Seguridad de la Federación Colombiana de Municipios) con música de noticiero y un poco de algarabía de parte de los presentadores (actores).

El actor presentador del noticiero está caracterizado muy parecido a Segurito. La actriz es la antagonista del sketch.

OFF: ATENCIÓN, ATENCIÓN BIENVENIDOS A LA PRIMERA, PRIMERISIMA EMISIÓN DE SU NOTICIERO S.M.S. EL NOTICIERO QUE NO TIENE PELOS EN LA LENGUA PARA DECIR LA VERDAD, VERDADERA DE LO QUE NECESITAN LOS COLABORADORES PARA CONOCER LA SEGURIDAD-SEGURA.

LOS ACTORES ENTRAN A ESCENA COMO CUANDO UN PERIODISTA LLEGA A CUBRIR UNA GRAN NOTICIA, UNA PRIMICIA NOTICIOSA.

SEGURITO: Buenos días estamos en vivo y en directo desde el lugar de la noticia con todos los colaboradores de la Federación Colombiana de Municipios, ¿y por qué estamos aquí? Para conocer a los protagonistas de algunas situaciones que se presentan con la seguridad de nuestra información, conoceremos de parte de ellos cuáles son sus inquietudes y conocimientos referentes a esta gran noticia.

Soy Segurito y este es nuestro informe especial.

(EN ESTE MOMENTO SEGURITO SE DIRIGE CON LA CAMARA A ENTREVISTAR A CADA COLABORADOR PREGUNTANDOLE SU NOMBRE Y EL TRABAJO QUE TIENE EN LA FEDERACION, ESTA PARTE VA A SER ALGO JOCOSA, DEPENDIENDO DE LAS PREGUNTAS QUE SE LE HACEN AL ENTREVISTADO)

ALGUNAS PREGUNTAS QUE SE LE PUEDEN HACER COMO:

¿COMO PROTEGE USTED SU INFORMACION?

R= LIBRE

¿CUALES SON LOS TRES PILARES QUE NO DEBES OLVIDAR PARA HACER TU INFORMACIÓN SEGURA?

R= CONFIDENCIALIDAD, DISPONIBILIDAD E INTEGRIDAD

EN ESE MOMENTO NUESTRO CAMAROGRAFO EMPIEZA HACER APUNTES REFERENTES A ESTA PROBLEMÁTICA.

LOLA SEGURA: La información es un activo muy valioso en la Federación, su seguridad es responsabilidad de todos.

SEGURITO: Así es mi querida Lola Segura no lo olviden con la seguridad de la información de la Federación no se juega.

SEGURITO: continuamos con nuestra información desde el lugar de la noticia y llego el momento de premiar a nuestros conocedores de la seguridad con este espectacular perrito inflado (se lo muestra a los colaboradores y les pregunta.)

SEGURITO: ¿Quién quiere ganarse este perrito?

LOLA SEGURA: Yo, yo, yo quiero ganarme ese perrito para que me cuide mi casa, para que muerda a los ladrones y no me vuelvan a robar mis cosas (llora).

SEGURITO: Tranquilo mi querida Lola Segura, para eso y más… estamos aquí en nuestra Federación Colombiana de Municipios.

SEGURITO: Vamos a retomar (saca una gaseosa o una bebida y se la toma con referencia a retomar)

SEGURITO: Seguimos en nuestra misión especial de seguridad con la Federación Colombiana de Municipios y sus colaboradores.

(Segurito se acerca desafiante a cualquiera del presente en cámara lenta y le dice muuuy misterioso hasta llegar muy cerca casi susurrado)

SEGURITO: Ten precaución, cada vez que te pares de tu puesto cierra siempre tu sesión del equipo……. ¿tú, (dirigiéndose a el entrevistado) si tú lo haces? ¿Cierras siempre tu sesión del equipo cuando te paras a tomar café, gaseosa, comer papitas, sacar fotocopias e ir a una reunión?

(Le pone el micrófono para que conteste) él va a contestar de una que sí y Segurito le dice que lo acompañe al puesto a ver si es cierto y si lo tiene cerrado le damos un chocolate y lo felicitamos si no… LOLA SEGURAA le baila y le dice ten cuidado con tu información (bailando y cantando)

LOLA SEGURA: Hey, hey Segurito ¿Por qué no le preguntas a alguno de nuestros invitados?.

Levante la mano el que ha entregado información personal, como: contraseñas, números importantes, información de la Federación a través de su correo electrónico personal o teléfono? El que se me sincere le entregare esta flor echa con globos de primera para que le entregue al novio o la novia y así no tiene que comprarle regalo de navidad jajajajajaja.

¿A ver quién? (seguramente ninguno lo va hacer, pero si alguien dice que si…le explicaremos el por qué no deben hacerlo.)

SUENA MUSICA DE NOTICIA DE ÚLTIMA HORA…

SEGURITO: Atención noticia de última hora, noticia de última hora……Si evidencias un incidente de seguridad de la información, repórtalo inmediatamente y cuanto antes, no se quede callado denuncie.

EN ESE MOMENTO LOLA SEGURA TRATA DE INGRESAR A UNO DE LOS CUBICULOS DE ALGUN COLABORADOR EN ESE MOMENTO SEGURITO PREGUNTA QUIEN TRABAJA EN ESE LUGAR Y LE PREGUNTA:

SEGURITO: Oye dime que debes hacer en este momento si ves a alguien en tu área de trabajo, que no conoces o que de pronto tiene cara de malo, de buena gente, pero no lo conoces, de vendedor de minutos, de carnicero, de visitador médico, de guapetón, de actor llorón, de actor gringo etc. (en ese momento Lola Segura hace muchas muecas chistosas referentes a lo que vaya describiendo Segurito).

¿Qué haces tú por ejemplo? (Segurito se dirige a alguien del público y le pregunta que hace)

R: Debes llamar de inmediato al personal de seguridad y reportar el incidentes respectivo para que no vuelva a suceder.

EN ESE MOMENTO ATRAPAMOS A LOLA SEGURA COMO A ENCARCELARLA Y EL EMPIEZA A GRITAR.

SEGURITO: Recuerden que las contraseñas son como los calzoncillos: úsalos todos los días, cámbialos frecuentemente y no se los prestes a nadie…lo recuerdas……

¿Quién me da otro ejemplo de contraseñas seguras? (se le pregunta a el público…y el que responde bien o da un buen ejemplo se le regala un chocolate o un globo dependiendo de la interacción que haga con Segurito)

EMPEZAMOS A HACER EL CIERRE DEL NOTICIERO EN ESE MOMENTO CON MUSICA Y PIDIENDOLE A TODOS QUE TENGAN ENCUENTA LOS SIGUIENTES PUNTOS ENTRE LOLA SEGURA Y SEGURITO LO VAN DICIENDO RAPIDAMENTE COMO UN CONTRAPUNTEO COMO SI FUERAN TITULARES NOTICIOSOS. (CON ALGUNOS ELEMENTOS VISUALES DONDE ESTEN ESCRITOS Y SE LE MUESTRAN AL PUBLICO MIENTRAS SE VAN NOMBRANDO)

SEGURITO: Confidencialidad, Disponibilidad e Integridad: Tres pilares que no debes olvidar para hacer tu información segura.
LOLA SEGURA: Nunca entregues información personal, como tus contraseñas, a través de correo electrónico o teléfono.
SEGURITO: Comunica los incidentes de seguridad de la información, lo antes posible

LOLA SEGURA: Conoce y practica las políticas de seguridad de la información de la Federación, son la guía para estar seguros.

SEGURITO: Utiliza los recursos informáticos, solo para tus labores asignadas.

LOLA SEGURA: A veces no todo es como parece, si vez algo sospechoso, repórtalo cuanto antes.

SEGURITO: Cuida la información impresa y digital de la Federación y la tuya, alguien puede usarla indebidamente.
LOLA SEGURA: Tu contraseña es la llave de tú información, descuidarla es muy grave.
SEGURITO: Cierra la sesión al levantarte de tu puesto de trabajo.

SEGURITO ENSEÑA AL PÚBLICO A UTILIZAR EL COMANDO: CTRL + Z,

Hasta aquí nuestro noticiero s.m.s con Lola Segura y Segurito
Y recuerde no se quede callado denuncieeeeeeeeeee…

SUENA MUSICA DE NOTICIERO Y SALEN LOS ACTORES A BUSCAR EL SIGUIENTE PISO.

ANEXO - GUIÓN VIDEO DE INDUCCIÓN Y REEDUCCIÓN

El formato a presentar es similar a:
https://www.youtube.com/watch?v=I4FCl4RZpqY
Fuente: Materia didáctico SuperHeng – Youtube.

Hola mi nombre es segurito y soy el encargado de enseñarte los aspectos más importantes de la seguridad de la información de la Federación Colombiana de Municipios.

En Federación trabajamos para fomentar e impulsar la seguridad de nuestra información, teniendo en cuenta que a diario está expuesta a infinidad de amenazas que pueden afectar su confidencialidad, integridad o disponibilidad y con ello afectar el logro de nuestra de misión institucional.
Las amenazas pueden provenir no solo del exterior sino también desde el interior de la entidad, las cuales se pueden aprovechar de las vulnerabilidades o brechas que podamos tener.

Para conocer, gestionar y reducir los riesgos de seguridad de la información, la entidad cuenta con el sistema de gestión de seguridad de la información el cual busca proteger los activos de información, entre los muchos de ellos, encontramos: los correos electrónicos, las bases de datos, contratos, el Sistema Integrado de Información sobre Multas y Sanciones por Infracciones de Tránsito SIMIT, consultas jurídicas, estadísticas e inclusive información relacionada con el programa de protección a alcaldes amenazados.

Como nos podemos dar cuenta la información se encuentra en diferentes soportes, como papel, medios magnéticos o sistemas de información, además es preciso tener en cuenta el ciclo de vida de la información, ya que lo que hoy puede ser crítico para la entidad puede perder su importancia con el tiempo.

Sabías que…
La política global de seguridad de la información establece que la información es un activo de valor crítico para la Federación Colombiana de Municipios y que los funcionarios y todos aquellos que tienen responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información deben adoptar los lineamientos establecidos en la POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. Estos lineamientos son establecidos con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información, así como minimizar los riesgos a los que se encuentra expuesta la información.

Recuerda:

- La confidencialidad implica el acceso a la información únicamente a quienes están autorizados.

- La integridad conlleva la protección de la exactitud o estado completo de la información
- La disponibilidad busca que la información se encuentre accesible o utilizable por parte de los autorizados en el momento que lo requieran.

Ahora presta atención a estas políticas, ten en cuenta que eres la pieza más importante para proteger la información que te ha sido asignada

- Utiliza la información únicamente para los fines que fue obtenida.

- Aquellos que intenten acceder a información para la cual no están autorizados, incurrirán en violación de la política.

- Las oficinas e instalaciones donde haya atención al público no deben permanecer abiertas y el equipo debe estar bloqueado cuando los funcionarios se levantan de sus puestos de trabajo, así sea por periodos cortos de tiempo.

- Debes permanecer con el carné que te identifica como funcionarios de la Federación Colombiana de Municipios, mientras permanezcan en las instalaciones de la entidad.

- Debes reportar a la dirección administrativa, a la mayor brevedad, cualquier sospecha de incidentes de seguridad de la información.

- Ten en cuenta que los visitantes que ingresan a la Federación, deben ser recibidos y estar acompañados por la persona a quien visitan durante su permanencia en las instalaciones de la misma.

- Debes garantizar que las descargas de archivos adjuntos de los correos electrónicos o descargados de Internet realizadas provienen de fuentes conocidas, seguras y exclusivas de acuerdo con las funciones encomendadas.

- Recuerda correr el software antivirus sobre archivos y/o documentos que son abiertos y/o ejecutados por primera vez y comunicarte con La Dirección de Tecnología al encontrar un virus.

- De ninguna manera o por ninguna circunstancia puedes compartir la identidad (usuario y contraseña), cada usuario es responsable por las acciones realizadas en cualquier recurso de información de la Federación Colombiana de Municipios.

Las siguientes son unas buenas prácticas que ayudaran a tener nuestra información segura

- Cuando recibas correos electrónicos sospechosos, por ejemplo, donde soliciten información personal, bancaria, nombres de usuario o contraseñas, no lo respondas, podrías ser víctima de fraude electrónico. Para todos los correos, verifica el origen y el destino antes de procesar la información.

- No expongas tu información personal, ni la compartas a través de la red con personal no autorizado.

- Utiliza contraseñas fuertes que incluyan mayúsculas, minúsculas, números y al menos un carácter especial. Asegúrate de que tu contraseña no sea fácil de deducir.

- No instales software no autorizado o pirata en los equipos de cómputo.

- Al tener información confidencial o sensible que deba ser desechada, asegúrate de destruirla, antes de enviarla a la basura, reutilizarla o reciclarla.

- Mantén tu escritorio de trabajo y su pantalla organizada y limpia. Recuerda no dejar a la vista documentos, datos sensibles o confidenciales.

Ahora ya lo sabes, tener nuestra información segura permite a la Federación contar con una buena imagen, cumplir requisitos legales (Ley 1581 de 2012, protección de datos personales; Ley 1712 de 2014, Transparencia y acceso a la información pública) y sobre todo cumplir su misión institucional.

Para finalizar recordemos que todos somos responsables de proteger la información de todas las amenazas que la puedan afectar y puede ser considerado una falta grave en nuestro trabajo. Contamos contigo.

9.4 Video de Charla y Sensibilizacion realizada en la FCM:

Ver video en Youtube desde la Url: https://www.youtube.com/watch?v=2YnUOEJ-ybE

10. ENTREGABLES ETAPA 3

10.1 Diseño del Centro de Respuestas para atención de Incidentes de seguridad – CSIRT

OBJETIVO

Administrar todos los incidentes y/o eventos de seguridad que se presenten con los activos de información de la FEDERACIÓN COLOMBIANA DE MUNICIPIOS, que atenten contra sus características de Integridad, confidencialidad y disponibilidad, y que éstos, sean atendidos eficaz y oportunamente, mediante el desarrollo de acciones correctivas que generen una base de datos de conocimiento, y con ello, actividades proactivas al interior de la organización.

ALCANCE

Inicia con la detección, registro y clasificación del incidente y/o evento de seguridad de la información; continua con su análisis e investigación; y finaliza con la contención y erradicación del mismo, estableciendo un plan de recuperación de aquellos activos de información afectados.

BASE LEGAL

Ley 527 de 1999

Ley 599 del 2000

Ley 1266 de 2008

Ley 1273 de 2009

Ley 1712 de 2014

Ley 1581 de 2012

Decreto 886 de 2014

Decreto 1377 de 2013

ISO/IEC 27001 versión 2013

ISO/IEC 27042 versión 2014

ISO/IEC 27037 versión 2012

Manual para Procedimientos de Cadena de Custodia

EQUIPO DE RESPUESTA A INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN (*ERISI*)

A continuación, se exponen los tópicos necesarios y requeridos para la creación y conformación de un Equipo de Respuesta a Incidentes en Seguridad de la Información, o conocidos también como: IRT (*Incident Response Team*), CSIRT (*Computer Security Incident Response Team*), CIRT (*Computer Incident Response Team*), CIRC (*Computer Incident Response Capability*) SIRT (*Security Incident Response Team*), SERT (*Security Emergency Response Team*), CERT (*Computer Emergency Response Team*), el cual gestionara los incidentes y/o eventos de seguridad de la información en la FEDERACIÓN COLOMBIANA DE MUNICIPIOS.

QUE ES EL *ERISI*

Es el equipo que ejecuta, coordina y apoya la respuesta a incidentes y/o eventos de seguridad de la información en la FEDERACIÓN COLOMBIANA DE MUNICIPIOS, y tiene como propósito, proteger la información y las infraestructuras críticas de la entidad, frente a cualquier tipo de amenaza.

MISIÓN

El equipo de Respuesta a Incidentes de Seguridad de la Información de la FEDERACIÓN COLOMBIANA DE MUNICIPIOS, administrará todos los incidentes de seguridad que se presenten y que atenten contra la integridad, disponibilidad y confidencialidad de la información, así como sobre aquellos recursos tecnológicos que la soporten, haciendo una clasificación del incidente, una recolección y aseguramiento de las evidencias, una contención, erradicación y recuperación de las plataformas e información afectadas, buscando la continuidad de negocio de la entidad.

MODELO DEL *ERISI*

Basados en el contexto de la FEDERACIÓN COLOMBIANA DE MUNICIPIOS, el modelo propuesto para el equipo *ERISI* es centralizado, es decir, este equipo se encargará de la administración de todas las incidencias de seguridad de la información que se presenten en la entidad, teniendo un único punto de contacto, y desde el cual, se coordinaran todas las actividades que deban ejecutarse con ocasión de los eventos registrados.

OBJETIVOS DEL EQUIPO *ERISI*

El Equipo de Respuesta a Incidentes de Seguridad de la Información tendrá como objetivos los siguientes:

- Coordinar de manera centralizada todos los incidentes de seguridad de la información e infraestructuras críticas de la FEDERACIÓN COLOMBIANA DE MUNICIPIOS, buscando la reducción de vulnerabilidades y amenazas, evitando el incremento de delitos informáticos y generando capacidades de detección, análisis y respuestas tempranas frente a estos eventos.
- Proteger la información sensible de la FEDERACIÓN COLOMBIANA DE MUNICIPIOS, así como sus infraestructuras críticas, generando continuidad en el servicio.
- Fomentar la confianza de los funcionarios de la FEDERACIÓN COLOMBIANA DE MUNICIPIOS en temas de seguridad de la información e informática, a través del cumplimiento de la política de seguridad de la entidad.
- Comunicar, promover y promocionar las mejores prácticas en temas de seguridad de la información e informática, buscando la prevención de incidentes y/o eventos de seguridad.
- Generar adecuados canales de comunicación y acuerdos interadministrativos que permitan denunciar, publicar y compartir aquella información, que con ocasión de la administración de incidentes y/o eventos pueda retroalimentarse, teniendo como ejes temáticos la seguridad de la información e informática.

SERVICIOS

El equipo *ERISI* de la FEDERACIÓN COLOMBIANA DE MUNICIPIOS ofrecerá servicios en tiempo real asociados a la administración de incidentes y/o eventos de seguridad que pongan en peligro la continuidad de negocio de la entidad, así como servicios proactivos que permitan prevenir la ocurrencia de éstos incidentes y/o eventos mediante acciones de sensibilización, educación y divulgación, auditorias de seguridad, evaluación de herramientas informáticas entre otras.

Servicios en tiempo real:

Detección y Análisis: Corresponde a la detección e identificación de los posibles incidentes y/o eventos de seguridad que son detectados a través de las diferentes fuentes de información que posee la FCM, los cuales deben ser analizados, determinando la credibilidad de los datos y de la fuente, la existencia del hecho y la clasificación del mismo de acuerdo a su criticidad, teniendo en cuenta la ponderación de los activos de información de la entidad.

Recolección y análisis de evidencias: Son servicios orientados al aseguramiento, recolección y análisis de las evidencias, usualmente digitales, que son obtenidas en el lugar de la escena, como resultado de la administración del incidente y/o evento de seguridad de la información.

Contención: Es el servicio tendiente a evitar la propagación de la amenaza que ocasiono el incidente de seguridad de la información.

Erradicación: Servicio que consiste en la eliminación de cualquier tipo de rastro que con ocasión de la amenaza pudiera existir.

Recuperación: Consiste en la restauración inmediata de la arquitectura y/o servicios de *TI* afectados.

Comunicación: Son las comunicaciones internas y externas que se deban expresarse con motivo del incidente de seguridad de la información.

Servicios proactivos

Los servicios proactivos se refieren a actividades orientadas a la prevención de incidentes de seguridad, basados en temas de sensibilización y formación a los funcionarios de la FERDERACIÓN COLOMBIANA DE MUNICIPIOS, dentro de los cuales se resaltan:

- Educación y Entrenamiento
- Evaluación de Productos
- Auditorias de Seguridad

RECURSO HUMANO Y COMPETENCIAS

El equipo *ERISI* de la FEDERACIÓN COLOMBIANA DE MUNICIPIOS debe contar con profesionales en temas de seguridad de la información que tengan competencias específicas en diferentes áreas, basados en las necesidades que se puedan requerirse frente a la administración de incidentes y/o eventos de seguridad.

A continuación, se sugieren los perfiles que deberían hacer parte del equipo:

- **Especialistas en el tratamiento de incidentes**: Funcionarios y/o personal externo capacitados para la administración y tratamiento de incidentes de seguridad de la información y administración de evidencia digital.
- **Especialistas en el tratamiento de vulnerabilidades**: Funcionarios y/o personal externo que está especializado en el tratamiento de deficiencias o fallos en la programación o configuración de los sistemas informáticos de la entidad.

- **Especialistas en análisis y seguimiento de casos**: Son los funcionarios y/o personal externo responsables de llevar los registros y brindar el seguimiento adecuado de los incidentes y/o eventos de seguridad y su análisis respectivo.
- **Especialistas en plataformas operacionales**: Funcionarios y/o personal externo experimentados y especializados en el manejo de plataformas informáticas que tengan dominio en los equipos, así como en los diferentes sistemas operativos y sistemas informáticos que posee la entidad

Es importante resaltar que los funcionarios que hagan parte del equipo de respuesta a incidentes de seguridad de la información deben tener unas competencias básicas, las cuales se resaltan a continuación:

- Trabajo en equipo
- Trabajo orientado al logro
- Habilidad de comunicación y relaciones interpersonales
- Personas dedicadas, innovadoras, detallistas, flexibles y metódicas
- Maneje coherentemente los valores personales y de entidad

Se expondrá en detalle, aquellos servicios que en tiempo real ofrecerá el Equipo de Respuesta a Incidentes de Seguridad de la Información de la FEDERACIÓN COLOMBIANA DE MUNICIPIOS.

DETECCIÓN Y ANÁLISIS

Los incidentes y/o eventos de seguridad de la información podrán ser identificados y/o detectados a través de las diferentes fuentes de información, dentro de las cuales se resaltan:

- Alertas de las plataformas de *TI*
- Caídas del sistema
- Ciudadanía
- Comunicaciones anónimas
- Consolas de antivirus
- Mesa de Servicio
- Redes sociales
- Registros de las herramientas administrativas
- Reportes de usuario

Los eventos y/o incidente de seguridad de la información serán registrados mediante los formatos que destine la FCM, en donde, estarán plasmados aquellos datos relacionados con las fuentes de información que lo reportan, una valoración de su credibilidad, así como, la ponderación de la información suministrada, lo anterior, con la finalidad de establecer su credibilidad, y con ello, determinar la ocurrencia del hecho.

En este documento se registrará información adicional asociada con la cronología del incidente, el activo de información afectado y su criticidad, de acuerdo con la matriz de activos definida por entidad, entre otros datos, que permitan identificar plenamente la incidencia ocurrida.

Los niveles de clasificación de los incidentes y/o eventos de seguridad son:

Tabla 28:Niveles de criticidad de los incidentes y/o eventos de Seguridad

NIVEL	NOMBRE	TIEMPO DE ATENCION
1	BAJO O NULO	1 SEMANA
2	MEDIO	2 DÍAS
3	ALTO	12 HORAS
4	CRÍTICO	1 HORA

La ponderación para la clasificación de estos niveles es la siguiente:

Bajo o Nulo: este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o denunciados como posibles amenazas para los activos de información, es decir, que pueden impactar sus características de integridad y/o confidencialidad y/o disponibilidad, sin embargo, los controles de seguridad resultan efectivos anulando cualquier impacto para la FEDERACIÓN COLOMBIANA DE MUNICIPIOS.

Medio: este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o denunciados como posibles amenazas, que pueden afectar los activos de información de la entidad, impactando de modo limitado sus características de integridad y/o confidencialidad y/o disponibilidad frente a un activo no crítico para la Federación.

Alto: este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o denunciados, porque en ellos, es posible establecer una amenaza sobre los activos de información capaz de impactar de manera considerable las características de integridad y/o confidencialidad y/o disponibilidad de un activo no crítico para FCM.

Crítico: este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o denunciados, porque en ellos, es posible establecer una amenaza sobre los activos de información capaz de impactar de manera

considerable las características de integridad y/o confidencialidad y/o disponibilidad de un activo crítico para la entidad.

El Grupo *ERISI* de la FEDERACIÓN COLOMBIANA DE MUNICIPIOS, o quien haga sus veces, deberá realizar un análisis del incidente y/o evento de seguridad para desarrollar un plan de acción, en el cual, quedarán plasmadas las actividades que se ejecutarán frente a la recolección de las evidencias, la contención y erradicación del incidente, así como la recuperación del activo de información en caso de que se halla afectado la continuidad del negocio.

RECOLECCIÓN, ASEGURAMIENTO Y ANÁLISIS DE EVIDENCIAS DIGITALES

Estas actividades comprenden el hallazgo, recaudo, aseguramiento, transporte, custodia y análisis de las evidencias digitales que con ocasión de un incidente y/o evento de seguridad de la información se haya recolectado por parte del Grupo *ERISI* en las diferentes oficinas de la FCM.

Las evidencias que podrían encontrarse y recaudarse con ocasión del incidente de seguridad de la información son entre otras:

- *Log* Servidores
- *Log* de aplicaciones
- *Log* de Sistemas
- *Log* de Herramientas de Seguridad
- Computadores de Escritorio
- Computadores Portátiles
- *Smartphone*
- *Tablet*
- Buzones de correo electrónico
- Entre otros

El recaudo de la evidencia debe documentarse en el lugar en donde éstas se encuentren – lugar de la escena –, para ello, deberá emplearse métodos de fijación, dentro de los cuales se encuentran, los descriptivos y fotográficos, y/o video gráficos, y/o planimétricos.

El aseguramiento de la evidencia digital se hace mediante técnicas propias de la informática forense, es decir, se identifica inicialmente la información contenida en los medios de almacenamiento recaudados, mediante técnicas

criptográficas denominadas *HASHING* o *CHECKSUMS*; así mismo, se extraen copias idénticas de los datos a través de la extracción de imágenes forenses físicas o lógicas, y de ser posible, se extrae una estampa de tiempo –*Time Stamping*–; finalmente, se realiza el diligenciamiento de la Cadena de Custodia, cumpliendo de esta manera con los preceptos básicos frente al aseguramiento de pruebas digitales y/o computacionales.

Las evidencias encontradas y recolectadas serán analizadas exhaustivamente por el Equipo de Respuesta a Incidentes de Seguridad de la Información de la entidad y/o un contratista especializado en estos temas, esto con la finalidad, de encontrar información pertinente para la investigación, logrando determinar y comprobar la ocurrencia de los hechos e identificación de los responsables.

Para la realización de las actividades de recaudo y análisis de evidencias computacionales, se requieren, por lo menos, los siguientes elementos Forenses:

- Portátiles Forenses
- Clonadores Forenses
- Laboratorios Fijos de Análisis Forense
- *Software* de adquisición de imágenes Forenses
- *Software* de Recolección de Evidencias
- Kit de Respuesta a Incidentes
- *Software* de Análisis forense
- Medios de almacenamiento

CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

Teniendo en cuenta el impacto del incidente de seguridad de la información, el cual estará ponderado por la criticidad del activo de información involucrado, es necesario y pertinente que se hagan las acciones correctivas, esto es, ejecutar actividades de contención, erradicación y recuperación, tal y como se muestra a continuación:

Contención

Son aquellas acciones tendientes a evitar la propagación de la amenaza que ocasiono el incidente de seguridad de la información detectado, esto, para evitar daños adicionales sobre los activos de información de la FEDERACIÓN COLOMBIANA DE MUNICIPIOS, así como sobre su infraestructura de *TI*.

Esta acción debe enfocarse en la detección del incidente y la estrategia de contención, tal como se muestra en la siguiente tabla:

Tabla 29: Estrategia de Contención de Incidentes de Seguridad

INCIDENTE DE SEGURIDAD	ESTRATEGIA
Accesos no Autorizados	Bloqueos de cuenta Apagado de la máquina Bloqueo de puertos
Códigos Maliciosos	Desconexión de la red del equipo afectado Bloqueo de Puertos Actualización de Antivirus y *Antimalware*
Reconocimiento	Nuevas reglas de filtrado Bloqueo de Puertos
Corrupción	Retiro de funcionario Bloqueo de Cuentas

Erradicación y Recuperación

Una vez el incidente de seguridad de la información es contenido, este debe erradicarse, es decir, eliminar cualquier tipo de rastro que pudiera existir con ocasión de comportamiento inusual sobre los activos de información y/o infraestructura de *TI* del FCM.

Por otra parte, debe existir una restauración inmediata de la arquitectura y/o servicios de *TI* afectados, que devuelvan de manera pronta y eficaz, no solo las funcionalidades a los sistemas, sino, que permitan realizar actividades inmediatas de endurecimiento –*Hardening*–, lo anterior, con el propósito de cerrar las vulnerabilidades detectadas.

A continuación, se exponen las estrategias de recuperación:

Tabla 30: Estrategia de Contención de Incidentes de Seguridad

INCIDENTE DE SEGURIDAD	ESTRATEGIA
Denegación de Servicios	Restitución del servicio caído Restauración de *Backups*
Códigos Maliciosos	Corrección de Efectos Restauración de *Backups* Actualización de Antivirus
Vandalismo	Nuevas reglas de filtrado Bloqueo de Puertos
Corrupción	Recuperación del Sitio *Web* Restauración de *Backups*
Intrusión	Restauración de equipos y servicios Recuperación de los Datos Restauración de *Backups*

COMUNICACIÓN

A través del Comité de Seguridad de la Información de la FEDERACIÓN COLOMBIANA DE MUNICIPIOS, se tomarán las decisiones que sean necesarias y pertinentes frente a las comunicaciones internas y externas que se deban expresarse con motivo del incidente de seguridad de la información, coordinando, de ser necesario, las denuncias que deban ser instauradas ante los diferentes entes de control, aportando como soporte de ésta, todas las evidencias recaudadas por parte del equipo ERISI, o quien haya hecho sus veces, así como aquellos informes desarrollados con ocasión de la administración del incidente por parte de este equipo de trabajo.

BASE DE DATOS DE CONOCIMIENTO

La adecuada administración de los incidentes de seguridad de la información, permite generar una mejora continua, y con ello, un repositorio de lecciones aprendidas, que permiten retroalimentar todos los temas de seguridad al interior de la Federación Nacional de Municipios, y por ende, es necesario que el equipo *ERISI* mantenga un registro de lecciones aprendidas debidamente documentado; puesto que con ello, se pueden conocer los pormenores frente a la gestión de incidentes de seguridad, las acciones ejecutadas, los recursos asignados, los resultados, las dificultades, información que permite realizar acciones correctivas frente a situaciones similares, en caso de volverse a presentar.

Desarrollo

Tabla 31: Desarrollo y/o Operación del CSIRT.

Nº	ACTIVIDAD	RESPONSABLE	DOCUMENTO
1 **©**	***1.1. Notificación del Incidente:*** Se hace la detección del incidente y/o evento de seguridad cuando este es evidenciado a través de las diferentes alertas y/o medios de comunicación que posee la Federación Colombiana de Municipios, Ejemplos de ello son: alertas de las plataformas de *TI*, caídas del sistema, reportes de usuario, registros de las herramientas administrativas, consolas de antivirus, comunicaciones anónimas, redes sociales, Mesa de servicio, ciudadanía, entre otros.	Usuarios Administradores de *TI*	Correo electrónico Llamada telefónica
2 **©**	***2.1. Registro del Incidente:*** Todo incidente y/o evento de seguridad de la información deberá ser registrado en el formato destinado para tal fin, documentando los datos solicitados en el mismo, tales como: línea cronológica del incidente, activo de información involucrado, identificación de las fuentes de información, entre otros.	Mesa de Ayuda Grupo *ERISI* o quien haga sus veces	Reporte y/o informe de administración de Incidente y/o evento de Seguridad

Nº	ACTIVIDAD	RESPONSABLE	DOCUMENTO
3	***2.1. Clasificación del Incidente:*** Tomando como referencia la tabla de clasificación de los incidentes y/o eventos de seguridad (Ver tabla 1 de este procedimiento), éste deberá ser ponderado estableciendo el impacto causado a la Federación Colombiana de Municipios y los tiempos de respuesta por parte del Grupo *ERISI*, o quien haga sus veces. Todo esto, deberá ser retroalimentado en el reporte o informe de administración del incidente u/o evento de Seguridad.	Mesa de Ayuda Grupo *ERISI* o quien haga sus veces	Reporte y/o informe de administración de Incidente y/o evento de Seguridad
4 ©	***2.1. Realización del Plan de Acción:*** El Grupo *ERISI,* o quien haga sus veces, deberá realizar un plan de acción que le permita definir las actividades que se deben ejecutar con ocasión de la administración del Incidente de Seguridad. Para ello, deberá determinar los lugares a intervenir frente al recaudo de las evidencias, las acciones de contención, erradicación y recuperación frente a los servicios y/o plataformas afectadas por la incidencia. Dentro de la planeación para la atención del incidente y/o evento de seguridad, deberá tener en cuenta los tiempos, así como aquellas necesidades de recursos logísticos, humanos, áreas que	Grupo *ERISI* o quien haga sus veces	Plan de Acción

Nº	ACTIVIDAD	RESPONSABLE	DOCUMENTO
	deben involucrarse, entre otros aspectos.		
5 **©**	***2.1. Manejo de escena y recolección de evidencias*** Se deberán recolectar las evidencias en las diferentes oficinas de la Federación Colombiana de Municipios que con ocasión del incidente y/o evento de seguridad existan. Para ello, se aplicarán los lineamientos propios de Cadena de Custodia e Informática Forense, preservando, ante todo, el valor probatorio de las pruebas que se recolecten.	Grupo ERISI o quien haga sus veces	Informe de Recolección de Evidencias y Formatos de Cadena de Custodia Evidencias Digitales
6 **©**	***5.1. Ejecución Plan de Contención:*** El Grupo *ERISI*, o quien haga sus veces, con apoyo de las Áreas de Tecnología de la Federación Colombiana de Municipios, deberá realizar una contención del incidente, evitando cualquier tipo de propagación que pueda seguir afectado los activos de información de la entidad.	Grupo ERISI o quien haga sus veces Áreas de TI	Informe de Contención del incidente de seguridad de la Información

Nº	ACTIVIDAD	RESPONSABLE	DOCUMENTO
7 **©**	***7.1. Realización del Plan de Erradicación y Recuperación:*** El Grupo *ERISI*, o quien haga sus veces, con apoyo de las áreas de Tecnología de la Federación Colombiana de Municipios, deberá eliminar cualquier tipo de rastro que pudiera existir con ocasión de la incidencia presentada. Además, deberá elaborar un plan de remediación, si es del caso, de todos aquellos activos de información que pudieron estar impactados, con la finalidad de poder cerrar las vulnerabilidades detectadas.	Grupo *ERISI o* quien haga sus veces Áreas de TI	Informe de Erradicación y Remediación
8 **©**	***8.1. Notificaciones y Comunicaciones:*** Según las disposiciones del Comité de Seguridad de la Información, y con el concurso de la Oficina de prensa y la Oficina Jurídica de la FCM, los incidentes podrán ser notificados y denunciados a los entes de control según sea el caso.	Comité de Seguridad de la Información Funcionarios de prensa Oficina Jurídico Oficina de Prensa	Informe de Recolección de Evidencias y Cadenas de Custodia Evidencias Digitales
9 **©**	***8.1. Registro Base de Datos de Conocimiento:*** Se hará un registro detallado de toda gestión de incidentes de seguridad evidenciados, con el fin de poder desarrollar acciones correctivas para posteriores actividades.	Grupo *ERISI* o quien haga sus veces	Reporte y/o informe de administración de Incidente y/o evento de Seguridad Formato Plan de Acción Informe de recolección de Evidencias. Informe de Contención del

Nº	ACTIVIDAD	RESPONSABLE	DOCUMENTO
			incidente de seguridad de la Información Informe de Erradicación y remediación.
10	**10.1. Cierre del incidente y/o evento de Seguridad de la Información:** El grupo *ERISI* hará el cierre del incidente de Seguridad de la Información.	Grupo *ERISI* o quien haga sus veces	Reporte y/o informe de administración de Incidente y/o evento de Seguridad

© → Punto de Control

10.2 Diseño/Revisión de las metodologías y procedimientos forenses que debe seguir la Federación Colombiana de Municipios – Dirección Nacional SIMIT.

Se detecto en la entidad que se debe implementar procedimiento en la administración de evidencias digitales en el marco de procedimientos forenses.

A continuación se recomienda el siguiente procedimiento:

Procedimiento para el hallazgo, recaudo, identificación, embalaje, transporte y custodia de la evidencia de tipo digital

OBJETIVO

Realizar el adecuado hallazgo, recaudo, identificación, embalaje, rotulado, transporte y custodia de la evidencia de tipo digital, recaudada en las instalaciones de la FEDERACIÓN COLOMBIANA DE MUNICIPIOS, de tal manera, que su contenido lógico (documentos electrónicos y mensajes de datos) preserve sus características de integridad, confidencialidad, disponibilidad, no repudio, originalidad, mismidad, autenticidad, entre otras, logrando mantener su valor probatorio y ser presentadas en procesos disciplinarios y/o judiciales y/o administrativos si así fuera el caso.

ALCANCE

Aplica a los funcionarios de la FEDERACIÓN COLOMBIANA DE MUNICIPIOS que realizan el recaudo de evidencias digitales como resultado de la administración de incidentes y/o eventos de seguridad de la información.

BASE LEGAL

Ley 527 de 1999

Ley 599 del 2000

Ley 1266 de 2008

Ley 1273 de 2009

Ley 1712 de 2014

Ley 1581 de 2012

Decreto 886 de 2014

Decreto 1377 de 2013

ISO/IEC 27001 versión 2013

ISO/IEC 27042 versión 2014

ISO/IEC 27037 versión 2012

Manual para Procedimientos de Cadena de Custodia

DEFINICIONES

A continuación, se mostrarán los términos más utilizados en éste documento, y que requieren de una interpretación clara y precisa para su entendimiento y aplicación.

ANTIVIRUS: Software capacitado para prevenir y realizar la búsqueda de código malicioso y de toda aquella programación que pueda ser potencialmente peligrosa para el sistema[7].

BLOQUEADOR: Dispositivo de Hardware que protegen un dispositivo de almacenamiento contra escritura para evitar modificaciones sobre el mismo[8]**.**

DATOS VOLATILES: Es aquella información que se encuentra almacenada en la memoria *RAM* y en donde puede existir evidencia frente al evento o incidente de seguridad que se está administrando, la cual puede desaparecer una vez la maquina es apagada y jamás ser recuperada[9].

ELEMENTOS MATERIALES DE PRUEBA: Son todos los materiales u objetos (sólidos, líquidos o gaseosos), que pueden servir para la determinación de la verdad durante la investigación, es un medio de prueba real y tangible (que se puede ver, tocar, oler, pesar o medir); para que tengan valor probatorio deben ser debidamente recolectados, protegidos, embalados, rotulados, transportados y entregados al Servidor competente, manejando la cadena de custodia[10].

---

[7] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

[8] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

[9] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

[10] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

ESTAMPA CRONOLOGICA: El estampado cronológico es un servicio mediante el cual se puede garantizar la existencia de un documento (o mensaje de datos en general) en un determinado instante de tiempo. Mediante la emisión de una estampa de tiempo es posible garantizar el instante de creación, modificación, recepción, etc., de un determinado mensaje de datos impidiendo su posterior alteración, haciendo uso de la hora legal colombiana[11].

EVIDENCIA DIGITAL: También conocida como evidencia computacional, única y conocida como: registros o archivos generados por computador u otro medio equivalente, registros o archivos no generados sino simplemente almacenados por o en computadores o medios equivalentes y registros o archivos híbridos que incluyen tanto registros generados por computador o medio equivalente como almacenados en los mismos[12].

***HARDWARE*:** Se denomina *hardware* o soporte físico al conjunto de elementos materiales que componen un computador. En dicho conjunto se incluyen los dispositivos electrónicos y electromecánicos, circuitos, cables, tarjetas, armarios o cajas, periféricos de todo tipo y otros elementos físicos[13].

***HASH* o HUELLA DIGITAL**: Son funciones algorítmicas que tiene como entrada un conjunto de elementos, que usualmente son cadenas y las convierte en un rango de salida finito, normalmente cadenas de longitud fija; Estas Cadenas pueden de 32 o 40 bits y permite identificar de una manera única e inequívoca un archivo digital sin importar su extensión[14].

---

[11] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

[12] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

[13] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

[14] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

INFORMÁTICA: La Informática es el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de un computador (llamado también ordenador o computadora)[15].

MD5: (Abreviatura de *Message-Digest Algorithm* 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado[16].

METADATOS: Literalmente «sobre datos», son datos que describen otros datos. Es una información de la información, es decir, son las propiedades que posee cada uno de los archivos al momento de ser creados, y estos van cambiando en la medida que el usuario realiza ingresos y/o modificaciones sobre el mismo[17].

PULSERA O MANILLA ANTIESTÁTICA: Es un elemento de protección, protege los componentes electrónicos de descargas de electricidad estática con la que se carga el cuerpo humano, y que les puede afectar y en algunos casos incluso destruir[18].

Nota: Todos los conceptos contenidos en este documento que no se encuentren plasmados en éste ítem, pueden ser consultados a través de diccionarios especializados de Informática.

---

[15] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

[16] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

[17] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

[18] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

CONDICIONES GENERALES

MARCO TEÓRICO

La evidencia digital es todo documento y/o mensaje de datos de origen electrónico presente en medios de almacenamiento, en donde es posible encontrar información relacionada con incidentes y/o eventos que ponen en peligro la seguridad de la información, convirtiéndose en pruebas que soporten procesos administrativos y/o judiciales, por ende, la adecuada administración de ésta es fundamental, desde el mismo momento de su hallazgo, ya que cualquier error, podría invalidarla, y, en consecuencia, generar una inadmisibilidad probatoria.

A continuación, se relacionarán unas recomendaciones extraídas de los estándares internacionales más importantes frente a la administración de este tipo de evidencias:

- Seguir estricto cumplimiento a las políticas de seguridad de la información de la FEDERACION COLOMBIANA DE MUNICIPIOS, relacionadas con administración de evidencia digital.

- Capturar la escena del incidente y/o evento de seguridad lo más exacta posible.

- Al intervenir una escena o lugar de los hechos en donde se encuentra evidencia digital, se deben mantener notas detalladas, éstas deben incluir fechas y horas, si es posible, generar reportes automáticos con la información recaudada, lo anterior para que pueda ser considerado como evidencia.

- Establecer las diferencias entre el reloj del sistema y la hora de referencia internacional *GMT* (*Greenwich Mean Time*).

- Minimizar los cambios en los datos que se han recolectado, se debe evitar actualizaciones de horas, fechas en los archivos y/o directorios que puedan llegar a ser recolectados.

- Documentar todo lo que se haga en la escena, y posteriormente, recolecte las evidencias.

- Aunque es necesario indicar que los procedimientos de atención a incidencias y/o eventos informáticos son realizables, debe asegurar su viabilidad y funcionamiento en un momento de crisis, de acuerdo a los planes implementados por la FEDERACIÓN COLOMBIANA DE MUNICIPIOS.

- La revisión de cada dispositivo es importante, por ende, es necesario ser metódico cuando se recolecte la evidencia digital.

- Recolectar las evidencias digitales desde lo más volátil a lo menos volátil.

- El análisis de la evidencia digital, debe realizarse sobre imágenes forenses, es decir, sobre copias binaras del medio origen.

ACTIVIDADES A DESARROLLAR

Se explicará la forma correcta de administrar las evidencias de tipo digital que sean encontradas en el lugar de la escena – FEDERACIÓN COLOMBIANA DE MUNICIPIOS –, como resultado de la investigación con ocasión de un incidente y/o evento de seguridad de la información, y de cómo asegurar ésta, frente a temas de cadena de custodia, de tal manera, que mantenga su valor probatorio.

MEDIOS DE ALMACENAMIENTO TECNOLÓGICO

Descripción general: Recaudar diferentes evidencias de tipo digital (discos duros, dispositivos drive flash, memorias *USB, CD ROM, DVD, SIM*, agendas digitales, celulares, entre otros), que puedan ser halladas como resultado de la administración de un incidente y/o evento de seguridad de la Información en la FEDERACIÓN COLOMBIANA DE MUNICIPIOS.

Se utilizarán herramientas forenses que permitan la protección de los datos y/o información contenida en éstos medios de almacenamiento de tipo tecnológico al momento de su recaudo.

Desarrollo de la actividad: Cuando se llegue al lugar en donde se ejecutará la actividad – lugar de la escena –, se deben buscar todos los medios de almacenamiento de tipo tecnológico que hayan sido definidos como relevantes por parte del equipo de trabajo *ERISI*, o quien haga sus veces.

Si se encuentra un computador (es) encendido (s), se evaluará, y de ser viable (esto debe ser definido por el funcionario líder del Equipo *ERISI* o quien haga sus veces) el recaudo de los datos volátiles y/o los metadatos - *Ver instructivo para la recolección de datos volátiles -,* y/o huellas digitales - *Ver instructivo para la extracción de la huella HASH* - de cada uno de los equipo de cómputo; es importante resaltar que la información extraída (datos volátiles y/o metadatos y/o huella digital) debe ser exportada a un medio de almacenamiento externo (memoria *USB*, disco duro externo, entre otros), haciendo especial énfasis en que éstos datos **NO PUEDEN SER** almacenados en el equipo que se está interviniendo.

Nota: El medio de almacenamiento al que se hace referencia con ocasión de la exportación de los datos volátiles y/o metadatos y/o huella digital, debe estar previamente esterilizado, es decir, debió pasar por un procedimiento de borrado seguro.

En caso de tener que revisar directamente la información y/o datos contenidos en un computador y/o medio de almacenamiento de tipo tecnológico en el desarrollo de la administración del incidente y/o evento de seguridad de la información, éste procedimiento deberá realizarse con herramientas forenses que permitan un análisis en vivo (*life analysis*), es decir, que se pueda ver el contenido del o los archivo (s) generando una protección frente a su metadata; adicionalmente el software que se emplee para realizar este análisis deberá tener la opción de ejecución mas no de instalación, es decir, deberá ser un programa que utilice los recursos de la memoria *RAM* para su ejecución, de tal manera que no se llegue a modificar ningún registro del sistema.

Una vez se determine cuál será la evidencia (s) que se recaudara por parte del equipo *ERISI* o quien hago sus veces, se deberá extraer una imagen forense del contenido total o parcial de los datos, esto mediante la utilización de un *software* forense especializado para este tipo de actividades - *Ver instructivo para la extracción de Imágenes Forenses* - teniendo como premisa fundamental, la protección de la información y/o los datos contenidos en el medio de almacenamiento original.

Según sea el caso, se utilizan bloqueadores de escritura que puede ser de *hardwar*e y/o *software*, con la finalidad de que los archivos pasen del medio original al medio destino sin que exista ninguna modificación en su contenido, particularmente de sus propiedades.

Es importante resaltar que se hará necesario el diligenciamiento del formato denominado – *Formato información técnica de la extracción de la imagen Forense* –, en el cual se consignan los datos asociados a la extracción de la imagen forense, así mismo, se deberán diligenciar los formatos correspondientes a la cadena de custodia, los cuales deberán estar anexos con la evidencia recaudada - *Formato de rotulo de evidencia y Formato de registro de continuidad* -.

Nota: El procedimiento debe ser documentado a través de los diferentes medios de fijación como son el descriptivo y fotográfico y/o video gráfico.

Como resultado del aseguramiento de la evidencia digital, se tendrá que verificar que esta(s) posea(n) lo siguiente:

- Extracción de la imagen forense (Física y/o Lógica)
- Formato debidamente diligenciado de la extracción técnica de la imagen forense
- Identificación de la evidencia a través de la huella digital bajo metodologías *MD5* y/o *SHA1*, o las que para la fecha de las actividades pueda llegar a ser válida
- Cadena de Custodia con sus respectivos formatos
- Medios de Fijación (descriptivo y fotográfico y/o video gráfico)

CORREOS ELECTRÓNICOS

Descripción General: Recaudar mensajes contenidos en cuentas de correo electrónico (gratuitas y/o corporativas) por parte del Equipo *ERISI* o quien haga sus veces en la FEDERACIÓN COLOMBIANA DE MUNICIPIOS, utilizando para ello, procedimientos forenses que permitan preservar características de Integridad, autenticidad, originalidad, entre otras, y con ello, lograr extraer estas cartas electrónicas en su formato original.

Desarrollo de la actividad: Cuando se traten de escenas virtuales, particularmente la intervención a cuenta (s) de correo electrónico corporativas y/o gratuitas, deberá mediar autorización del propietario del buzón, para lo cual se diligenciará formato de autorización – *Ver Formato de autorización para la revisión de información presente en medios de almacenamiento (discos duros, e-mails, entre otros)* -, y así,

extraer los mensajes relacionados con el incidente y/o evento de seguridad de la información de la FCM; Es importante resaltar que los e-mails que revistan importancia deberán ser exportados en su formato original preservando todas sus características, como son: 1 - Encabezado de direccionamiento *IP*, 2 - mensaje y 3 - archivos adjuntos en caso de existir. Este procedimiento deberá ser documentado llevando una línea de tiempo ordenada frente a las actividades que se desarrolle con ocasión del recaudo de estas cartas electrónicas.

Los mensajes (archivos) recolectados serán alojados en una imagen lógica y/o serán identificados mediante la extracción individual de su huella digital o *hash* - *Ver instructivo para la extracción de la huella HASH* -.

Una vez ejecutadas estas actividades de aseguramiento, la información será alojada en un medio de almacenamiento tecnológico (se recomienda que sea un medio óptico), aplicando los principios de cadena de custodia con el debido diligenciamiento de los formatos (rotulo y registro de continuidad). *Formato de rotulo de evidencia y Formato de registro de continuidad* -.

Con el propósito de poder extraer éstos mensajes electrónicos con su estructura completa (encabezado de direccionamiento *IP*, mensaje y adjuntos), se recomienda emplear gestores de correos electrónicos como por ejemplo el *Outlook*, *Thuderbird*, entre otros, que permitan a través de protocolos de comunicaciones *POP3* y/o *IMAP* exportar de un servidor remoto los mensajes alojados en éste, importándolos a buzón local para su posterior extracción forense. Una vez hecha esta importación es posible guardar esta información como archivos con extensión *PST* y/o guardarlos de manera individual como mensajes con extensiones *msg* y/o *eml*.

Como resultado del aseguramiento de la evidencia digital (e-mails), se tendrá que verificar que esto (s) posea (n) lo siguiente:

- Extracción de la imagen forense (Física y/o Lógica)
- Formato debidamente diligenciado de la extracción técnica de la imagen forense
- Formato de autorización para la revisión de información presente en medios de almacenamiento (discos duros, e-mails, entre otros)
- Identificación de la evidencia a través de la huella digital bajo metodologías *MD5* y/o *SHA1*, o las que para la fecha de las actividades pueda llegar a ser válida
- Cadena de Custodia con sus respectivos formatos
- Medios de Fijación (descriptivo y fotográfico y/o video gráfico)

SISTEMAS INFORMÁTICOS Y/O TELEMÁTICOS

Descripción General: Realizar análisis a sistemas informáticos y/o telemático con la finalidad de poder entender su funcionamiento, y extraer con ello, la evidencia que sea necesaria de acuerdo a los lineamientos establecidos por el equipo *ERISI* o quien haga sus veces en la FEDERACIÓN COLOMBIANA DE MUNICIPIOS, particularmente la identificación de las tablas de las bases de datos que hacen parte del o los sistema (s) de información, haciendo especial énfasis en *log* de seguridad, auditoria, eventos o trazas que permitan establecer las acciones que han hechos los usuarios frente al sistema y/o los cambios de información realizados sobre éstos.

Desarrollo de la actividad: Cuando así lo amerite el equipo *ERISI* o quien haga sus veces, deberá realizar una entrevista a los administradores de las diferentes plataformas tecnológicas que gestionen los diferentes sistemas de información y/o telemáticos de la organización, lo anterior, con la finalidad de entender el modelo entidad – relación de la (s) base (s) de datos, y comprender los diferentes

mecanismos de seguridad que se tienen implementados para poder generar control frente a los usuarios y a los cambios de la información consignada en el sistema.

Nota: Esta información deberá quedar registrada en un documento (Acta, informe ejecutivo, entre otros) como constancia del funcionamiento del sistema, así como de lo manifestado por parte de los administradores de TI, haciendo énfasis en los mecanismos de seguridad que poseen estos sistemas informáticos y/o telemáticos para cumplir con los principios orientados hacia la seguridad de la información, como lo son: la integridad, disponibilidad, confidencialidad y no repudio.

Una vez se tenga claridad frente al sistema(s) de información, el equipo *ERISI* o quien haga sus veces, deberá recaudar forensemente, según sea el caso, la base de datos en su totalidad o la información referentes a las tablas que se estime conveniente y/o los *log* de eventos (*log* de seguridad y/o auditoria) del o los sistemas (s) de información, de acuerdo a las necesidades de incidente y/o evento de seguridad. Es importante resaltar, que para el recaudo de estas evidencias se tendrá en cuenta las fechas de ocurrencia de los hechos basados en la cronología del incidente y/o evento de seguridad establecida por el Equipo de Respuestas a Incidencias de Seguridad de la Información.

Para la extracción de esta información, deberá tomarse una imagen forense física y/o lógica, según lo estime conveniente, extrayendo todos los datos que se requieran con ocasión al sistema de información intervenido - *Ver instructivo para la extracción de Imágenes Forenses -.*

Nota: En caso de tratarse de algún arreglo de discos duros, deberá extraerse la configuración de *hardware* y/o *software*, esto con la finalidad de reconstruir el arreglo. Para éste tipo de intervenciones se recomienda extraer el volumen

lógico del arreglo de disco, es decir, la extracción de la imagen lógica con el computador (servidor) encendido.

En caso de no extraerse la imagen física completa de los discos duros, en donde se halla la base de datos, y solamente se requiera extraer parte de la estructura y/o de los datos del modelo entidad – relación, se deberá exportar ésta a través del *script* en conjunto con la estructura de la misma, y/o realizar procedimientos para la exportación de la información hacia archivos planos. Para ambos casos deberá generarse una imagen forense lógica - *Ver instructivo para la extracción de Imágenes Forenses* - con el contenido de los archivos recaudados y en donde se encuentre la información requerida frente al incidente y/o evento de seguridad de la información, y/o la identificación de cada uno de archivos extraídos mediante la extracción de su huella digital o comúnmente conocido como *hash* - *Ver instructivo para la extracción de la huella HASH -.*

Como resultado del aseguramiento de la evidencia digital (Información de sistemas informáticos), se tendrá que verificar que esto (s) posea (n) lo siguiente:

- Extracción de la imagen forense (Física y/o Lógica)
- Formato debidamente diligenciado de la extracción técnica de la imagen forense
- Identificación de la evidencia a través de la huella digital bajo metodologías *MD5* y/o *SHA1*, o las que para la fecha de las actividades pueda llegar a ser válida
- Cadena de Custodia con sus respectivos formatos
- Medios de Fijación (descriptivo y fotográfico y/o video gráfico)

RECOLECCIÓN Y ANÁLISIS DE PÁGINAS WEB

Descripción General: Realizar estudio con el propósito de recaudar los contenidos de sitios web que hagan parte de un incidente y/o evento de seguridad de la

información en la FEDERACIÓN COLOMBIANA DE MUNICIPIOS, así mismo, determinar la ubicación geográfica del *hosting* y/o servidores en donde se encuentren alojadas dichas páginas.

Desarrollo de la actividad: Como desarrollo frente a la administración del incidente y/o evento de Seguridad de la Información, se ingresará a la red mundial de Internet digitando exactamente la dirección *URL (Uniform Resource Locator)* de la página que se esté analizando, de tal manera, que, si la misma existe, el equipo *ERISI* o quien haga sus veces, deberá documentar paso a paso la navegación que se haga sobre la misma, es decir, hará un escaneo sobre los links y/o hipervínculos registrados dentro de ésta.

Es importante resaltar que esta actividad debe ser registrada mediante la utilización de herramientas informáticas (Capturadores de Pantalla (*snap shot* o video), ejemplo: *Print Screen*, *Team Viewer*, *camtasia*, entre otros), y de ser posible, guardar esta página bajo el formato en que fue desarrollada (*html, htm, xml, ph*p, entre otras), alojando éstos hallazgos en un medio de almacenamiento propio de la FCM, y posteriormente, la extracción de imagen forense lógica - *Ver instructivo para la extracción de Imágenes Forenses* - y/o la identificación de los archivos obtenidos a través del cálculo de la huella digital o hash bajo las metodologías *MD5* o *SHA1* - *Ver instructivo para la extracción de la huella HASH -,* aplicando protocolos de cadena de custodia - *Formato de rotulo de evidencia y Formato de registro de continuidad.*

Nota: Cuando se esté documentando la existencia de la página web a través de capturadores de pantalla, deberá ingresarse al sitio web http://www.inm.gov.co/es/ con la finalidad de extraer el día y la hora en que se realiza el procedimiento.

En caso de no encontrar la página, se deberá recurrir a los motores de búsqueda existentes en *Internet*, tratando de ubicar el sitio web o algún indicio frente a la existencia del mismo, y/o buscar en páginas especializadas que almacenan información histórica de sitios electrónicos (*www.archive.org*). En caso de encontrar alguna información, ésta deberá documentarse a través de capturadores de Pantalla (*snap shot* o video), ejemplo: *Print Screen, Team Viewer, camtasia* entre otros), y de ser posible, guardar esta página bajo el formato en que fue desarrollada (*html, htm, xml, php*, entre otras), alojando éstos hallazgos en un medio de almacenamiento propio de la entidad, para que posteriormente se extraiga la imagen forense lógica - *Ver instructivo para la extracción de Imágenes Forenses* - y/o identificar los archivos extraídos a través de la huella digital o *hash* bajo las metodologías *MD5* o *SHA1* - *Ver instructivo para la extracción de la huella HASH* - , aplicando posteriormente protocolos propios de la cadena de custodia - *Formato de rotulo de evidencia y formato de registro de continuidad* -.

Una vez identificada y ubicada la página web, se deberá determinar la dirección *IP* del equipo en donde se encuentra alojada y así determinar el proveedor de *hosting* que facilita este servicio, lo anterior con el propósito de solicitar algún tipo de información adicional a esta empresa que permita apoyar el desarrollo de la investigación con ocasión del incidente y/o evento de Seguridad de la Información.

Como resultado del aseguramiento de la evidencia digital (página *web*), se tendrá que verificar que esto (s) posea(n) lo siguiente:

- Extracción de la imagen forense (Física y/o Lógica)
- Formato debidamente diligenciado de la extracción técnica de la imagen forense
- Identificación de la evidencia a través de la huella digital bajo metodologías *MD5* y/o *SHA1*, o las que para la fecha de las actividades pueda llegar a ser válida

- Cadena de Custodia con sus respectivos formatos
- Medios de Fijación (descriptivo y fotográfico y/o video gráfico)

DESARROLLO

Se explicará a través de la siguiente tabla, el paso a paso de la intervención al lugar de los hechos en donde existe evidencia digital (documentos electrónicos y/o mensajes de datos), los responsables frente a cada actividad y los documentos que deberían generarse con ocasión de cada acción, determinando aquellos ítems que tienen seguimiento y control, logrando una retroalimentación, así como memoria histórica frente al manejo del incidente y/o evento de seguridad.

Tabla 32. Proceso de Evidencia Digital.

No.	ACTIVIDAD	RESPONSABLE	REGISTRO
1 **©**	**1.** ***Recepción de Información***. Proceder según sea el caso: **1.1. Manejo al lugar de los hechos:** Se determina el o los lugares a intervenir, de acuerdo a lo definido por el Grupo *ERISI* de la Federación Colombiana de Municipios, o quien haga sus veces, en donde se encuentran los medios de almacenamiento de tipo tecnológico que deberán ser intervenidos, es decir, en donde se encuentra la evidencia digital que debe ser administrada por los expertos. **1.2. Recepción de los medios de almacenamiento:** Es	Grupo *ERISI* o quien haga sus veces	Reporte del incidente o evento de seguridad. Acta de diligencia y/o Informe y/o formato de entrega de medios de almacenamiento tecnológico.

	posible que las evidencias digitales puedan ser aportadas por entidades externas y/o departamentos de la Federación Colombiana de Municipios, por ende, las mismas serán analizadas directamente. **Ir al proceso 7**		
2 ©	***2. <u>Reunión de Trabajo.</u>*** **2.1. Definición de Actividades:** Se reunirán el Equipo de Respuesta a Incidentes de Seguridad de la Información (*ERISI*), o quien haga sus veces, con la finalidad de planear, diseñar y ejecutar las actividades necesarias para intervenir el lugar de los hechos, así como la preparación del kit de herramientas forenses para la recolección de la evidencia digital y la definición de roles de cada uno de los miembros del equipo que va a intervenir. En estas reuniones de trabajo se debe analizar la información suministrada por las diferentes fuentes (formales y no formales), antecedentes y documentación relacionada con el tema,	GRUPO *ERISI* o quien haga sus veces	Acta y/o informe de la reunión de trabajo

	esto con la finalidad de formular una hipótesis frente a los hechos conocidos y determinar que labores técnicas – Científicas y de investigación se deban realizar. De igual manera es necesario y pertinente establecer las restricciones legales que se puedan presentar con ocasión de afectación de derechos fundamentales, haciendo especial énfasis en limitaciones relacionas con la intimidad. Cuando la respuesta al incidente o evento de seguridad no requieran procedimientos especiales de informática Forense, se remitirá al **ítem 8** de éste procedimiento.		
3 ©	***3. <u>Intervención al lugar de los hechos.</u>*** ***3.1.* Búsqueda de medios de almacenamiento tecnológico**: Una vez se intervine el lugar de los hechos por parte de los integrantes del Grupo *ERISI* de la Federación Colombina de Municipios, o quien haga sus veces, éste	GRUPO *ERISI* o quien haga sus veces	Acta o informe de la administración del lugar de los hechos. Álbum fotográfico. Registro fílmico. Bosquejo y/o o plano planimétrico

	deberá realizar la búsqueda minuciosa de evidencia digital presenté *PC*, laptops, Cámaras Fotográficas, de Video, *DVR,* discos duros externos, *Flash Drives*, medios ópticos, agendas digitales, *tablet,* Celulares, *Smartphones, Sim Cards, micro SD,* entre otros*.* **3.2. Medios de Fijación:** Es importante resaltar que no importa la evidencia digital que se recaude (medios de almacenamiento de tipo tecnológico, correos electrónicos, log de seguridad o contenido de páginas *web*), todo el procedimiento de intervención al lugar de los hechos debe quedar documentado, haciendo especial énfasis en la recolección de la evidencia digital y su descripción; para ello existen los siguientes medios de fijación: **3.2.1. Descriptivo:** Es el diligenciamiento de formatos, informes, actas, entre otros, que permite hacer una descripción		

	exacta de las actividades realizadas en el lugar de los hechos y una explicación detallada del procedimiento ejecutado frente al recaudo y administración de la evidencia digital. **3.2.2. Fotográfico:** Es una representación gráfica de la intervención al lugar de los hechos, así como de la identificación de todas las evidencias recaudadas en el sitio, resaltando obviamente las digitales. **3.2.3. Video gráfico:** Es el registro fílmico de todos los procedimientos realizados en la escena, así como una descripción visual del lugar de los hechos y una identificación detallada de los elementos materiales probatorios recaudados; Este registro es uno de los		

	mejores medios de fijación teniendo en cuenta su continuidad, lo que asegura una intervención detallada y sin omisión de las acciones realizadas en el lugar de los hechos. **3.2.4. Planimétrico:** Es el levantamiento de un bosquejo en donde se describe el lugar de los hechos y la ubicación de cada una de las evidencias recaudadas, para ello se utilizan medidas las cuales deben ser fijadas a elementos que permanezcan perennes en el tiempo (Columnas, puertas, ventanas, entre otros). Este medio de fijación sirve para realizar reconstrucciones de escenas, si así se hiciera necesario.		

© → Punto de Control

4 ©	***4. <u>Recaudo de la evidencia digital.</u>*** Proceder según sea el caso, de acuerdo a la evidencia digital recaudada: **4.1. Medios de almacenamiento Tecnológico:** Cuando se llegue al lugar de los hechos se debe buscar todos los medios de almacenamiento tecnológico, para que los mismos sean recolectados de una manera técnica, aplicando todos los principios de la informática forense y de la cadena de custodia. Si se encuentran computadores encendidos, de ser viable y si así lo amerita el incidente de seguridad de la información (esto debe ser evaluado por el equipo *ERISI* o quien haga sus veces) se deben recolectar los datos volátiles, los metadatos y las huellas digitales de cada uno de los archivos contenidos en este medio de almacenamiento que está siendo interviniendo; es importante resaltar que esta información extraída	GRUPO *ERISI* o quien haga sus veces	Acta o informe de la administración del lugar de los hechos. Registro fílmico. Formato de Incautación

	(datos volátiles, metadatos y huella digital) debe ser exportada a un medio de almacenamiento externo (memoria *USB*, disco duro externo, disquete, entre otros), haciendo especial énfasis en que estos datos **NO PUEDE SER** almacenados en el equipo intervenido. Todo este procedimiento debe ser documentado a través de actas y/o formatos y/o informes, documentos que serán entregados al responsable del grupo *ERISI*, o quien haga sus veces, que hará el análisis a las evidencias, para que haga parte de la carpeta con ocasión de la administración del evento o incidentes de seguridad de la información. **4.2. Correos electrónicos:** El grupo *ERISI*, o quien haga sus veces, deberá administrar la escena en donde se encuentren las cartas electrónicas, que para este caso en particular se trata de una escena virtual (cuenta (s) de correo electrónico); para ello, ingresara al e-mail con la finalidad de extraer todos		

		los mensajes relacionados con los hechos del evento o incidente de seguridad de la información, así mismo, se configuraran los mensajes de tal manera que se puedan extraer los encabezados de direccionamiento IP (configuración de la cuenta de correo electrónico dependiendo del proveedor). Este procedimiento será documentado mediante herramientas informáticas que permitan capturar la información contenida en la pantalla, y se deben grabar los mensajes en su formato original que permitan extraer el contenido del mensaje, así como su encabezado. Estos archivos generados serán copiados en un medio de almacenamiento tecnológico (se recomienda un medio de almacenamiento óptico), a los cuales se les extraerá la imagen forense y/o la huella digital a través del hash**,** con el propósito de identificar cada uno de ellos de una manera única e inequívoca.		

	4.3. Log de eventos: Cuando se trate de hechos en donde se encuentren vinculadas plataformas tecnológicas y/o sistemas de información, y/o bases de datos de la Federación Colombiana de Municipios, el equipo *ERISI*, o quien haga sus veces, deberá recaudar los log de eventos (*log* de seguridad y/o auditoria y/o trazas) de éste (os) sistema (s), para lo cual tendrá en cuenta las fechas de ocurrencia del incidente y/o evento de seguridad de la Información. Adicionalmente deberá consignar en actas la explicación de los esquemas de seguridad que poseen estos sistemas informáticos y/o telemáticos para cumplir con los principios orientados hacia la información como lo son la integridad, disponibilidad, confidencialidad, seguridad y no repudio. A estos *log* de seguridad se les extraerá la imagen forense y/o la huella digital a través del *hash*.		

	4.4. Contenido de páginas *Web*: Se trata de evidencia digital presente en de sitios *web* cuyos contenidos deban ser intervenidos por tratarse de un evento o incidente de seguridad de la información. Para ello, se ingresará a la red mundial de Internet digitando exactamente la dirección *URL* (*Uniform Resource Locator*) del sitio web que deberá ser intervenido, de tal manera que, si esta se encuentra publicada, el equipo *ERISI*, o quien haga sus veces, documentará paso a paso la navegación que se haga sobre la misma, es decir, hará un escaneo sobre los *links* y/o hipervínculos registrados en ésta. Es importante resaltar que esta actividad debe ser registrada mediante la utilización de herramientas informáticas (Capturadores de Pantalla, ejemplo: *Print Screen*), y de ser posible guardar esta página bajo el formato en que fue hecha (*html, htm, xml*, entre otras), almacenando estos hallazgos en un medio de almacenamiento tecnológico (se sugiere un		

		medio óptico), para que este sea sometido a los protocolos de cadena de custodia como elemento material probatorio demostrando la existencia de este sitio *web*. En caso de no encontrar la página, se deberá recurrir a los motores de búsqueda que existen en Internet, para que a través de ellos se pueda ubicar el sitio *web*. Por otra parte, deberá determinar la dirección *IP* en donde se encuentra alojado dicho sitio *web*, para los cual podrá utilizar el intérprete de comandos (*MS-DOS*), utilizando la instrucción *ping* seguida de la dirección electrónica, ejemplo: ping www.lolitas.com; posteriormente se determinara el *ISP* o *Hosting* en donde se encuentra alojada esta página web, para ello podrá utilizar sitios web públicos que tenga relación con la organización *IANA* (*Internet Assigned Numbers Authority*), buscando a través de la palabra *Who is*? El resultado de esta intervención serán los		

	archivos extraídos con ocasión de la captura de la página, así como la documentación de la dirección IP y Proveedor o Hosting en donde se halla alojada, por ende y con el propósito de asegurar la evidencia es necesario extraer la imagen forense y/o la huella digital a través del hash.		
5 ©	***5. <u>Extracción de imágenes Forenses</u>:*** Procede según sea el caso. **5.1. Incautación del medio almacenamiento original:** Cuando el equipo *ERISI* de la FEDERACIÓN COLOMBIANA DE MUNICIPIOS, o quien haga sus veces, intervenga el lugar de los hechos, evaluara si se hace necesario la incautación del medio de almacenamiento original. **Ir ítem 6**	GRUPO *ERISI* o quien haga sus veces	Imagen Forense Física o Lógica. Reporte de Extracción de la Imagen forense

	5.2. Imagen Física Forense: Cuando se haga necesario extraer una imagen física (Copia *bit* a *bit* de TODO el medio de almacenamiento, es decir, del sector 0 hasta el último sector) del medio de almacenamiento tecnológico original, se utilizaran las herramientas forenses de hardware (Clonadores de disco) y/o software (*FTK, ENCASE, HELIX, RAPTOR*, entre otros) que tengan el aval por parte de la comunidad técnica–científica, esto con el propósito de hacer la devolución del medio original a su propietario y tomar como evidencia la imagen forense. **Nota:** Cuando existan incidentes o eventos de seguridad de la información en donde se encuentre involucrado equipos o medios de almacenamientos que sean estrictamente necesarios para la operación de la Federación Colombiana de Municipios y el cumplimiento de la misión de la entidad, se deberá extraer una imagen física.		

	5.3. Imagen Lógica: Cuando equipo *ERISI* determine que no es necesario extraer toda la información del equipo intervenido, sino solamente un fragmento (archivos, carpetas, volúmenes lógicos (*VBR*), *log* de seguridad, Bases de Datos), extraerá una imagen lógica, la cual será tomada como evidencia sin que se deba incautar o decomisar el medio de almacenamiento origen. Cuando se trata de la intervención de servidores que tengan configurados arreglos de discos de *hardware* o *software*, se recomienda extraer una imagen lógica frente a los volúmenes lógicos (*VBR*) que éste posea; esta actividad se recomienda que en lo posible se haga cuando el equipo se halla encendido, esto con la finalidad de no afectar su sistema de archivos.		
	6. <u>Cadena de Custodia</u> **6.1. Embalaje:** La evidencia digital es de origen electrónico, por ello, es necesario tener en cuenta	GRUPO *ERISI* o quien haga sus veces	Formato de Cadena de Custodia Rotulo de descripción de la evidencia digital

6 ©		las siguientes recomendaciones frente al contenedor en donde se vaya alojar este medio de almacenamiento de tipo tecnológico: El contenedor debe permitir aislar la energía estática producida por los seres humanos, lo anterior teniendo en cuenta el contacto permanente de ésta evidencia con los funcionarios que la recaudan, la transportan, custodian y analizan. El contenedor debe aislar la evidencia frente a campos magnéticos producidos por imanes, señales electromagnéticas de radios, celulares o cualquier otro medio de comunicación, lo anterior se basa, en que la exposición permanente a éstos campos puede alterar algunos de los bits de información contenidos en éstos dispositivos, lo cual iría en detrimentos de las características de Integridad, mismidad y autenticidad de la evidencia.		

	6.2. Cadena de Custodia: La cadena de custodia es un procedimiento documentado que permite hacer una descripción de la evidencia digital recaudada, el lugar en donde fue hallada, el tipo de embalaje utilizado y los funcionarios que han tenido algún tipo de intervención frente a éste elemento. Es necesario tener en cuenta dos (2) formatos, el rotulo y el registro de continuidad, los cuales deben ser diligenciados por el funcionario que haga parte del equipo *ERISI* de la Federación Colombiana de Municipios, o quien haga sus veces, una vez se haga el recaudo de la evidencia y ésta haya sido alojada en el contenedor respectivo que permita proteger la misma de acuerdo a lo comentado en apartes anteriores. **6.3. Transporte de la Evidencia:** Al momento de realizar el transporte de la evidencia digital es necesario tener los mínimos cuidados con la finalidad de que estos medios no vayan a sufrir		

	deterioros, por ende, se recomienda lo siguiente: Cuando se traslade la evidencia hay que tener cuidado de pasar éste elemento por puertas o dispositivos que hacen barridos electromagnéticos (utilizados para verificar contenidos de paquetes, o elementos metálicos en la indumentaria o humanidad de una persona), por ende, se debe advertir con una etiqueta que se trata de elementos susceptibles a daños por campos electromagnéticos. Al transportarla en un vehículo se debe tener especial cuidado de donde se ubica la evidencia, se recomienda que la misma pueda ir en un lugar dentro de éste que no permita la generación golpes, movimientos extremos o que algunos elementos pueda caer sobre esta, ya que podría generar daños físicos irreversibles, y con ello, la perdida de información y/o datos totales o parciales.		

	6.4. Almacenamiento: El bodegaje de la evidencia resulta ser muy importante, ya que, si la evidencia digital es alojada en un sitio que no posea las condiciones adecuadas, el contenedor (*hardware*) podría sufrir deterioros que redundaran en la perdida, daño, deterioro o modificación de la evidencia lógica. Por ello se recomienda tener en cuenta lo siguiente: • Alojar la evidencia digital en un lugar seco, con condiciones climáticas adecuadas para el almacenamiento de ésta. • Almacenar esta evidencia lejos de dispositivos que generen campos magnéticos, señales electromagnéticas, o energía estática. • Tener habitáculos adecuados para alojar los medios de almacenamiento tecnológico de manera individual, con su respectiva descripción para su posterior ubicación.		

7 ©	***7. <u>Entrega de la evidencia al Grupo ERISI, o quien haga sus veces.</u>*** **7.1. Imagen Física Forense:** Se extraerá la imagen física (Copia *bit* a *bit* de TODO el medio de almacenamiento, es decir, del sector 0 hasta el último sector) del o los medio (s) de almacenamiento tecnológico incautados, para ello, se utilizarán herramientas forenses de *hardware* (Clonadores de disco) y/o *software* (*FTK, ENCASE, HELIX, RAPTOR*, entre otros) que tengan el aval por parte de la comunidad técnica–científica. **Nota: De ser posible,** se extraerá en el laboratorio de Informática Forense una estampa (s) cronológica (s) a la imagen (es) a través del software desarrollado para tal fin. **7.2. Análisis de las Imágenes extraídas:** Una vez recaudadas la imagen (es)	GRUPO *ERISI* o quien haga sus veces	Imagen Forense Física o Lógica. Reporte de Extracción de la Imagen forense. Formato de Cadena de Custodia Rotulo de descripción de la evidencia digital Acta o informe de la administración del lugar de los hechos. Álbum fotográfico. Registro fílmico. Bosquejo y/o o plano planimétrico. Acta y/o Formato de Incautación. Acta de diligencia y/o Informe y/o formato de entrega de medios de almacenamiento tecnológico. Acta y/o formato de devolución de elementos.

	forense (s) (física (s) o lógica (s)), se determinará el tipo de análisis que se deberá realizar teniendo en cuenta la información del evento o incidente de seguridad, así como la selección de la (s) herramienta (s) forenses a utilizar. **7.3. Devolución de medio (s) de almacenamiento tecnológico original:** Una vez extraiga la imagen forense en el laboratorio, se determinará por parte del equipo de trabajo la devolución de este medio original a la persona propietario o responsable de éste.		
8 ©	***8. <u>Otras Actividades</u>*** En caso de no requerir expertos en administración de evidencia digital, se evaluará la situación y se enviará a la oficina o dependencia correspondiente.		

Diseño de procedimientos y metodologías para el combate del fraude electrónico que se pueda presentar en la organización.

Se detecta en la entidad que debe implementar el siguiente procedimiento con urgencia, debido a que ha sido victima de phishing.

A continuación se desarrolla el siguiente procedimiento:

Objetivo

Este procedimiento le indica las actividades que se deben realizar en el caso de presentarse un evento de phishing.

Descripción del Procedimiento

Indica los pasos necesarios que se deben realizar para llevar una adecuada respuesta a incidentes de phishing.

Alcance

Este procedimiento inicia con la actividad de analizar acciones y termina con la actividad seguimiento de cumplimiento. Está enfocado en la identificación de posibles fraudes en el Simit.

Requisitos y Políticas

Norma ISO 27001:2013, ISO27002, Ley Estatutaria 1581 DE 2012 de Datos Personales, Ley 1273 de 2009.

Definiciones

- **Spam**: Se denomina 'spam' a todo correo no deseado recibido por el destinatario, procedente de un envío automatizado y masivo por parte del emisor. El 'spam' generalmente se asocia al correo electrónico personal, pero no sólo afecta a los correos electrónicos personales, sino también a foros, blogs y grupos de noticias[19].

- **Phishing**: Es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc) de forma fraudulenta. El estafador o phisher suplanta la personalidad de una persona o empresa de confianza para que el receptor de una comunicación electrónica aparentemente oficial (vía e-mail, fax, sms o telefónicamente) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el estafador[20].

- **Malware**: Palabra que nace de la unión de los términos software malintencionado "malicious software". Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, backdoors, spyware, etc. La nota común a todos estos programas es su carácter dañino o lesivo[21].

  - Virus: Programa diseñado para copiarse y propagarse a sí mismo, normalmente adjuntándose en aplicaciones. Cuando se ejecuta una aplicación infectada, puede infectar otros archivos. Se necesita acción humana para que un virus se propague entre máquinas y sistemas. Esto puede hacerse descargando archivos, intercambiando disquetes y discos USB, copiando archivos a y desde servidores de archivos o enviando adjuntos de e-mail infectados. Los efectos que pueden provocar varían dependiendo de cada tipo de virus: mostrar un mensaje, sobrescribir archivos, borrar archivos, enviar información confidencial mediante correos electrónicos a terceros, etc. Los más comunes son los que infectan a ficheros ejecutables[22].

---

[19] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

[20] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

[21] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

[22] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

- Troyanos; Este tipo de 'malware' carente de la capacidad de autoduplicación requiere del uso de la ingeniería social para obtener un correcto funcionamiento. Ya sea por la confianza en quien entrega el programa a la víctima o por su falta de cautela, la víctima instala un 'software' aparentemente inocuo en su ordenador. Al ejecutarse el software no se evidencian señales de un mal funcionamiento; sin embargo, mientras el usuario realiza tareas habituales en su ordenador, el programa abre diversos puertos de comunicaciones del equipo de la víctima que permiten el control absoluto de forma remota[23].

- **Dirección IP**: En inglés, IP Address. Número que identifica una interfaz de un dispositivo conectado a una red que utilice protocolo IP[24].

[23] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

[24] Glosario ISO 27001. [En linea]. Disponible en:< http://www.iso27000.es/glosario.html>

Desarrollo

Analizar Acciones

Se debe realizar el análisis detallado e implementar acciones inmediatas del phishing presentado.

Coordinar Contención

Se requieren ejecutar actividades de contención que permitan restablecer los servicios que se puedan estar viendo impactados por el incidente de phishing. Se deben cambiar las contraseñas de los sistemas de información que utiliza el usuario.

Apoyar contención Incidente

Conjuntamente con el Líder de Seguridad o quien cumpla este rol, tomar acciones para contener el incidente y minimizar el impacto.

Notificar a organismos

Todos los incidentes de phishing presentados independientes de si ha causado daños, robo de dinero o de algún tipo de información sensible, o no alcanzó a lograr el objetivo, se deben reportar a organizaciones encargadas de trabajar en este tipo de incidentes (*ver anexo 9.1*).

Analizar Planes

Realiza el análisis detallado del incidente ocurrido y formular los planes de acción a implementar con el fin de que incidentes como el ocurrido no se vuelva a presentar

Solicitar Creación

Solicita a la mesa de servicio la creación de casos a los Grupos de gestión para que ejecuten los planes de acción definidos

Crear casos adicionales

La Mesa crea los diferentes casos de phishing para los grupos que deben gestionar los planes de acción definidos

Ejecución planes de acción

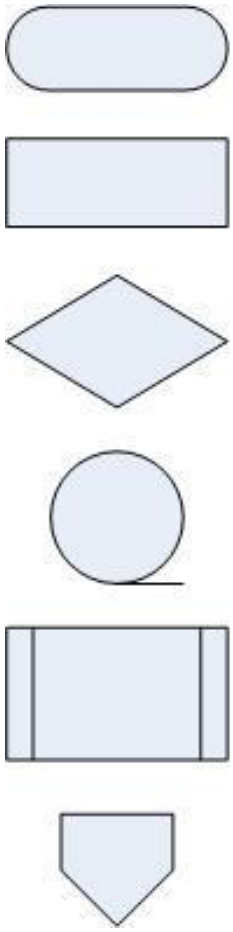
Realiza la ejecución de los planes de acción definidos de acuerdo al tipo de phishing presentado.

Seguimiento Cumplimiento

Monitorear el debido cumplimiento de los planes de acción establecidos.

Diagrama de Flujo

Figura 42. Simbología de Diagrama de Flujo



Inicio o fin de un procedimineto

Indica la actividad que se debe realizar en el procedimiento.

Actividad de Control que se realiza al procedimiento para **verificar** que se esté cumpliendo según los lineamientos, es aquí donde se toman **decisiones;** haciendo efectivas las acciones necesarias al **manejo de riesgos** y orientando la operación hacia la consecución de sus resultados, metas y objetivos.

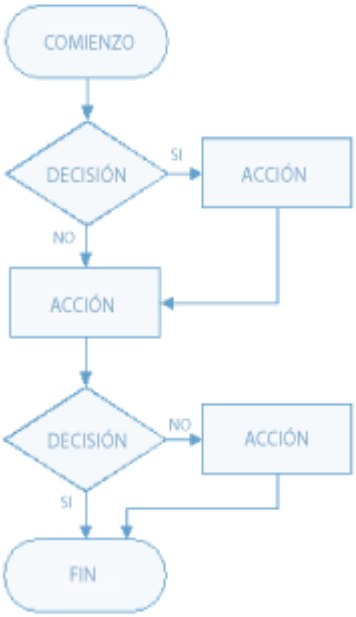
Conector que lleva a una cierta actividad del mismo procedimiento.

Actividad que al finalizar continúa con otro procedimiento.

Conector de Página, sirve para vincular el flujograma cuando se termina una página.

Fuente: Autor.

Tabla 33. Diagrama de flujo del procedimiento

DIAGRAMA	ACTIVIDAD	RESPONSABLE (S)	OBSERVACIONES
	Analizar Acciones	Oficina de TIC	
	Coordinar Contención	Oficina de TIC	
	Apoyar contención Incidente	Oficina de TIC	
	Notificar a organismos	Oficina de TIC	
	Analizar Planes	Oficina de TIC	
	Solicitar Creación	Oficina de TIC	
	Crear casos adicionales	Oficina de TIC	
	Ejecución planes de acción	Oficina de TIC	
	Seguimiento Cumplimiento	Oficina de TIC	

Fuente: Autor.

Anexos

Reporte ante entes Judiciales

Se recomienda seguir las actividades establecidas por los entes de control externos:

Centro Cibernético Policial de la Dirección de Investigación Criminal:

- http://www.ccp.gov.co/caivirtual.php
- http://www.ccp.gov.co/ciberseguridad.php
- http://www.ccp.gov.co/archivos.php?id=3
- http://www.ccp.gov.co/articulo-imagen.php?id=33
- https://m.facebook.com/story.php?story_fbid=599859323359023&id=126142030730757

Fiscalía General de la Nación:

- http://www.fiscalia.gov.co/colombia/servicios-de-informacion-al-ciudadano/centros-de-atencion-ciudadana/

NAP Colombia (administrado por la Cámara Colombiana de Informática y Telecomunicaciones-CCIT):

- http://nap.co/
- http://www.ccit.org.co/index.php/sobre-la-ccit/nap-colombia

Así mismo, se recomienda al momento de denunciar ante la Policía Judicial los casos de PHISHING, o correos donde se evidencie solicitud de captura de información personal o laboral, que pueda llevarlo a ser víctima de un delito.

Recomendaciones para prevenir el phishing

- APRENDE A IDENTIFICAR CLARAMENTE LOS CORREOS ELECTRÓNICOS SOSPECHOSOS DE SER 'PHISHING'

  Existen algunos aspectos que inequívocamente, identifican este tipo de ataques a través de correo electrónico:

  - Utilizan nombres y adoptan la imagen de empresas reales
  - Llevan como remitente el nombre de la empresa o el de un empleado real de la empresa
  - Incluyen webs que visualmente son iguales a las de empresas reales
  - Como gancho utilizan regalos o la perdida de la propia cuenta existente

- VERIFIQUE LA FUENTE DE INFORMACIÓN DE LOS CORREOS ENTRANTES

  Su entidad financiera nunca le pedirá que le envíe sus claves o datos personales por correo. Nunca responda a este tipo de preguntas y si tiene una mínima duda, llame directamente a su entidad financiera para aclararlo.

- NUNCA ENTRE EN LA WEB DE SU ENTIDAD FINANCIERA PULSANDO EN LINKS INCLUIDOS EN CORREOS ELECTRÓNICOS

  No haga clic en los hipervínculos o enlaces que le adjunten en el correo, ya que de forma oculta lo podrían dirigir a una web fraudulenta.

  Teclee directamente la dirección web en su navegador o utilice marcadores/favoritos si quiere ir más rápido.

- REFUERCE LA SEGURIDAD DE SU ORDENADOR

  El sentido común y la prudencia es tan indispensable como mantener su equipo protegido con un buen antivirus que bloquee este tipo de ataques. Además, siempre debe tener actualizado su sistema operativo y navegadores web.

- INTRODUZCA SUS DATOS CONFIDENCIALES ÚNICAMENTE EN WEBS SEGURAS

  Las webs ‘seguras’ empiezan por ‘https://’ y debe aparecer en tu navegador el icono de un pequeño candado cerrado.

- REVISE PERIÓDICAMENTE SUS CUENTAS

  Nunca está de más revisar sus cuentas bancarias de forma periódica, para estar al tanto de cualquier irregularidad en sus transacciones online.

- NO SÓLO DE BANCA ONLINE VIVE EL PHISHING

  La mayor parte de ataques de phishing van contra entidades bancarias, pero en realidad pueden utilizar cualquier otra web popular del momento como gancho para robar datos personales: ebay, facebook, Pay Pal, etc.

- EL PHISHING SABE IDIOMAS

  El phishing no conoce fronteras y pueden llegarte ataques en cualquier idioma. Por norma general están mal escritos o traducidos, así que este puede ser otro indicador de que algo no va bien.

Si nunca entra a la web en inglés de su banco, ¿Por qué ahora debe llegarte un comunicado suyo en este idioma?

- ANTE LA MÍNIMA DUDA SEA PRUDENTE Y NO SE ARRIESGUE

  La mejor forma de acertar siempre es rechazar de forma sistemática cualquier correo electrónico o comunicado que incida en que facilite datos confidenciales.

  Elimine este tipo de correos y llame a su entidad financiera para aclarar cualquier duda.

- INFÓRMESE PERIÓDICAMENTE SOBRE LA EVOLUCIÓN DEL MALWARE
  Hay que mantenerse al día de los últimos ataques de malware, recomendaciones o consejos para evitar cualquier peligro en la red.

- NO ENTREGAR CONTRASEÑAS
  No responder a correos en los que se pida su contraseña.

- DIFERENCIAR INFORMACIÓN CONFIDENCIAL
  No enviar información sensible o confidencial a través del correo electrónico, sino es estrictamente necesario.

- USO ADECUADO DEL CORREO
  No utilizar el correo electrónico para el envío o recepción de datos personales.

  - RESPONSABILIDADES SOBRE EL USO DE CUENTAS

  No utilizar el correo electrónico de la empresa para darse de alta en sitios web o servicios que no estén relacionados con la actividad laboral.

  - CORROBORAR REMITENTES

  No abrir archivos adjuntos ni enlaces sin comprobar el remitente y el contenido del correo electrónico.

  - CONTRASEÑAS ROBUSTAS

Usar contraseñas robustas y cambiarlas de forma regular, por lo menos cada tres meses.

  - AUTORIZACIÓN DE APLICACIONES

Nota: No instalar programas o aplicaciones que no estén relacionados con la actividad laboral.

10.3 Socialización de cada uno de los documentos y metodologías con las personas que designe el supervisor del proyecto o la alta Direccion de la FCM.

Para este punto, se realiza la socialización de entregables del proyecto, se sustenta los criterios de evaluación definidos para el desarrollo del proyecto, mediante el cual se soporta en un acta de entrega de aceptación de los entregables desarrollados en el proyecto y se aceptan por los miembros directivos de la Federacion Colombiana de Municipios.

El acta y los entregables del proyectos presentados y socializados reposa con sus anexos en el archivo del sistema de gestión documental de la entidad por temas de seguridad y confidencialidad de la información.

11. CONCLUSIONES

- ✓ Se concluye que el desarrollo del proyecto hubo lugar a la previa planificacion para la ejecución del proyecto, también definir y validar el alcance del proyecto de manera delimitada, teniendo en cuenta el tiempo y el costo en base del cronograma y sus planes de gestión para la dirección y gestión del proyecto que por directriz que demanda la entidad - Federacion Colombiana de Municipios.

- ✓ La Federación Colombiana de Municipios cuenta con un SGSI y está preparada para dar cumplimiento a los requisitos de GEL en el mediano plazo.

- ✓ De acuerdo a los plazos definidos por GEL para el 2015 la meta de avance en seguridad y privacidad de la información es de completar un 40%, para el año 2016 la meta es del 60%.

- ✓ Para el año 2017 la meta es del 80% Debido a que la FCM cuenta con un SGSI, y la articulación de sus componentes, estos valores son una meta alcanzable siempre y cuando el ejercicio sea continuo, el comité de seguridad de la información defina su agenda para 2018 y se realicen las mejoras dentro del alcance del sistema.

- ✓ El tema de la seguridad de la información no es una responsabilidad del Departamento de Sistemas o Tecnología, su principal protagonista y gestores la Alta Dirección.

- ✓ Este es un inicio, el tema de la seguridad en la información es una actividad que no debe ser interrumpida.

- ✓ Tenemos una cuota de responsabilidad de ir cerrando la actual brecha de cultural en seguridad de la información, con el propósito de dejar en el futuro, entidades que ayuden un mejor estilo de vida de las próximas generaciones.

BIBLIOGRAFIAS

- Activos de Información (Formatos y procedimientos) de la Federación Colombiana Municipios para la construcción de estudios previos y formulación y formalización de proyectos.

- Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. (2013). Seguridad informática. Madrid, ES: Macmillan Iberia, S.A.. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10820963&p00=seguridad+inform%C3%A1tica

- Roa, B. J. F. (2013). Seguridad informática. Madrid, ES: McGraw-Hill España. Recuperado de: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10692460&p00=seguridad+inform%C3%A1tica

- Elvira, M. (2012). Introducción a la seguridad informática. Recuperado de http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la- seguridad-informatica

- Sánchez, R. H. A. (2009). ¿Cómo iniciar los proyectos de sistemas de información?. Córdoba, AR: El Cid Editor | apuntes. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10312298&p00=c%C3%B3mo+iniciar+proyectos+sistemas+informaci%C3%B3n

- Torres, H. Z., & Torres, M. H. (2014). Administración de proyectos. México, D.F., MX: Larousse - Grupo Editorial Patria. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=11013678&p00=administraci%C3%B3n+proyectos

- Gutiérrez, D. M. J. A., & Pagés, A. C. (2008). Planificación y gestión de proyectos informáticos. Alcalá de Henares, ES: Servicio de Publicaciones. Universidad de Alcalá. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10280334&p00=planificaci%C3%B3n+gesti%C3%B3n+proyectos+inform%C3%A1ticos

- Ferreyro, A., & Longhi, A. D. (2014). Metodología de la investigación. Córdoba, Argentina: Encuentro Grupo Editor. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?user=proveedor&pass=danue0a0&url=http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=e000xww&AN=847674&lang=es&site=eds-live

- Lerma González, H. D. (2009). Metodología de la investigación : propuesta, anteproyecto y proyecto. Bogotá, D.C.: Ecoe ediciones. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?user=proveedor&pass=danue0a0&url=http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=nlebk&AN=483354&lang=es&site=eds-live

- Ruiz Olabuénaga, J. I. (2012). Metodología de la investigación cualitativa. Bilbao: Universidad de Deusto. Recuperado de http://bibliotecavirtual.unad.edu.co:2048/login?user=proveedor&pass=danue0a0&url=http://bibliotecavirtual.unad.edu.co:2051/login.aspx?direct=true&db=edsebk&AN=869656&lang=es&site=eds-live

- PMI, Libro PMI Versión 5ta Edición (Descarga gratuita para Miembros PMI)

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G6_Gestion_Documental.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G9_Indicadores_Gestion_Seguridad.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G10_Continuidad_Negocio.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G15_Auditoria.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G16_evaluaciondesempeno.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G17_Mejora_continua.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G18_Lineamientos_terminales.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones, http://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones,
- http://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

- MSPI - Ministerio de las Tecnologías de la Información y las Comunicaciones,, http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

ANEXOS

ANEXO A. RESUMEN ANALITICO ESPECIALIZADO - R.A.E.

TEMA	Modelo de Seguridad y Privacidad de la Información en el marco de la Estrategia de Gobierno en Linea / Gobierno Digital.
TITULO	Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) con base al Modelo de Seguridad y Privacidad de la Información según lineamentos del Ministerio de las Tecnologías de la Información y las Comunicaciones en el marco de la estrategia GEL (Gobierno en Línea) / Gobierno Digital.
AUTORES	Ing. Ronald Mauricio Cely Espitia.
FUENTES BIBLIOGRAFICAS	Fuentes bibliográficas entre marcos de referencia, artículos, estándares y mejores practicas de seguridad y ciberseguridad, guias, lineamientos, ámbitos, artefactos, instrumentos, portales y consultas a páginas de gobierno como el Ministerio de Tecnologias de la Informacion y las Comunicaciones.
AÑO	2018
RESUMEN	El presente documento representa el resumen analítico especializado del proyecto de grado en su versión final, con el fin de ser la base de sustentación para lograr un objetivo empresarial en la organización para la cual se diseño la implementación de un sistema de gestión de seguridad de la información según norma ISO 27001 versión 2013, esto teniendo en cuenta los lineamientos del modelo de seguridad y privacidad de la información que dispuso el Ministerio de las Tecnologías de la Información y las Comunicaciones de Colombia en el marco de la estrategia de Gobierno en línea y conforme a lo señalado en el decreto 1078 de 2015 y al decreto 2573 de 2014.
PALABRAS CLAVES	Sgsi, ethical hacking,controles, dominios,modelo de seguridad, privacidad de la información, csirt, forense, plan de seguridad, diseño, implementación,sensibilización, estrategia, gobierno, seguridad, información.
CONTENIDOS	La Federacion Colombiana de Municipios - Direccion Nacional Simit, administra un sistema de información el cual hace uso de internet, en el desarrollo de sus actividades cotidianas, lo que lo hace vulnerable a ataques infromaticos (secuestro o robo información , etc), para salvaguardar su integridad cuenta con estandares de seguridad pero a pesar de esto, los ataques informaticos evolucionan constantemente, por lo que en algún momento se podría llegar a comprometer la continuidad y operación del core del negocio. Por lo que se hace necesario generar un procolo de mejora continua y buscar minimizar los potenciales ataques que pueda llegar a sufrir los sistemas e infraestructura tecnológica de la entidad, todo esto con base al MSPI (Modelo de Seguridad y Privacidad de la Informacion) que dispuso el Ministerio de las

	Tecnologias de la Informacion y las Comunicaciones en el marco de la estrategia GEL y en cumplimiento de lo señalado en el articulo 5 del decreto 2573 del 2014. Estadísticamente Latinoamérica sufre en promedio 12 ataques informáticos por segundo, lo que hace una cifra a tener en cuenta a la hora de salvaguardar la información de la entidad, por tal motivo nace la necesidad de un estudio de las potenciales amenazas y del diseño del sistema de gestión de seguridad la información con base al MSPI (Modelo de Seguridad y Privacidad de la Informaición) para la entidad. Atendiendo a que las actividades propias de seguridad de la información demandan conocimientos especializados en donde predomina el factor intelectual, el cual se requiere contar con el Ing. Ronald Mauricio Cely Espitia, quien, a través de su proyecto de grado, conocimiento y experiencia en implementación de soluciones de tecnología con proyectos de consultoría, auditoria en la norma iso 27001, capacitación e Interventoría de Proyectos están enfocados en la Seguridad de la Información. El Ing. Ronald Mauricio Cely Espitia, como responsable en seguridad de la información para la Federación Colombiana de Municipios busca mantener vigentes los requerimientos de la entidad en los procesos que serán analizados para posteriormente complementar, ajustar e implementar la seguridad lógica con las mejores prácticas, para administrar y mitigar razonablemente los riesgos informáticos relacionados con pérdida de confidencialidad, integridad y disponibilidad. Por estas razones, dada la necesidad de acceder a la información cualificada en el marco de las funciones encomendadas por expreso mandato legal; se hace necesario gestionar a través de los servicios profesionales contratados del Ing. Ronald Mauricio Cely Espitia, un acompañamiento en el logro de objetivos en materia de confidencialidad, integridad y disponibilidad de los sistemas y activos de información con los que cuenta la Federación Colombiana de Municipios – Dirección Nacional Simit.
DESCRIPCION DEL PROBLEMA	La Federación Colombiana de Municipios es una persona jurídica de carácter privado, sin ánimo de lucro, creada mediante el concurso y consenso de los entes territoriales en ejercicio del derecho constitucional de asociación. A ella pertenecen por derecho propio todos los municipios, distritos y asociaciones de municipios del país y tiene como finalidad la defensa de sus intereses. En este sentido, la Federación Colombiana de Municipios se rige por el derecho privado, salvo en lo que concierne a la función pública asignada según los artículos 10 y 11 de la Ley 769 de 2002, cuyo fundamento constitucional se esgrime en el artículo 209 de la Constitución Política.

	Luego, si bien es cierto que la Federación Colombiana de Municipios se rige por las normas del derecho privado, en lo concerniente a la función pública delegada por disposición legal, se encuentra sometida a las normas propias del derecho público, siendo aplicable entonces para el presente proceso de contratación, los procedimientos contemplados en la Ley 80 de 1993, modificada por la Ley 1150 de 2007, Ley 1474 de 2011 y el Decreto Reglamentario 1082 de 2015. La Federación Colombiana de Municipios por expreso mandato legal, ha requerido desde sus inicios, contar con una infraestructura tecnológica suficiente que garantice un adecuado y permanente funcionamiento, y que sea susceptible de perfeccionamiento a través de la implementación de nuevas tecnologías aplicadas siempre al logro del fin perseguido, con métodos de control, seguridad, privacidad y calidad de la información.
OBJETIVOS	➢ Diseñar en la Federación Colombiana de Municipios - Dirección Nacional Simit, el Sistema de Gestión de Seguridad de la Información (SGSI) en base del Modelo de Seguridad y Privacidad de la Información según lineamentos del Ministerio de las Tecnologías de la Información y las Comunicaciones en el marco de la estrategia GEL (Gobierno en Línea) y en cumplimiento del decreto 2573 de 2014, articulo 5. ➢ Identificar el marco metodológico para adoptar el Modelo de Seguridad y Privacidad de la Información en la FCM-DNS en cumplimiento del artículo 5 del decreto 2573 de 2014. ➢ Identificar la planeación adecuada para capacitar, concientizar y sensibilizar la seguridad de la información en la FCM. ➢ Determinar el Análisis Forense Digital para la FCM. ➢ Precisar el asesoramiento en Ethical Hacking. ➢ Diseñar y asesorar la atención de Incidentes y fraudes ➢ Identificar las amenazas y vulnerabilidades de los activos de información de la entidad.
METODOLOGIA	La metodología investigativa del proyecto de Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) con base al Modelo de Seguridad y Privacidad de la Información según lineamentos del Ministerio de las Tecnologías de la Información y las Comunicaciones en el marco de la estrategia GEL (Gobierno en Línea), permitirá que el diseño metodológico logre describir la estrategia de seguridad de la información que requiere la institución, y generar una trasferencia social de conocimiento que contribuye de manera innovadora a la solución de problemas de seguridad de la información; por lo tanto, podemos definir que el tipo de proyecto es **aplicado y el tipo de investigación es de tipo descriptivo.**

PRINCIPALES REFERENTES TEORICOS	Como referente teorico se aborda todo el modelo y marco de trabajo que realizo el Ministerio de Tecnologias de Informacion y las Comunicaciones en el marco de la Estrategia de Gobierno en Linea / Gobierno Digital, con el fin de diseñar el modelo de seguridad y privacidad de la información(MSPI) para la Federacion Colombiana de Municipios.
PRINCIPALES REFERENTES CONCEPTUALES	A nivel conceptual se toma como referentes los actores que apoyaron al desarrollo de este proyecto como son los ingenieros especialistas en redes, administración de infraestructura, bases de dataos, service desk y los asesores de seguridad de la información de Mintic.
RESULTADOS	Se materializo los entregables del proyecto según los objetivos específicos para el diseño del sistema de gestión de seguridad la información con base al modelo de seguridad y privacidad de la información que dispuso Mintic.
CONCLUSIONES	Se concluye que la Federación Colombiana de Municipios cuenta con un SGSI y está preparada para dar cumplimiento a los requisitos de GEL en el mediano plazo. De acuerdo a los plazos definidos por GEL para el 2015 la meta de avance en seguridad y privacidad de la información es de completar un 40%, para el año 2016 la meta es del 60%. Para el año 2017 la meta es del 80% Debido a que la FCM cuenta con un SGSI, y la articulación de sus componentes, estos valores son una meta alcanzable siempre y cuando el ejercicio sea continuo, el comité de seguridad de la información defina su agenda para 2018 y se realicen las mejoras dentro del alcance del sistema.

ANEXO B: DIVULGACION DEL PROYECTO.

Compromisos de los Directivos de la FCM:

- ✓ La información es con siderada como el activo numero # 1 de todo tipo de Entidad.
- ✓ Es responsabilidad de todo tipo de Entidad contar con Información **Confiable**, **Integra** y **Disponible** para el desarrollo de su objeto y demás.
- ✓ La implementación de controles,normas y procedimientos en seguridad de la información, genera un mayor nivel de **Credibilidad** y **Liderazgo** de la Entidad, ante sus clientes y sus asociados.

Divulgación y Sensibilizacion del Proyecto, mediante las Politicas de Seguridad y Privacidad de la Información Implementadas a traves de videos pedagogicos:

- ✓ https://www.youtube.com/watch?v=Z2vrw1uWiUI
- ✓ https://www.youtube.com/watch?v=wpelt61Akjw
- ✓ https://www.youtube.com/watch?v=5XUqlNzze4g
- ✓ https://www.youtube.com/watch?v=M55JKGj_D8M
- ✓ https://www.youtube.com/watch?v=2YnUOEJ-ybE

Divulgacion de Operación Ciberdefensa contra CiberAtaques recibidos en la FCM. " Virus RansonWare WannCry 2.0" el dia 12 de Mayo de 2017.

- ✓ https://youtu.be/enofHnMfllA

ANEXO C. SOCIALIZACION DEL INFORME EJECUTIVO Y TECNICO DE ETHICAL HACKING.

Federación Colombiana de Municipios

FEDERACIÓN COLOMBIANA DE MUNICIPIOS
NIT. 800.082.665 - 0
Dirección de Tecnologías de Información y las Comunicaciones
Registro de Asistencia

Tema Principal: Proyecto del SGSI, según lineamientos de GEL; en cumplimiento del Decreto 1078 de 2015.

Temas Especificos: Informe Ejecutivo y Tecnico de Ethical Hacking

Asistentes

No.	Identificación	Nombres y Apellidos	Cargo	Entidad	Firma
1	52498194	Oscelle Ingrid Barbosa Abril	Prof. Esp TIC	DTIC	
2	79985431	Edgar Mauricio Rangel	Jefe Oficina	DTIC	
3	1049612524	Adrian Mauricio Barrera	Prof. B.D	DTIC	
4	80087263	Ronald Cely Gaitán	CISO	DTIC	
5	1077341810	Edwin Fonseca	Pto. Soporte	DTIC	
6	80007946	Germán Alberto Duque B	Pto IRC	DTIC	
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
Fecha: 29/09/2017		Conferencista: CISO - Director del Proyecto (Ing. Ronald Cely).		Lugar: Piso 19 - Sala 1 de 4:00 PM - 5:00PM	

Elaboró: Ing. Ronald Cely- CISO
Revisó: Ing. Ronald Cely- CISO
Aprobó: Ing. Alejandro Murillo Pedroza - Director de Tecnologías de Información y las Comunicaciones