IDENTIFICACIÓN DEL ESTADO DE MADUREZ Y DISEÑO DE CONTROLES PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO TIC DE ESTRATEGIAS EMPRESARIALES DE COLOMBIA S.A.S

ING. LILIANA ANDREA TORRES PÉREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI
2017

IDENTIFICACIÓN DEL ESTADO DE MADUREZ Y DISEÑO DE CONTROLES PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO TIC DE ESTRATEGIAS EMPRESARIALES DE COLOMBIA S.A.S

ING. LILIANA ANDREA TORRES PÉREZ

Trabajo de Grado como requisito para optar al título de:
Especialista en Seguridad Informática

ING. GABRIEL MAURICIO RAMÍREZ VILLEGAS
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CALI
2017

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Santiago de Cali, 22 de febrero de 2018

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

1. INTRODUCCIÓN

En la actualidad la información es catalogada como uno de los activos más importantes de la empresa, puesto que ella contiene datos privilegiados de clientes, empleados, proveedores, productos/servicios, cifras, estrategias, ingresos, activos, gastos e información del Core de negocio, la pérdida o divulgación de esta puede causar sanciones, multas o incluso el cierre de la empresa, lo cual puede ser aprovechado por la competencia; por estas y otras razones las empresas deben implementar un sistema de gestión de seguridad de la información, para minimizar la pérdida de información privilegiada.

Para que los sistemas de gestión implementados en las empresas sean exitosos y se mantengan, se debe contar con apoyo de la gerencia, establecer políticas, procedimientos, formatos, capacitación, realizar auditorías, seguimientos y mejorarlo continuamente. El sistema de gestión de seguridad de la información debe estar basado en el modelo PHVA (Planear, Hacer, Verificar y Actuar) de la norma ISO 27001.

Contar con un sistema de seguridad de la información, representa para las empresas, cumplir con una serie de requisitos y controles mínimos que les permitan prepararse preventiva, reactiva y en especial a sus sistemas tecnológicos, para proteger la información buscando mantener su confidencialidad, disponibilidad e integridad. Por ello resulta fundamental implementar medidas de control como políticas, directrices y procedimientos que direccionen y permitan su implementación en todos los niveles de la organización.

La norma ISO 27001:2013 es una metodología que indica que el sistema de gestión de seguridad de la información se diseña y mantiene para asegurar controles de seguridad suficientes protegiendo los activos de información y generando confianza a las partes interesadas sobre el manejo de activos y seguridad de la información.

Estrategias Empresariales de Colombia S.A.S., es una empresa ubicada en la ciudad de Cali que presta servicios de asesoría y consultoría y cuenta con un proceso de TIC, el cual está catalogado como de apoyo en su mapa de procesos. Este cubre la empresa de extremo a extremo, administra el sistema Core y asesora los clientes en la implementación de las mejores prácticas.

El presente proyecto busca evaluar el sistema de gestión de seguridad de la información para el proceso TIC, de manera que se tenga claridad acerca de la protección y mantenimiento que se tiene y de debería tener sobre los activos de información, y se cree una cultura entre los empleados promoviendo la continuidad de las operaciones.

2. JUSTIFICACIÓN

En la actualidad la información es el activo más valioso para la empresa, su almacenamiento, transmisión, gestión y seguridad está a cargo del proceso TIC, en el cual, se deben implementar controles y/o sistema de gestión de seguridad de la información (SGSI), para administrar los recursos tecnológicos de forma adecuada. Metodologías de implementación de controles, como la recomendada por la NTC ISO 27001:2013, resalta que la seguridad de la información es indispensable en las empresas, y se debería aplicar sin importar su tamaño.

Estrategias Empresariales de Colombia S.A.S., presta servicios de asesorías a los procesos administrativos, financiero, tesorería, jurídico, auditoría, comercial, tecnología y comunicaciones a empresas en toda Colombia. En el desarrollo de estas actividades, la empresa actúa como encargado y responsable de información o datos personales de sus clientes, empleados y proveedores, asumiendo un alto grado de responsabilidad frente a la correcta gestión que debe realizar de la misma y al cumplimiento de las normas que regulan su actividad.

Lo anterior, hace que sea necesario, establecer medidas de protección, controles, validaciones, procedimientos, políticas, manuales y estrategias que permitan gestionar de manera eficiente y eficaz la información que se encuentra al interior de la empresa.

El proceso TIC, en Estrategias Empresariales de Colombia S.A.S. no cuenta con una metodología que cumpla lo anteriormente expuesto para el control de las actividades que se ejecutan al interior del proceso y que afectan la operación de la empresa, desatendiendo lo establecido por las metodologías especializadas de implementación, de manera que logre integrar sus actividades en un sistema de gestión de seguridad de la información completo y dinámico que se pueda replicar a sus empresas cliente.

Entre las actividades más críticas identificadas en el proceso TIC se encuentran falta de procedimientos, políticas, control de activos, accesos seguros, manuales de funciones e instructivos, los usuarios tienen rol de administrador en los equipos de cómputo y ERP, los cambios a programas son realizados en ambientes productivos y no en ambiente de pruebas, las solicitudes para conexiones remotas o VPN no están autorizadas por jefes y/o gerentes.

Además de lo anterior, los proyectos del proceso no están alineados a la planeación estratégica de la empresa, realizando inversiones que no generan retorno, y, por consiguiente, no tienen el impacto que se espera en la operación, generando retrasos y/o reprocesos.

La empresa al no contar con un sistema de gestión de seguridad de la información ejecuta sus actividades sin una planificación direccionada o sin una metodología, que le permita realizar las tareas de forma secuencial y controlada. De esta manera, los servicios ofrecidos a sus empresas clientes no generan el valor agregado establecido en la propuesta comercial.

Esta situación puede generar, pérdida de información privilegiada, uso de recursos tecnológicos de forma inadecuada, accesos no autorizados, denegación de servicios, pago de sanciones legales, segregación de funciones, uso de contraseñas débiles, asesorías inadecuadas en temas de gobierno y gestión del proceso TIC.

Al implementar un sistema de gestión de seguridad de la información, Estrategias Empresariales de Colombia SAS, organizará su sistema de control interno tecnológico, mejorará el desarrollo de sus actividades y ofrecerá un servicio integral para la seguridad de la información a sus empresas clientes.

De igual manera, le permitirá generar confianza en los servicios que presta, lo cual tendrá un impacto directo sobre la imagen que se tiene de la empresa en el sector. Además, podrá ampliar su portafolio de servicios, generando crecimiento y rentabilidad.

El desarrollo de este proyecto busca identificar el grado de madurez del sistema de gestión de seguridad de la información para el proceso TIC en Estrategias Empresariales de Colombia S.A.S., tomando como marco de referencia la metodología establecida por la norma ISO 27001, la cual permite identificar los activos, los riesgos de seguridad de la información y su gestión en cuanto seguridad, confidencialidad, disponibilidad e integridad.

De esta manera, se dejarán las bases que le permitirán a la empresa minimizar el riesgo de pérdida de información crítica, administrar los recursos de forma efectiva y eficiente, establecer controles a las actividades realizadas al interior del proceso y generar una cultura que puede ser compartida y entregada a sus clientes.

3. OBJETIVOS

3.1. GENERAL

Identificar el nivel de madurez y diseñar los controles establecidos en los objetivos específicos para iniciar un Sistema de Gestión de Seguridad de la Información en el proceso TIC de Estrategias Empresariales de Colombia S.A.S,

3.2. ESPECIFICOS

- Realizar análisis GAP para identificar el estado actual de la empresa vs el Anexo A que se encuentra en la NTC-ISO-IEC 27001:2013.
- Definir el alcance, política, objetivos y responsabilidades frente al Sistema de Gestión de seguridad de la información,
- Establecer una metodología para la identificación de activos y gestión de riesgos de seguridad de la información del proceso TIC.
- Definir los procedimientos que hacen parte integral del sistema de gestión de la seguridad – SGSI de acuerdo con la norma ISO 27001:2013.

4. MARCO REFERENCIAL

4.1 MARCO TEORICO

La información en la actualidad se encuentra clasificada como uno de los activos más valiosos de la empresa, por lo cual debe ser cuidada para garantizar que no sea consultada o enviada a personal no autorizado. La información cada día está expuesta a amenazas, las cuales pueden ser aprovechadas, generando riesgos sobre los activos sensibles de la organización.[1]

En la actualidad los virus informáticos, el “hacking” y/o los ataques de denegación de servicio son algunos de los casos más comunes de pérdida de información. Es por ello que las empresas deben contar un sistema de gestión de seguridad de la información (SGSI), para minimizar los riesgos de pérdida de integridad, confidencialidad y disponibilidad de la información. En Colombia se dispone de una serie de Normas ISO 27000, que describen las actividades que se deben realizar para implementar y mantener los SGSI. [2]

1.Politica de seguridad de la información: Es un documento en el cual la gerencia de la empresa menciona su compromiso para mantener la confidencialidad, disponibilidad e integridad de la información, satisfacer los clientes, partes interesadas y contar con personal idóneo o competente, este documento debe ser medido con el fin de evidenciar su cumplimiento.

La NTC-ISO- 27001:2013, es una guía que establece los requisitos para la implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información o SGSI, que permite preservar la integridad, confidencialidad y disponibilidad de la información. Esta tiene una estructura de alto nivel alineada con el ciclo PHVA (planear, hacer, verificar y actuar). A continuación, se detalla la estructura y descripción de los numerales de la NTC-ISO- 27001:2013:

[1] Sistema de gestión de seguridad de la información. {En línea}. {10 Mayo 2017}, disponible en: http://www.iso27000.es/download/doc_sgsi_all.pdf

[2] Gestión de incidentes de seguridad de la información. {En línea}. {10 mayo 2017}, disponible en: <https://iso27002.wiki.zoho.com/13Incidentes.html>

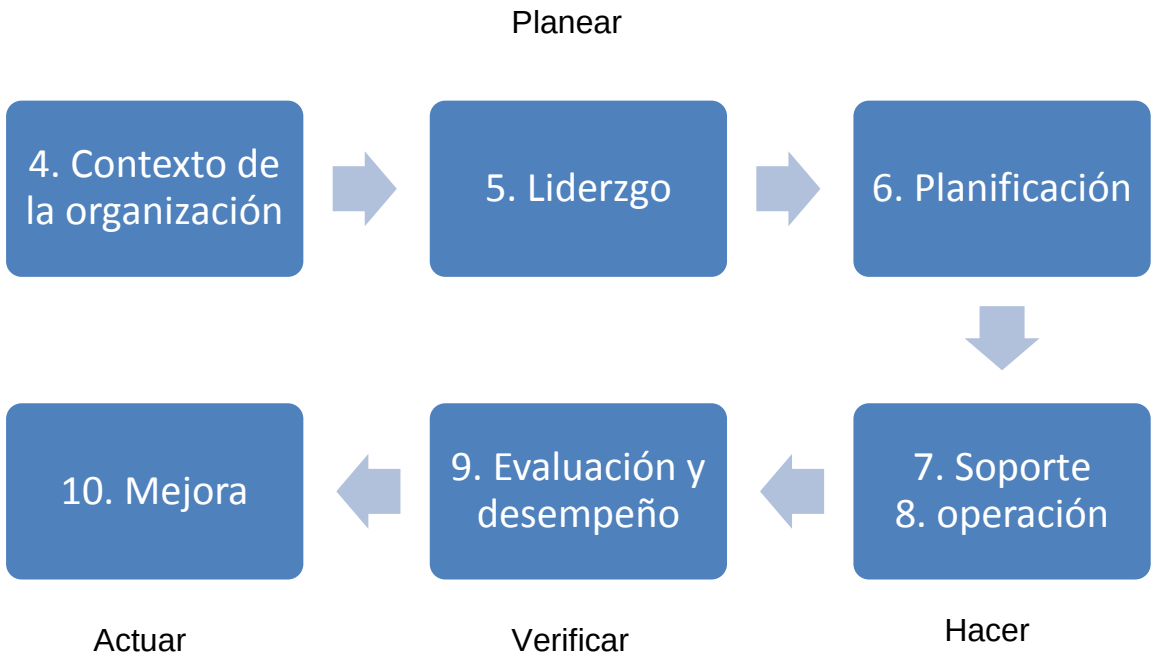


Imagen 1: Ciclo PHVA - planear, hacer, verificar y actuar

	Etapa	Actividad a implementar
	4. Contexto de la organización	- Conocimiento de la empresa. - Identificación de las partes interesadas.
	5. Liderazgo	- Establecer política de seguridad de la información. - Definir los roles y responsabilidades en el sistema de gestión de seguridad de la información. (SGSI).
	6. Planificación	- Identificar riesgos - Estimar riesgos - Evaluar riesgos - Tratamiento de riesgos - Aceptación de riesgos
	7. Soporte	- Definir los recursos para implementar, mantener y mejorar el sistema de gestión de seguridad de la información. - Determinar la competencia para el personal que tiene relación con la seguridad de la información.

		- Documentar los procedimientos necesarios para la seguridad de la información.
	8. Operación	- Evaluar riesgos. - Tratamiento de riesgos.
	9. Evaluación y desempeño	- Realizar auditoría interna - Realizar la revisión por la dirección.
	10. Mejora	- Establecer las acciones correctivas, no conformes y mejora del sistema de gestión de seguridad de la información.

Tabla 1: Descripción de los numerales de la NTC - ISO 27001:2013

Esta norma promueve la conservación de la confidencialidad, integridad y disponibilidad de la información con la que cuenta una empresa y establece 114 controles que se deben llevar a cabo para que la información sea utilizada para lo que fue dispuesta y no pueda ser accedida por personal no autorizado. A continuación, se describen los pilares de seguridad de la información (Instituto Colombiano de Normas Técnicas y Certificación ICONTEC. Compendio seguridad de la información, segunda edición 2015.[3]

Confidencialidad: La información solo estará disponible para el personal autorizado, esta no puede ser accedida por personal externo o ajeno a ella y en caso de suceder, estas no podrían acceder a la información o a su interpretación. La confidencialidad puede fundarse en normas legales, morales y/o en acuerdo entre partes (ICONTEC. Instituto Colombiano de Normas Técnicas y Certificación (2015) Compendio seguridad de la información, segunda edición.[4]

Integridad: La información debe estar completa, exacta e inalterable. Asegurar que no se ha realizado modificación desde su creación, es decir que la información es válida y consistente sin variación respecto a la original. (ICONTEC. Instituto Colombiano de Normas Técnicas y Certificación (2015) Compendio seguridad de la información, segunda edición[5].

[3] Mini SGSI. {En línea}. {10 Mayo 2017}, disponible en <https://www.incibe.es/protege-tu-empresa/blog/minisgsi>

[4] ICONTEC, Instituto Colombiano de Normas Técnicas. Compendio de seguridad de la información, segunda edición. 2015. P260

[5] ICONTEC, Instituto Colombiano de Normas Técnicas. Compendio de seguridad de la información, segunda edición. 2015. P260

Disponibilidad: La información solo debe ser accedida por personal autorizado, quien dispondrá de la misma en modo, el momento y lugar en que sea requiera, por lo que se debe asegurar la funcionalidad de los sistemas definidos para su consulta y tener respaldo en caso de contingencia. (ICONTEC. Instituto Colombiano de Normas Técnicas y Certificación (2015) Compendio seguridad de la información, segunda edición.[6]

Las empresas deben establecer controles para que los pilares (confidencialidad, disponibilidad e integridad) se implementen de forma adecuada. La Norma NTC-ISO- 27002:2013, contiene ejemplos de las actividades que se deben realizar para implementar los 114 controles que se encuentran documentados en el anexo A de la Norma NTC-ISO- 27001:2013. (Instituto Colombiano de Normas Técnicas y Certificación ICONTEC. Compendio seguridad de la información, segunda edición 2015.[7]

Para la construcción de un SGSI es importante definir o listar las amenazas a las que está expuesta la empresa y sus activos, estas se documentan con base en la metodología de riesgos Norma NTC ISO 31000 de 2009 o Norma NTC 27005:2009 e identificar las Leyes y regulaciones que aplican al sector y a TIC como: Ley 6003 de 2209 Derechos de autor, Ley 1273 de 2009 delitos informáticos[8], Ley 1581 Protección de datos personales[9].

La NTC-ISO- 27002:2013, es un estándar para la seguridad de la información y proporciona recomendaciones de las mejores prácticas en seguridad de la información, para implementar un sistema de gestión de seguridad de la información o SGSI. Esta consta de 14 dominios, 35 objetivos de control y 114 controles. Estos controles se pueden aplicar a cualquier tipo de empresa. A continuación, se detalla los 14 dominios de la NTC-ISO- 27002:2013:

[6] ICONTEC, Instituto Colombiano de Normas Técnicas. Compendio de seguridad de la información, segunda edición. 2015. P260

[7] ICONTEC, Instituto Colombiano de Normas Técnicas. Compendio de seguridad de la información, segunda edición. 2015. P260

[8] • DELTAASESORES. Ley 1273 de 2009. {En línea}. {10 mayo 2017}, disponible en internet: <http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia>

[9] • SIC. Protección de datos personales – Guía de responsabilidad demostrada. {En línea}. {10 Mayo 2017}, disponible en internet: <http://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada>

Imagen 2: Dominios de la NTC-ISO- 27002:2013

Al implementar un SGSI, se deben tener en cuenta las necesidades de las partes interesadas, los aspectos legales, el contexto o entorno de la empresa, los objetivos estratégicos, la misión, visión, políticas, clientes internos, externos y proveedores con el fin de establecer el norte o ruta.[10]

[10] Controles Anexo A NTC- NORMA ISO 27001:2013. {En línea}. {10 Mayo 2017}, disponible en: <http://www.iso27000.es/download/ControlesISO27002-2013.pdf>

Para la implementación y mantenimiento del sistema, la gerencia debe proporcionar los recursos que sean necesarios y documentar dicho compromiso en la política de seguridad de la información, la cual será revisada anualmente. El SGSI debe contar con información, implementación de controles de seguridad a los cuales se les puede realizar exclusiones, sin embargo, deben estar justificadas en un documento llamado declaración de aplicabilidad. Además, se debe establecer la gestión de riesgos. [11]

Contar con un sistema de gestión de seguridad de la información (SGSI) ayuda a las empresas a:

1. Minimizar el riesgo de pérdida de información
2. Establecer una metodología para validar la efectividad de los controles asociados a los riesgos identificados.
3. Implementar controles para validar la seguridad de la información.
4. Generar cultura para identificar las incidencias por cualquier empleado de la empresa.
5. Cumplir con la normatividad
6. Reconocimiento a nivel internacional.

Por lo anterior contar con un SGSI mejora los controles y actividades al interior del proceso TIC y minimiza la pérdida de información privilegiada, aumentando la seguridad, estabilidad y control interno del proceso, permitiendo establecer relaciones con aliados estratégicos en otros países. [12]

[11] Controles Anexo A NTC- NORMA ISO 27001:2013. {En línea}. {10 mayo 2017}, disponible en: <http://www.iso27000.es/download/ControlesISO27002-2013.pdf>

[12] Controles Anexo A NTC- NORMA ISO 27001:2013. {En línea}. {10 Mayo 2017}, disponible en: <http://www.iso27000.es/download/ControlesISO27002-2013.pdf>

4.2 MARCO LEGAL

NTC ISO 31000 de 2009: Esta Norma es llamada gestión de riesgos, principios directrices y se utilizada para gestionar los riesgos de la empresa sin importar su sector o tamaño. Su objeto es integrar el proceso de riesgos con el gobierno corporativo de la empresa, la planeación, los procesos y políticas. [13]

NTC ISO 27005:2009: Guía adoptada por el ICONTEC (Instituto Colombiano de Normas Técnicas) Que proporciona directrices para la gestión de riesgos de seguridad de la información, estas directrices se encuentran divididas en 7 pasos: establecimiento del contexto, identificación del riesgo, estimación del riesgo, evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo. [14]

LO 15/1999 -Ley de Protección de Datos de Carácter Personal: Es conocida como LOPD, la cual fue documentada y a la fecha es supervisada por la Agencia Española de protección de datos, con el fin de cuidar y proteger los derechos de los ciudadanos en cuanto a la información personal almacenada en bases de datos. [15]

La HIPAA es la Ley de Responsabilidad y Transferibilidad de Seguros Médicos (Health Insurance Portability and Accountability Act): Fue decretada en 1996 y protege los datos relacionados con salud de los ciudadanos, para que estos solo sean visualizados por el personal médico que los está tratando.[16]

Ley 603 de 2000

Por la cual se modifica el artículo 47 de la ley 222 de 1995**[17]** Esta es controlada por la Dirección de Impuestos y Aduanas Nacionales (DIAN) para prevenir el uso de software ilegal en las empresas. Al utilizar software legal minimiza el riesgo de pérdida de información e intrusión.[18]

---

[13] NTC ISO 31000 de. 2009 {En línea}. {10 mayo 2017}, disponible en https://calidadgestion.wordpress.com/2016/10/28/gestion-del-riesgo-iso-31000/

[14] ICONTEC, Instituto Colombiano de Normas Técnicas. Gestión del riesgo en la seguridad de la información. 2015. P68

[15] Ley de protección de datos personales España {En línea}. {10 mayo 2017}, disponible en: < http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/index-ides-idphp.php>

[16] HIPAA {En línea}. {10 mayo 2017}, disponible en: < http://www.davisvision.com/Que-es-la-HIPAA/

[17] Ley 603. {En línea}. {10 Mayo 2017}, disponible en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960>

[18]ALCALDIABOGOTA. Ley 603. {En línea}. {10 mayo 2017}, disponible en internet: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960>

Ley 1273 de 2009

Con la cual se modifica el código penal y 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**.**[19]

Ley 1581 de 2012

Por la cual se dictan disposiciones generales para la protección de datos personales, Reglamentada parcialmente por el Decreto Nacional 1377 de 2013**.**[20]**,** las empresas deben implementar un sistema de Gestión de protección de datos o SGPD para cuidar los datos de ciudadanos, clientes, proveedores y partes interesadas, la NTC ISO 27002: 2013 en el punto A 18.1.4 Privacidad y protección de información de datos personales.[21]

4.3 MARCO CONTEXTUAL

Los sistemas de información requieren de una estructura funcional para lograr su objetivo, cada componente tiene una función específica que le permite interactuar con los demás componentes, siendo los más elementales las personas, actividades, datos, redes y tecnología.[22]

La interrelación entre los componentes permite a las organizaciones modernas mantener la sinergia de la información en función del propósito del sistema, lo cual se refleja en la disponibilidad oportuna, especialmente en los procesos que implican la toma de decisiones de la alta gerencia. La seguridad de la información hace referencia a un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza. [23]

Estrategias Empresariales de Colombia S.A.S, es una empresa privada ubicada en la ciudad de Cali, que presta servicios de asesorías a los procesos administrativos, financiero, tesorería, jurídico, auditoría, comercial, tecnología y comunicaciones a

[19] Ley 1273 de 2009. {En línea}. {10 mayo 2017}, disponible en: <http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia>

[20] Ley 1581 de 2012. {En línea}. {10 Mayo 2017}, disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[21] SIC. Protección de datos personales. {En línea}. {10 mayo 2017}, disponible en internet: <http://www.sic.gov.co/proteccion-de-datos-personales>

[22] Whitten,J, Bentley, L. y Barlow, V. (2003). Análisis y diseño de sistemas de información. México : McGraw-Hill

[23] Ramió, J. (2006). Libro Electrónico de Seguridad Informática y Criptografía. Madrid España: Escuela electrónica de informática.

empresas en toda Colombia.[24] La misión es la excelencia en el servicio para facilitar la vida de nuestros clientes. Dentro los objetivos estratégicos de la empresa se encuentra el desarrollo del ser humano, la excelencia en el servicio y la calidad, crecimiento, rentabilidad sostenida y responsabilidad social. La estructura organizativa se encuentra relacionada en el organigrama.

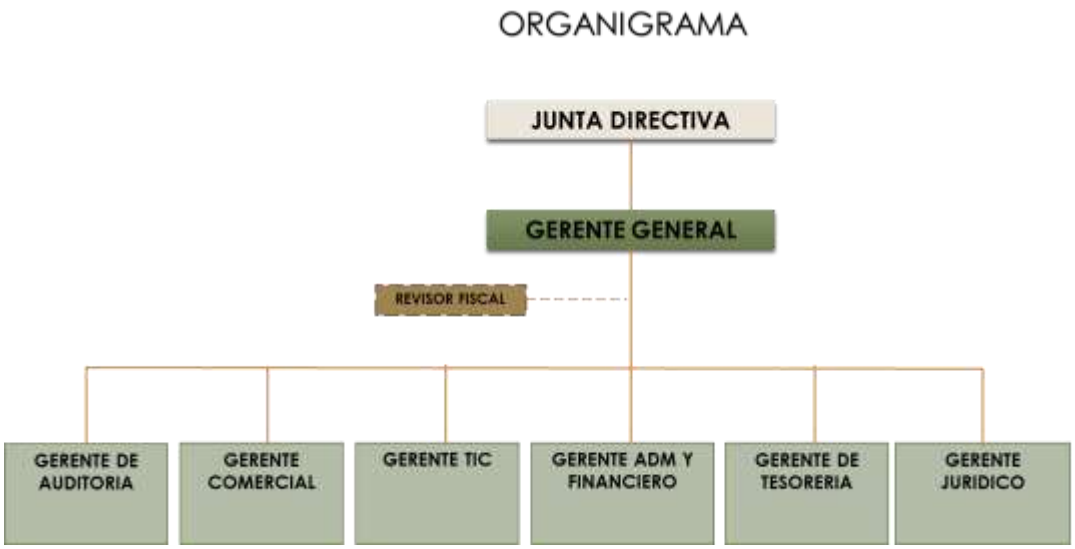


Imagen 3: Organigrama corporativo

El proceso TIC desarrolla, implementa, mantiene y gestiona la plataforma tecnológica para la operación de la empresa, tiene asociado cuatro subprocesos, (Servicios tecnológicos, infraestructura y comunicaciones, Desarrollo y ERP), encargados de soportar las operaciones de la empresa y asesorar a los clientes, el proceso cuenta con 24 colaboradores.

[24] Información tomada de Estrategias Empresariales de Colombia S.A.S, con corte a abril de 2017

Organigrama proceso TIC

Imagen 4: Organigrama proceso TIC

4.4 MARCO CONCEPTUAL

La seguridad de la información son las medidas que se toman en las empresas para proteger los activos y minimizar la pérdida de información privilegiada, estas medidas se establecen en políticas, procedimientos, seguridad lógica y física para que solo puedan ser utilizadas por personal autorizado. La información es procesada, enviada y almacenada en medios como equipos de cómputo, Smartphone, tabletas, lo cual la hace vulnerable. Un sistema de gestión de seguridad de la información debe contener:

Información documentada: Son los procedimientos que las empresas deben elaborar para implementar un sistema de gestión de seguridad de la información, teniendo en cuenta la forma de controlar y mantener, así como el medio en que se encuentre contenida la información para su conservación y consulta. – ISO 9001, Sistemas de gestión de la calidad, términos y definiciones[25]. [26]

Identificación y valoración de activos: Son las actividades que se deben realizar para medir las amenazas y vulnerabilidad que tienen los activos, de manera que se

[25] ICONTEC, Instituto Colombiano de Normas Técnicas. NTC ISO 9001:2015. 2015. P33

[26] Información documentada. {En línea}. {10 mayo 2017}, disponible en: <http://gestion-calidad.com/informacion-documentada-iso-27001-2013>

pueda determinar cuáles y como deben ser protegidos para mitigar el riesgo al que están expuestos [27]

Evaluación y tratamiento de los riesgos: Son las actividades realizadas para identificar el impacto y probabilidad de los riesgos y validar la efectividad de los controles o tratamientos, a través de una metodología estándar que sea conocida y apropiada por todos los involucrados al interior de la empresa.[28]

La seguridad de la información según la Norma NTC ISO27001:2013 consiste en la conservación de su confidencialidad, integridad y disponibilidad dentro de una organización. (Instituto Colombiano de Normas Técnicas y Certificación ICONTEC. Compendio seguridad de la información, segunda edición 2015.[29]

La empresa debe implementar controles, revisiones, auditorías con el fin de conocer el estado de los pilares. Estos deben realizarse con una frecuencia establecida al interior de la empresa y aprobada por la Gerencia. Las validaciones o controles más importantes son[30]:

- **Política de seguridad de la información**: Es un documento en el cual la gerencia declara el compromiso de tiempo, recursos (físicos, económico y humanos), responsabilidad social, con el sistema de gestión de seguridad de la información, este documento debe ser revisado mínimo cada año.[31]

- **Gestión de medios removibles:** Se deben establecer controles sobre la información almacenada en medios removibles como (discos duros, USB, cintas) con el fin de identificar las personas autorizadas para utilizarlos y los controles que se establecen sobres los mismos. [32]

---

[27] Metodología Magerit. {En línea}. {10 Mayo 2017}, disponible en: <https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/>

[28] NTC ISO 31000 de. 2009 {En línea}. {10 mayo 2017}, disponible en https://calidadgestion.wordpress.com/2016/10/28/gestion-del-riesgo-iso-31000/

[29] Controles de seguridad de la información. {En línea}. {10 mayo 2017}, disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

[30] ICONTEC, Instituto Colombiano de Normas Técnicas. Nueve claves para el éxito – una visión general de la implementación de la norma NTC-ISO/IEC 27001. 2016. P127

[31] Política de seguridad de la información. {En línea}. {10 mayo 2017}, disponible en: <https://iso27002.wiki.zoho.com/5-1-Pol%C3%ADtica-de-seguridad-de-la-informaci%C3%B3n.html>

[32] Gestión de puertos USB. {En línea}. {10 mayo 2017}, disponible en: <http://www.intedya.com/internacional/54/consultoria-gestion-de-la-seguridad-de-la-informacion-isoiec-27001.html>

- **Seguridad de las operaciones**: El objetivo de este control es evitar el acceso físico no autorizado a los recursos e información almacenada por los empleados y por las estaciones que la procesan, en este se incluyen los procedimientos gestión de cambios, gestión de capacidades, entre otros. [33]

- **Seguridad de las comunicaciones**: El objetivo de este control es blindar la información que es transmitida por las redes de la empresa, para garantizar que el pilar de la confidencialidad no sea vulnerado. Las empresas deben controlar los accesos internos y externos.[34]

- **Incidentes de seguridad de la información**: Las empresas deben establecer gestión de incidentes de seguridad de la información con el fin de identificar los riesgos a los que se encuentra expuesta la información. Todos los empleados deben estar en la facultad de reportar los incidentes al encargado de seguridad de la información.[35]

- **Control de acceso:** Controles que se establecen al interior de la empresa, para que el acceso a la red y software seguro. Con la definición de este control se concede la autorización para el uso de un sistema, software o área de la empresa.[36]

- **Auditoría de seguridad de la información**: Son las revisiones que se realizan al Sistema de gestión de seguridad de la información (SGSI) para determinar si es adecuado, si es acorde con lo establecido en la norma e identificar oportunidades de mejora.[37]

- **Declaración de aplicabilidad**: Es un documento donde se relacionan los 114 controles del anexo A, para comprobar y contar con evidencia de que la empresa creó los controles establecidos por la Norma NTC ISO 27001:2013.[38]

---

[33] Seguridad informática o seguridad de la información. {En línea}. {10 mayo 2017}, disponible en: <http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html>

[34] ISO, International Organization for Standardization Information technology -- Security techniques. Information security management systems Overview and vocabulary. 2016. P37

[35] Gestión de incidentes de seguridad de la información. {En línea}. {10 mayo 2017}, disponible en: <https://iso27002.wiki.zoho.com/13Incidentes.html>

[36] ISO, International Organization for Standardization Information technology -- Security techniques. Information security management systems Overview and vocabulary. 2016. P37

[37] ISO, International Organization for Standardization Information technology -- Security techniques. Information security management systems Overview and vocabulary. 2016. P37

[38] Declaración de aplicabilidad. {En línea}. {10 mayo 2017}, disponible en: <https://www.idu.gov.co/documents/20181/251887/FO-TI-27+Formato+Declaracion+de+Aplicabilidad++V_1.0+-+Diligenciado+Dic2015.pdf/1138b1b6-6f0c-41cf-85b1-7383c5f15f54>

- **Continuidad de negocio**: La empresa debe gestionar la continuidad de la seguridad de la información durante el uso de la misma, pruebas, planes de contingencia y regreso a la normalidad de las operaciones. Se debe establecer un plan de pruebas para conocer el uso adecuado de la información. [39]

- **Magerit**: Es una metodología gratuita para la identificación, análisis, valoración y gestión de activos y riesgos de seguridad de la información. Creada por Consejo Superior de Administración Electrónica. La metodología se encuentra disponible en su página WEB.[40]

[39] Contingencia TIC vs continuidad de negocio. {En línea}. {10 mayo 2017}, disponible en <https://www.incibe.es/protege-tu-empresa/blog/contingencia-vs-continuidad>

[40] Metodología Magerit. {En línea}. {10 Mayo 2017}, disponible en: <https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/>

5. DISEÑO METODOLÓGÍCO PRELIMINAR

La metodología utilizada para verificar el estado actual de la empresa frente a los requisitos del Anexo A[41] que se encuentra en la Norma NTC- ISO 27001:2013, es cuantitativa, y se desarrollara a través de la aplicación de encuestas, entrevistas, reuniones y observación con el fin de diseñar el sistema de gestión de seguridad de la información para la empresa Estrategias Empresariales de Colombia S.A.S.

Para el diseño del sistema de gestión de seguridad de la información (SGSI), se tendrá en cuenta el ciclo Deming o ciclo PHVA que consiste en planear, hacer, verificar y actuar, este se aplica en todas las fases del proyecto, en la construcción de documentos, políticas y procedimientos. La metodología se aplica de la siguiente forma: [42]

En la etapa planear se definen los objetivos, política de seguridad de la información, se identifican las necesidades de las partes interesadas, las regulaciones y las Leyes. En la etapa hacer se definen los responsables del SGSI, en la etapa verificar se valida que la política y objetivos se cumplan. En la etapa actuar se establecen las mejoras del SGSI. [43]

5.1 TIPO DE INVESTIGACIÓN

La investigación a realizar es de tipo exploratoria y cuantitativa, puesto que busca analizar el estado actual de los controles del Anexo A[44] de la NORMA NTC/ISO 27001:2013, identificar las necesidades de las partes interesadas.[45] Explicativa puesto que se analizará la información obtenida en cuestionarios, observaciones, entrevistas, para establecer procedimientos, políticas, riesgos, controles y seguridad de los activos.

A continuación, se detallan las actividades que se realizaran para cumplir con los objetivos establecidos:

---

[41] Anexo A. {En línea}. {10 mayo 2017}, disponible en <https://advisera.com/27001academy/es/knowledgebase/resumen-del-anexo-a-de-la-norma-iso-270012013/>

[42] Ciclo Deming. {En línea}. {10 Mayo 2017}, disponible en: <http://www.pmg-ssi.com/2015/06/iso-27001-ciclo-de-deming/>

[43] Ciclo Deming. {En línea}. {10 mayo 2017}, disponible en: <http://www.pmg-ssi.com/2015/06/iso-27001-ciclo-de-deming/>

[44] Controles Anexo A NTC- NORMA ISO 27001:2013. {En línea}. {10 mayo 2017}, disponible en: <http://www.iso27000.es/download/ControlesISO27002-2013.pdf>

[45] • ICONTEC, Instituto Colombiano de Normas Técnicas. Compendio de seguridad de la información, segunda edición. 2015. P260

Tabla 2 Actividades a realizar para el diseño del SGSI

1	Realizar diagnóstico del estado actual de los procesos vs el Anexo A de la Noma NTC-ISO-IEC 27001:2013.
2	Definir los responsables de la seguridad de la información.
3	Validar las necesidades y requerimientos de las partes interesadas de la empresa frente a la seguridad de la información.
4	Definir el alcance del Sistema de gestión de seguridad de la información y que este sea adecuado con los objetivos de la empresa.
5	Definir la política y objetivos de seguridad de la información.
6	Realizar la valoración de los activos de seguridad de la información del proceso TIC.
7	Validar los riesgos de seguridad de la información del proceso TIC, revisando los controles de los mismos.
8	Asesorar en el diseño de la información documentada.
9	Definir la declaración de la aplicabilidad

Fuente: El autor

5.2. POBLACIÓN

El diseño del sistema de gestión de seguridad de la información – SGSI, bajo la Norma NTC ISO 27001:2013, se realizará en el proceso de tecnología y comunicaciones TIC de la empresa Estrategias Empresariales de Colombia S.A.S., ubicada en la ciudad de Cali.[46]

5.3. MECANISMOS PARA RECOLECCIÓN DE INFORMACIÓN

Para la recolección de información que se requiere en el desarrollo del proyecto se solicitará aprobación a la empresa para el uso de su información, se realizarán entrevistas, observaciones, encuestas con el personal del proceso TIC, gestión humana, logística, jurídico y auditoría. También se validarán documentos o libros físicos y electrónicos relacionados con seguridad de la información, seguridad informática y la Norma NTC ISO 27001:2013. [47]

[46] Información tomada de Estrategias Empresariales de Colombia S.A.S, con corte a abril de 2017
[47] ICONTEC, Instituto Colombiano de Normas Técnicas. Nueve claves para el éxito – una visión general de la implementación de la norma NTC-ISO/IEC 27001. 2016. P127

6. RESULTADO

6.1 ANÁLISIS GAP

El objetivo de realizar el análisis de brechas o análisis GAP, es comparar el estado actual de la empresa frente al cumplimiento de los 114 controles documentados en el anexo A que se encuentra en la Norma NTC- ISO 27001:2013, con el fin de evaluar el nivel de madurez de los mismos.[48]

Se validaron los controles del anexo A de la Norma ISO 27001:2013, que se relacionan a continuación[49]:

1. Políticas de seguridad de la información
2. Organización de la seguridad de la información.
3. Seguridad de los recursos humanos
4. Gestión de activos
5. Control de acceso
6. Criptografía
7. Seguridad física y del entorno.
8. Seguridad de las operaciones
9. Seguridad de las comunicaciones
10. Adquisición, desarrollo y mantenimiento de sistemas
11. Relaciones con los proveedores
12. Gestión de incidentes de seguridad de la información
13. Aspectos de seguridad de la información de la gestión de continuidad del negocio
14. Cumplimiento

Para la realización de esta actividad se generó un listado con los procesos de la empresa y estos se asociaron a los 114 controles contenidos en el anexo A, con el fin de identificar el personal a entrevistar. De igual manera, diseño una pregunta para cada control en una lista de chequeo, en donde se analiza y evalúa el nivel de madurez.

La lista de chequeo está conformada por diez (10) columnas que permiten calificar los cientos catorce (114) controles del anexo A, con las actividades ejecutadas actualmente en la empresa. A continuación, se presenta una descripción, con el fin de realizar de manera apropiada la calificación:

---

[48] Análisis GAP. {En línea}. {10 mayo 2017}, disponible en: http://www.sigea.es/assessment27001.pdf

[49] ICONTEC, Instituto Colombiano de Normas Técnicas. Compendio de seguridad de la información, segunda edición. 2015. P260

- **Ítem:** Contiene la numeración del Anexo A de la norma NTC-ISO/IEC 27001:2013.
- **Controles del Anexo A:** Controles del Anexo A de la norma NTC-ISO/IEC 27001:2013 a evaluar.
- **RE:** Es la respuesta que se obtiene durante la entrevista y/o revisión documental. Las respuestas pueden ser SI, NO, NA y PA, que se explican a continuación.

    - **SI:** Se selecciona de forma automática en caso de que en la casilla de "RE" la respuesta sea "si". Hace referencia a que el control está implementado según lo documentado en el control.

    - **NO:** Se selecciona de forma automática en caso de que en la casilla de "RE" la respuesta sea "no". Hace referencia a que el control no está implementado.

    - **NA:** Se selecciona de forma automática en caso de que en la casilla de "RE" la respuesta sea "na". Hace referencia a que el control no aplica en la organización.

    - **PA:** Se selecciona de forma automática en caso de que en la casilla de "RE" la respuesta sea "pa". Hace referencia a que el control está implementado según lo documentado en el control, pero de forma parcial.

- **Cumplimiento control:** Consolida el porcentaje de cumplimiento de los numerales.

Para la identificación del nivel de madurez el cual es basado en el estándar internacional COBIT 4.1, se utiliza la tabla No. 2 la cual describe y establece los parámetros o rangos de calificación de cada objetivo de control de la Norma NTC ISO 27001: 2013:

Tabla 3: Nivel de madurez

Nivel de madurez	Limite inferior	Limite superior
Optimizado	91%	100%
Administrado	71%	90%
Definido	61%	70%
Repetible	40%	60%
Inicial	16%	39%
Inexistente	0%	15%

Fuente: El autor

A continuación, se relaciona la explicación de cada uno de los niveles de madurez:

Nivel 0 - Inexistente: La empresa no ha reconocido siquiera que existe un problema a resolver.[50]

Nivel 1 - Inicial: Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar, en su lugar existen enfoques ad hoc[51] que tienden a ser aplicados de forma individual o caso por caso. [52]

Nivel 2 - Repetible- La empresa ha documentado procedimientos y si estos se aplican en todos los procesos que interviene en la realización de la actividad. La empresa no tiene establecido un plan de formación, la ejecución del procedimiento es responsabilidad del empleado, por esta razón la probabilidad de errores es alta.[53]

Nivel 3 - Definido: Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida si utilizarlos o no, y es poco probable que se detecten desviaciones.[54]

Nivel 4 - Administrado: Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se llega a utilizar la automatización y herramientas de una manera limitada o fragmentada.[55]

Nivel 5 - Optimizado: El desarrollo y ejecución de procesos tienen nivel de madurez alto y se encuentra basado en la mejora continua. El proceso tecnológico o TIC trabaja en la automatización de las actividades, para que el proceso realice las actividades con calidad y efectividad.[56]

---

[50] MSAFFIRIO. NIVEL DE MADUREZ {En línea}. {10 mayo 2017}, disponible en internet https://msaffirio.wordpress.com/2008/06/21/escala-de-madurez-%E2%80%93-process-maturity-model/

51 Ad hoc: Generalmente se refiere a una solución específicamente elaborada para un problema o fin preciso

[52] MSAFFIRIO. NIVEL DE MADUREZ {En línea}. {10 mayo 2017}, disponible en internet https://msaffirio.wordpress.com/2008/06/21/escala-de-madurez-%E2%80%93-process-maturity-model/

[535353] MSAFFIRIO. NIVEL DE MADUREZ {En línea}. {10 mayo 2017}, disponible en internet https://msaffirio.wordpress.com/2008/06/21/escala-de-madurez-%E2%80%93-process-maturity-model/

[54] MSAFFIRIO. NIVEL DE MADUREZ {En línea}. {10 mayo 2017}, disponible en internet https://msaffirio.wordpress.com/2008/06/21/escala-de-madurez-%E2%80%93-process-maturity-model/

[5555] MSAFFIRIO. NIVEL DE MADUREZ {En línea}. {10 mayo 2017}, disponible en internet https://msaffirio.wordpress.com/2008/06/21/escala-de-madurez-%E2%80%93-process-maturity-model/

[56] MSAFFIRIO. NIVEL DE MADUREZ {En línea}. {10 mayo 2017}, disponible en internet https://msaffirio.wordpress.com/2008/06/21/escala-de-madurez-%E2%80%93-process-maturity-model/

El desarrollo de esta encuesta se encuentra documentado en el Anexo A.

Entregable de Análisis GAP

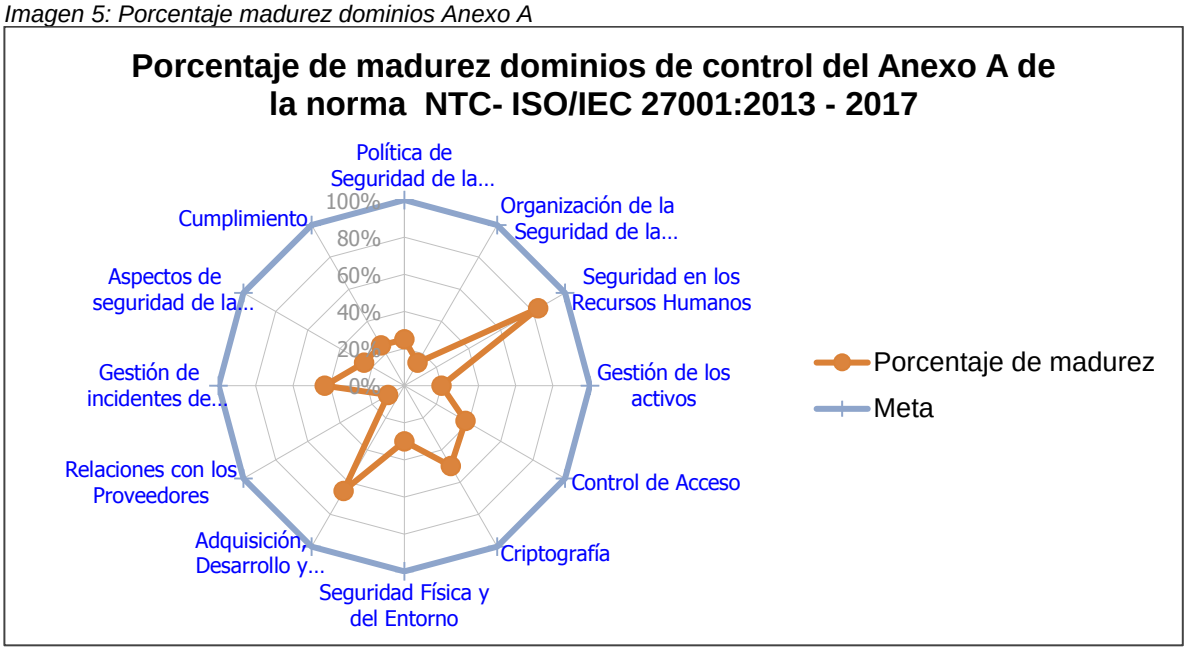
A continuación, se presenta el resultado del diagnóstico de los controles definidos en el anexo A de la norma NTC-ISO/IEC 27001:2013. El porcentaje y nivel de madurez de cada uno en la empresa Estrategias Empresariales de Colombia SAS., se presenta en la tabla No. 3

Tabla 4: Resultado

Ítem	Dominios	Porcentaje de madurez	Meta	Nivel de madurez Dominios
A.5..	Política de Seguridad de la Información	25%	100%	Inicial
A.6..	Organización de la Seguridad de la Información	14%	100%	Inexistente
A.7..	Seguridad en los Recursos Humanos	83%	100%	Administrado
A.8..	Gestión de los activos	20%	100%	Inicial
A.9..	Control de Acceso	38%	100%	Inicial
A.10..	Criptografía	50%	100%	Repetible
A.11..	Seguridad Física y del Entorno	30%	100%	Inicial
A.11.1.	Áreas Seguras			
A.14..	Adquisición, Desarrollo y Mantenimiento de Sistemas	65%	100%	Definido
A.15..	Relaciones con los Proveedores	10%	100%	Inexistente
A.16..	Gestión de incidentes de Seguridad de la Información	43%	100%	Repetible
A.17..	Aspectos de seguridad de la información de la Gestión de Continuidad de Negocio	25%	100%	Inicial
A.18..	Cumplimiento	25%	100%	Inicial
TOTAL	TOTAL	36%	100%	Inicial

Fuente: El autor

Imagen 5: Porcentaje madurez dominios Anexo A



Fuente: El autor

Se identifica que la empresa tiene un nivel de madurez de un **36%** frente a los 114 controles del Anexo A, encontrándose en un nivel de madurez **Inicial,** lo cual indica que "Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar, en su lugar existen enfoques ad hoc[57] que tienden a ser aplicados de forma individual o caso por caso."[58]

De acuerdo con este resultado el proceso TIC debe realizar o implementar políticas con el fin de garantizar la continuidad de las operaciones, minimizar el riesgo de pérdida de información privilegiada, salvaguardar los activos de la empresa y generar control, estas políticas deben ser creadas, aplicadas y socializadas con todo el personal de la empresa.

DESARROLLO

Siguiendo lo establecido por la Norma NTC- ISO 27001:2013, donde se relaciona los componentes que debe contener un sistema de gestión de seguridad de la información (SGSI), los cuales desarrollan en este proyecto y se relacionan a continuación en la siguiente gráfica:

57 Ad hoc: Generalmente se refiere a una solución específicamente elaborada para un problema o fin preciso

58 MSAFFIRIO. NIVEL DE MADUREZ {En línea}. {10 mayo 2017}, disponible en internet https://msaffirio.wordpress.com/2008/06/21/escala-de-madurez-%E2%80%93-process-maturity-model/

Imagen 6: Componentes del Sistema de gestión de seguridad de la información

A continuación, se describe como a través del diseño del presente proyecto, se desarrollaron cada uno de esos componentes propuestos en el cronograma de trabajo, estos son basados en la Norma NTC- ISO 27001:2013 y Norma NTC- ISO 27002:2013:

7. CONTEXTO

7.1 IDENTIFICACIÓN DE LAS PARTES INTERESADAS

Para iniciar el desarrollo de un SGSI, es importante conocer información que muestre o ilustre por que la empresa requiere un sistema de gestión de seguridad de la información, cuáles son sus objetivos en la prestación del servicio a quienes afecta y quienes son las partes interesadas que interviene.

Para identificar las necesidades de las partes interesadas de la empresa se realizó reunión con todas las personas que intervienen en la prestación del servicio, donde se identificaron: sus necesidades, impacto y nivel de influencia. El nivel de influencia e interés fue evaluado con la Gerencia General y se refleja en la tabla que se relaciona a continuación:

Tabla 5: Necesidades de las partes interesadas

Parte interesada	Denominación	Objetivo	Nivel de influencia	Nivel de interés
CLIENTES	Empresas ubicadas en cualquier ciudad del país que requieran servicios de auditoría y consultoría	Prestar servicios oportunos y confiables	ALTO	ALTO
EMPLEADOS	Gerentes, Directores, Jefes, Coordinadores, Asistentes, Auxiliares	Satisfacer a los clientes, entregar estabilidad laborar y bienestar	BAJO	ALTO
SOCIOS	Junta directiva	Contar con rentabilidad, buen nombre	ALTO	ALTO
PROVEEDORES	Operador tecnológico, hosting, Redes, Dispositivos, Software	Cumplir con los pagos, entregar los requerimientos de forma clara	BAJO	ALTO

Fuente: El autor

Con este insumo la empresa ya ha identificado sus partes interesadas, objetivos para dar inicio al diseño de un sistema de gestión de seguridad de la información SGSI. Al calificar el nivel de influencia e interés se valora el impacto que tiene la parte interesada para la empresa.

8. LIDERAZGO

8.1 RESPONSABILIDADES EN EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

En esta etapa se definen las personas responsables de llevar a cabo las actividades para el diseño del sistema de gestión de seguridad de la información basado en la Norma NTC- ISO 27001:2013[59] y así dar la puesta en marcha para que este se implemente y se mantenga.

Para desarrollar este punto se realizó una reunión con los líderes de proceso, se explicaron las responsabilidades y actividades que se deben ejecutar para implementar y mantener un SGSI, de acuerdo con lo descrito en la Norma NTC ISO 27001:2013. Se creó una tabla con los cargos que tiene la empresa y se asociaron las responsabilidades citadas que cada uno debe asumir.

La Gerencia General y los líderes aceptaron estas actividades y definieron que estas se incluirán en los perfiles de cargo para posterior socialización. La tabla responsabilidades en el sistema de gestión de seguridad de la información, se encuentra en el Anexo B.

[59] ICONTEC, Instituto Colombiano de Normas Técnicas. Compendio de seguridad de la información, segunda edición. 2015. P260

9. ALCANCE DEL SGSI

La Norma ISO 27001:2013 en su numeral 4.3 describe “la organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad para establecer su alcance” Para desarrollar el alcance se realizó reunión con la gerencia y el responsable del SGSI y se determinó el alcance [60] del SGSI así: el sistema de gestión de seguridad de la información SGSI, cubre los servicios prestados por el proceso de TIC, con el fin de incrementar la seguridad de la información de los activos de la empresa la integridad, disponibilidad y confidencialidad de la información manejada por los procesos.[61]

9.1 POLÍTICA DE SEGURIDAD DEL SGSI

Para el desarrollo de este punto se realizó reunión con la gerencia y el responsable del SGSI y se definió: La dirección de Estrategias Empresariales de Colombia S.A.S., reconoce la importancia de gestionar la información y se ha comprometido en la implementación y mantenimiento de un sistema de gestión de seguridad de la información (SGSI), para asegurar la confidencialidad, integridad y disponibilidad de la información. Con el fin de garantizar que la política se cumpla la gerencia revisará anualmente:

- Los objetivos de seguridad de la información.
- Velará por que se realice de forma adecuada el análisis y tratamiento de riesgos.
- Revisará el adecuado tratamiento de las desviaciones identificadas en el SGSI.

9.2 OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos del Sistema de Gestión de Seguridad de la Información se documentan con el fin de evaluar si se cumplen los compromisos descritos en la política del sistema de gestión de seguridad de la información, los cuales se detallan a continuación:

---

[60] ICONTEC, Instituto Colombiano de Normas Técnicas Guía para la implementación de un sistema de gestión de seguridad de la información. 2014. P81

[61] • ICONTEC, Instituto Colombiano de Normas Técnicas. Compendio de seguridad de la información, segunda edición. 2015. P260

- Aumentar la protección de los activos de seguridad de la empresa
- Implementar y mantener programas de sensibilización en temas relacionados con la seguridad de la información.
- Minimizar los riesgos de los activos, conservando la confidencialidad, integridad y disponibilidad.

El desarrollo de la política remitirse al Anexo C.

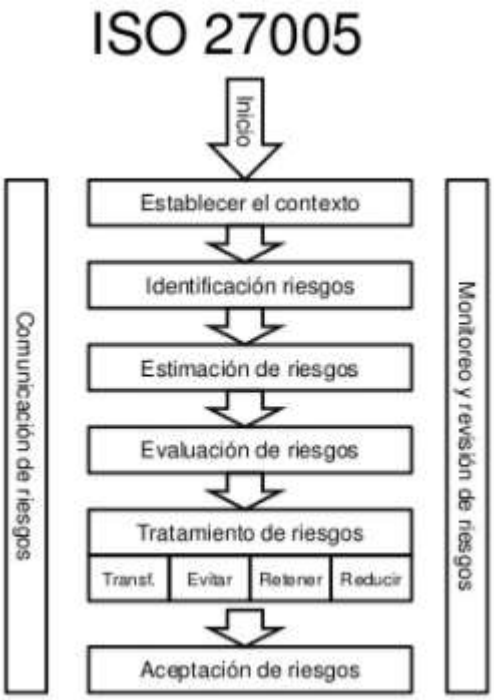
10. PLANEACIÓN

En esta fase se define la metodología para gestionar los riesgos de seguridad de la información, la empresa utiliza el estándar ISO 31000:2009, por esta se estableció utilizar la metodología ISO 27005, que se integra con la utilizada y permite identificar y valorar los activos de seguridad de la información.

10.1 METODOLOGÍA GESTIÓN DE RIESGOS

Para desarrollar este punto se realizó una reunión con los líderes de proceso, la coordinadora de calidad y la gerencia general, donde se explicaron cada uno de los puntos de la Norma NTC ISO 27005:2008[62] [63] y como se alinea con la metodología creada. A continuación, se relacionan los pasos de la Norma:

Tabla 6:: ISO 27005:2008



Fuente: https://es.slideshare.net/besair/latin-cacs-isaca-2009-312-auditoria-de-la-gestion-de-riesgos-de-tecnologiamaricarmen-garcia

[62] ICONTEC, Instituto Colombiano de Normas Técnicas. Gestión del riesgo principios y directrices. 2011.P29

[63] ICONTEC, Instituto Colombiano de Normas Técnicas. Gestión del riesgo en la seguridad de la información. 2015. P68

Esta metodología se socializó con las personas involucradas en el diseño de este proyecto en la empresa, resaltando los pasos a seguir y las actividades que se deben realizar para gestionar los riesgos del proceso TIC. (ICONTEC, 2008). La metodología se encuentra en el ANEXO D de este documento.

Con el desarrollo de esta, se identificaron en conjunto con los líderes de cada proceso, los riesgos asociados a sus activos de información, lo cual permitió dar claridad en la cuantificación del activo, es decir, identificar su valor, amenazas y vulnerabilidades de manera particular. De esta manera, se establecieron con una base sólida, los controles más apropiados para cada uno de ellos y se consolido la forma en la cual deben ser evaluados y actualizados.

Cada riesgo fue valorado de acuerdo a las escalas de medición concertadas con los responsables de la gestión de los mismos.

Teniendo como guía estas escalas, se determinó que los riesgos a tratar serían aquellos cuya calificación se encuentra definida como ALTO y MUY ALTO, ya que son lo que resultan más críticos por afectar directa y significativamente la operación de la empresa.

10.2 LEVANTAMIENTO DE ACTIVOS DE INFORMACIÓN DEL PROCESO TIC

Para iniciar el levantamiento de activos de información se realizó una reunión con los jefes, el director y el gerente de TIC, donde se explicó cómo identificarlos y calificarlos. El inventario de activos debe realizarse identificando aquellos que contienen información de la empresa, empleados y partes interesadas como software, bases de datos, equipos de cómputo, servidores, personas que conocen o manejan información sensible y otros de acuerdo con la metodología gestión de riesgos.

Al tener identificados los activos se debe: calificar la integridad, disponibilidad, confidencialidad e impacto. Después de tener estos resultados se establecen los controles aquellos que su calificación fue altos y muy alto. (SSI, 2017). La matriz de riesgos de SGSI, se encuentra en el Anexo E. El plan de tratamiento se encuentra en el Anexo F.

Los activos de información se identificaron tomando como guía la norma ISO 27001, valorando cada activo según el tipo, clase y valor. Además, el establecer las amenazas, permitió conocer las vulnerabilidades a que están expuestos los activos, clasificarlos según estas y definir detalladamente cuales son las que se presentan desde el punto de vista lógico, físico, locativo, legales y naturales.

El impacto de cada activo, fue calificado por su responsable, de acuerdo al criterio que tiene en cuanto al daño que se ocasionaría en el momento en que las amenazan se materialicen sobre cada una de las vulnerabilidades identificadas.

De acuerdo con las escalas de clasificación y la metodología establecida, se logró identificar con cada líder de proceso, los activos de información y cuáles de estos son los que resultan más críticos para la empresa (SERVIDOR SIIGO PRODUCCION, SERVIDOR SIIGO CONTINGENCIA) y los respectivos controles a implementar. (ver anexo F).

11. SOPORTE

En esta etapa se definen los procedimientos que forma parte del sistema de gestión de seguridad de la información SGSI, antes de iniciar con la documentación de los mismo se debe definir su estructura, es importante que los documentos se pongan a disposición del personal que lo requiera, los documentos originales y versionados deben ser custodiados y administrados por el director de seguridad. A continuación, se detallan los procedimientos elaborados:

11.1 INFORMACIÓN DOCUMENTADA DEL SGSI TIC

Tabla 7: PROCEDIMIENTO DE GESTIÓN DE INCIDENTES

	**PROCESO: TIC**	Código	TIC- PRO- O2
		Versión	1
	PROCEDIMIENTO	Fecha	17 /10/2017
		Clasificación	Privado
		Página 1	

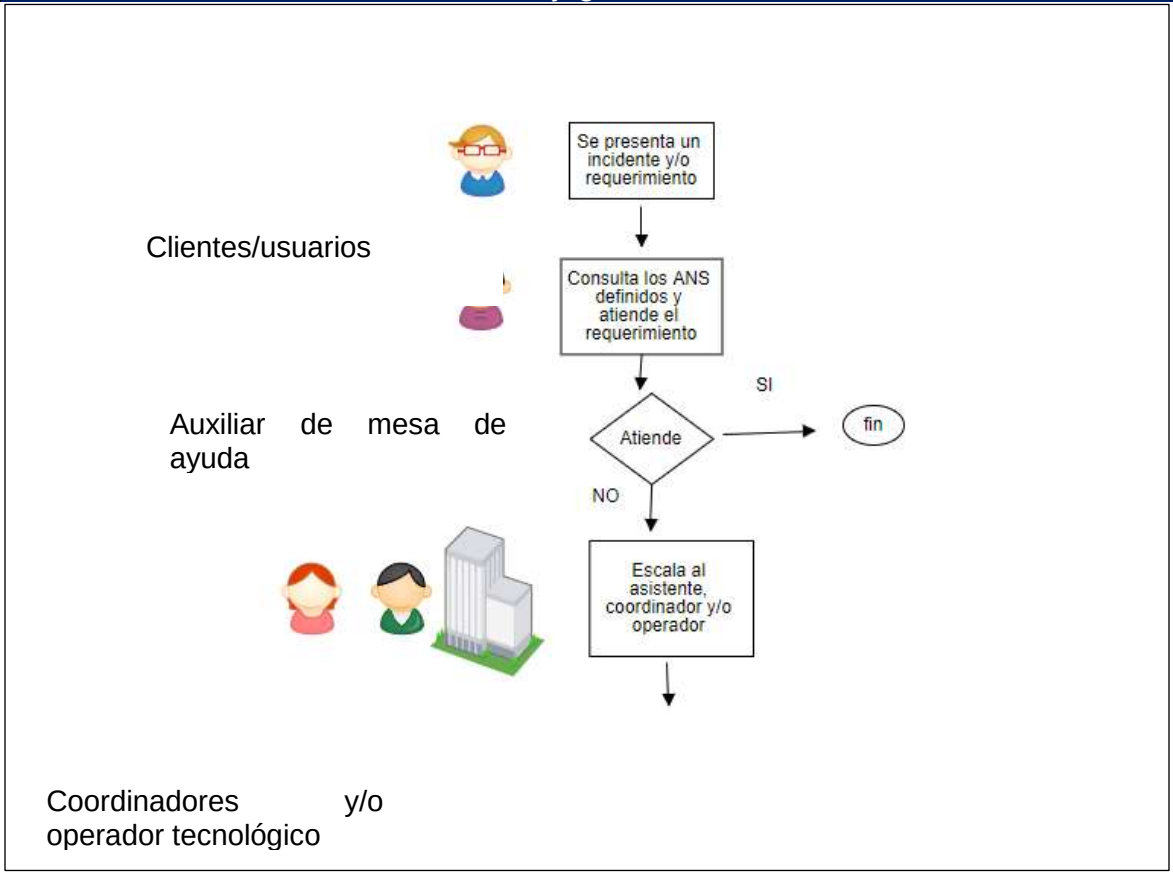
Nombre del procedimiento	GESTIÓN DE INCIDENTES
Objetivo	Brindar los lineamientos para atender las solicitudes que se clasifiquen como requerimientos incidentes que afecten la prestación del servicio cómo la disponibilidad, integridad o confidencialidad de los activos de información de la empresa[64].
Alcance	El procedimiento inicia con la identificación de un incidente por parte del cliente o parte interesada.
Responsables	Gerente de TIC

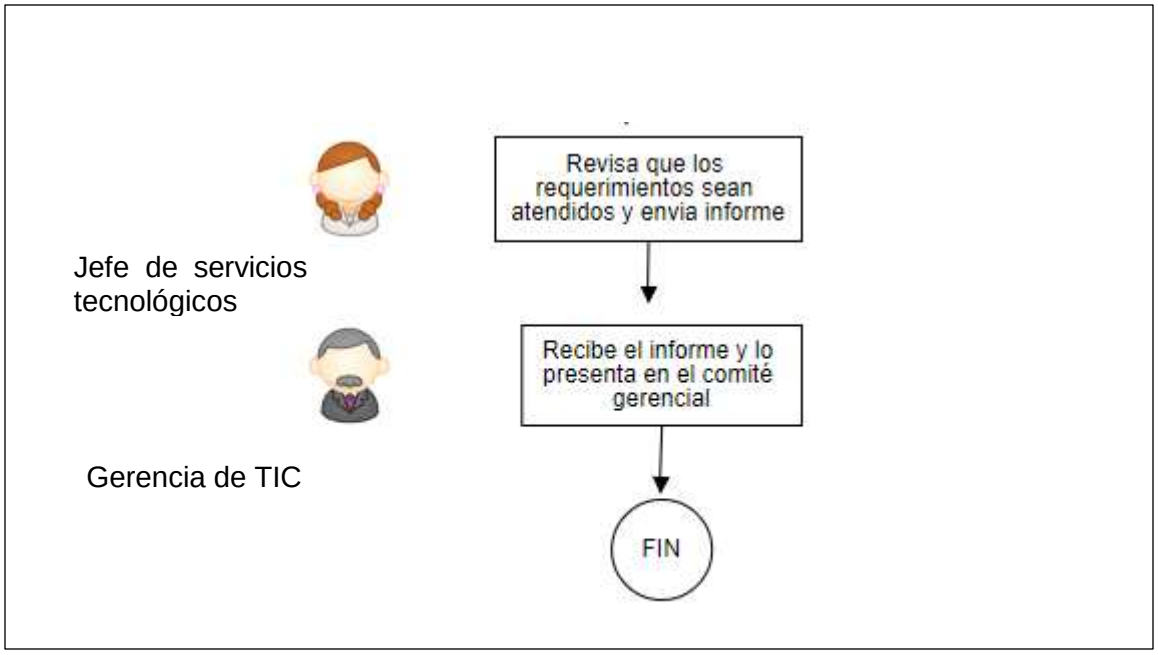
Actividades	Líder de la actividad
Se presenta una necesidad que puede ser: Requerimientos del servicio, Incidentes, Requerimientos de Desarrollo, entre otros, este registra por medio de la mesa de ayuda el ticket	Clientes /usuarios
consulta los acuerdos de niveles de servicio definidos con los clientes para atender las solicitudes registradas en la mesa de ayuda SYSAID	Auxiliar de mesa de ayuda

[64] ICONTEC, Instituto Colombiano de Normas Técnicas. Compendio de seguridad de la información, segunda edición. 2015. P260

ayuda atiende los Requerimientos del servicio categorizados como bajos, tales como: Creación de usuarios, cuentas de correo, reseteo de contraseñas, entre otros similares.	Auxiliar de mesa de ayuda
En caso de no poder ser atendida la escala	Asistente de mesa de ayuda
Analiza y resuelve la solicitud, a su vez le notifica al cliente sobre los avances y solución de manera oportuna y eficiente	Asistente de mesa de ayuda
En caso de que la solicitud no pueda ser solucionada este deberá escalarla a un nivel superior	Coordinadores y/o operador tecnológico
Verifican que toda solicitud se encuentre registrada y atendida desde la mesa de ayuda. Los incidentes graves, repetitivos y/o bloqueantes sean documentados en la base de datos de conocimiento	Jefe de servicios tecnológicos
Diligencia el formato TIC-F-02 Informe tickets de manera mensual con sus respectivos indicadores, el cual se debe enviar a su supervisor inmediato	Jefe de servicios tecnológicos
Recibe el informe y lo presenta en el comité gerencial	Gerente de TIC
Nota: Si identifica que el requerimiento es un incidente grave o de seguridad lo escala	Director de seguridad

Flujograma





Fuente: El autor

Tabla 8: PROCEDIMIENTO DE GESTIÓN DE ACTIVOS

	PROCESO: TIC	Código	TIC- PRO- O3
		Versión	1
	PROCEDIMIENTO	Fecha	17/10/2017
		Clasificación	Privado
		Página 1	

Nombre del procedimiento	GESTIÓN DE ACTIVOS
Objetivo	Mantener actualizado el inventario de activos de la información de la empresa
Alcance	Aplica para la gestión de activos de seguridad de la información de la empresa.
Responsables	Director de seguridad de la información Directora de Auditoría TIC

Actividades	Líder de la actividad
La empresa cuenta con una matriz que contiene los activos de seguridad de la información en donde se califica o identifica la integridad, disponibilidad y confidencialidad de los mismos. La matriz debe documentarse y actualizarse cada que se presenten cambios o nuevos activos. Si no se presentan cambios se debe actualizar cada año	Director de seguridad de la información

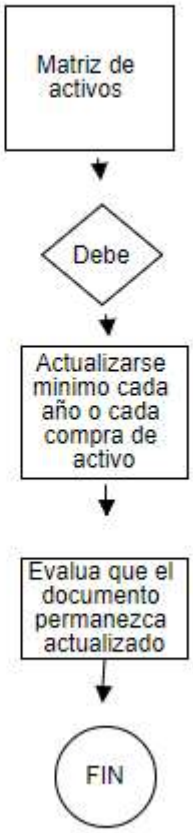
Evalúa que el documento permanezca actualizado	Directora de Auditoría TIC

Flujograma

Empresa

Director de seguridad de la información

Directora de auditoría TIC



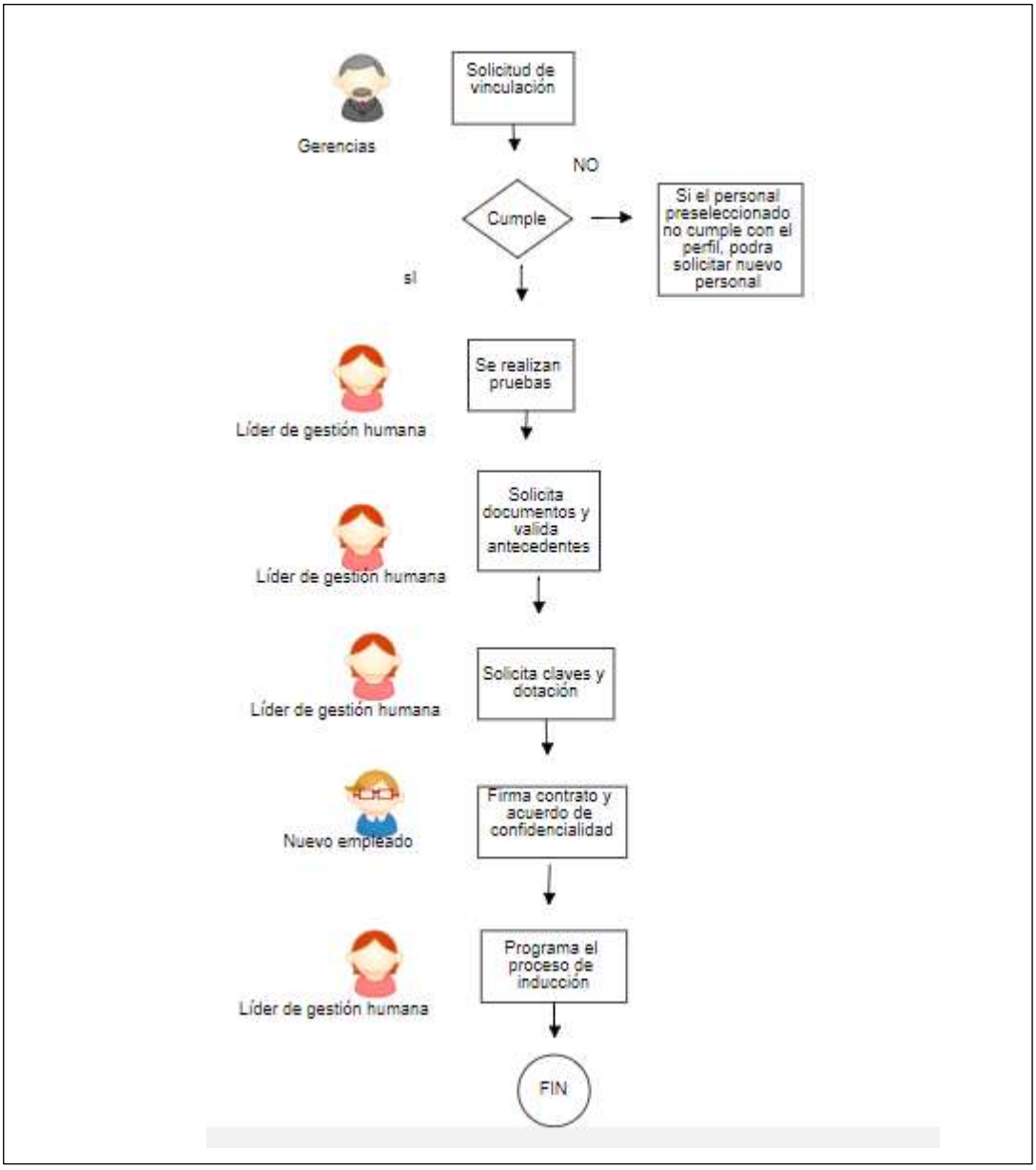
Fuente: El autor

Tabla 9: PROCEDIMIENTO DE GESTIÓN DE TALENTO HUMANO

	PROCESO: TIC	Código	GH - PRO-01
		Versión	1
	PROCEDIMIENTO	Fecha	17/10/2017
		Clasificación	Privado
		Página 1	

Nombre del procedimiento	GESTIÓN DE TALENTO HUMANO
Objetivo	Identificar, seleccionar y contratar a personas calificadas para desempeñar actividades dentro de la empresa
Alcance	Inicia con el requerimiento de personal y finaliza con la contratación del candidato seleccionado. Aplica para todas las contrataciones que se realizan
Responsables	Líder de gestión humana

Actividades	Líder de la actividad
Para iniciar el reclutamiento del personal debe existir una solicitud.	Gerencias
Si el personal preseleccionado no cumple con el perfil, podrá solicitar nuevo personal y dependiendo de la complejidad del cargo se realizarán las pruebas.	Gerencias
Para el proceso de contratación de nuevo personal es obligatorio que se anexe los documentos personales del seleccionado, de lo contrario No se podrá realizar la vinculación formal con la organización.	Líder de gestión humana
Verificar los antecedentes de los candidatos preseleccionados una vez hayan proporcionado los documentos personales.	Líder de gestión humana
Debe solicitar la asignación de claves y dotación requerida, una vez haya seleccionado el candidato idóneo para ocupar el puesto disponible dentro de la organización.	Líder de gestión humana
Firmar el contrato y el acuerdo de confidencialidad en documento original y copia.	Empleado nuevo
Programa el proceso de inducción en temas como seguridad de la información, en su área técnica especifica en donde se desempeñará, reglamento interno de trabajo y normativa de la organización.	Líder de gestión humana
Flujograma	



Fuente: El autor

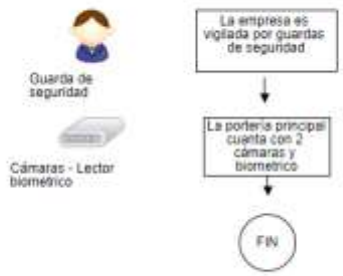
Tabla 10: PROCEDIMIENTO DE GESTIÓN DE SEGURIDAD FÍSICA

	PROCESO: TIC	Código	TIC- PRO- O4
		Versión	1
	PROCEDIMIENTO	Fecha	17/11/2017
		Clasificación	Privado
		Página 1	

Nombre del procedimiento	GESTIÓN DE SEGURIDAD FÍSICA
Objetivo	Definir y describir el estado actual de la seguridad locativa de las instalaciones de la compañía
Alcance	Aplica para la seguridad física de las instalaciones de la compañía
Responsables	Director de seguridad de la información

Actividades	Líder de la actividad
La empresa cuenta con un guarda de seguridad, donde el personal se anuncia, para que sea atendido por la recepcionista para minimizar los riesgos de pérdida o hurto de activos de seguridad de la información, para velar por que esta funcione correctamente cuenta con un contrato con la empresa OPV Security. Además, cuenta con un contrato de seguridad con la empresa ATLAS, la cual tiene una cobertura 7*24*365	Empresa de seguridad
Descripción de la zona de ingreso a las instalaciones. a) El ingreso a las instalaciones es realizado por la portería principal la cual se encuentra custodiada por 2 guardas, cámaras de seguridad y lector biométrico. Para minimizar el ingreso de personal no autorizado. b) Es importante aclarar que el acceso del personal a la organización se encuentra monitoreado por cámaras de seguridad que graban las 24 horas del día a intervalos de 15 minutos.	Empresa de seguridad

Flujograma



Fuente: El autor

Tabla 11: PROCEDIMIENTO DE COMPRAS

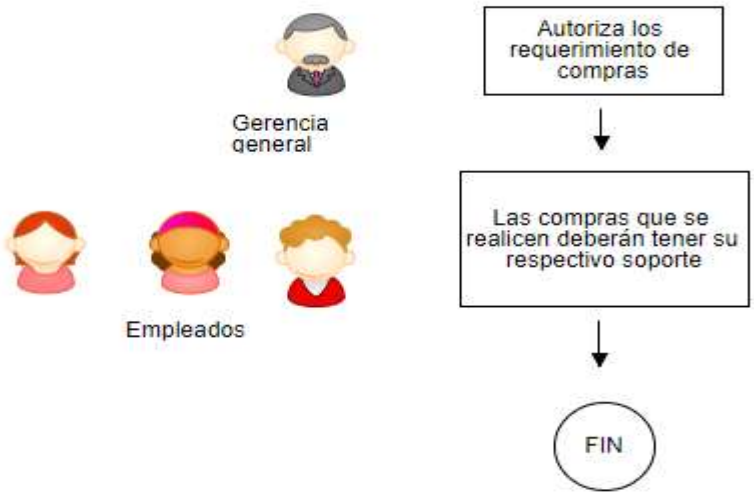
	PROCESO: TIC	Código	GH - PRO-02
		Versión	1
	PROCEDIMIENTO	Fecha	17/11/2017
		Clasificación	Privado
		Página 1	

Nombre del procedimiento	COMPRAS
Objetivo	Describir los pasos necesarios para llevar a cabo las compras dentro de la empresa.
Alcance	Inicia con el registro de la solicitud de compra por parte de un colaborador y finaliza con la entrega de la compra a satisfacción
Responsables	Directora administrativa y financiera Empleados

Actividades	Líder de la actividad
Las compras o requerimientos dentro de la organización como son: compra de activos, pagos requeridos dentro de un proyecto y las compras que afecten directamente la calidad o el servicio a brindar, sólo se podrán realizar con previa autorización	Gerencia General
Las compras que se realicen deberán tener su respectivo soporte (factura, cuenta de cobro o recibo) expedidos a nombre de nuestra organización. Si el soporte es una cuenta de cobro se deberá solicitar a la persona o entidad que presta el servicio los documentos necesarios para la legalización	Todos los empleados
Todo equipo computo que se vaya adquirir debe cumplir con las siguientes características mínimas: 1. Equipo portátil tamaño 14" 2. Sistema operativo Linux o Licencia Windows Profesional 3. Disco Duro mínimo 500GB 4. Memoria Ram 4G 5. Tarjeta de red Ethernet 10/100/1000 y tarjeta inalámbrica. 6. 1 Puerto HDMI 7. 3 puertos USB ideal mínimo 1 con	Todos los empleados

velocidad 3.0 8. Garantía mínimo 1 año 9. Ofimática Office Hogar y empresa	

Flujograma



. Fuente: El autor

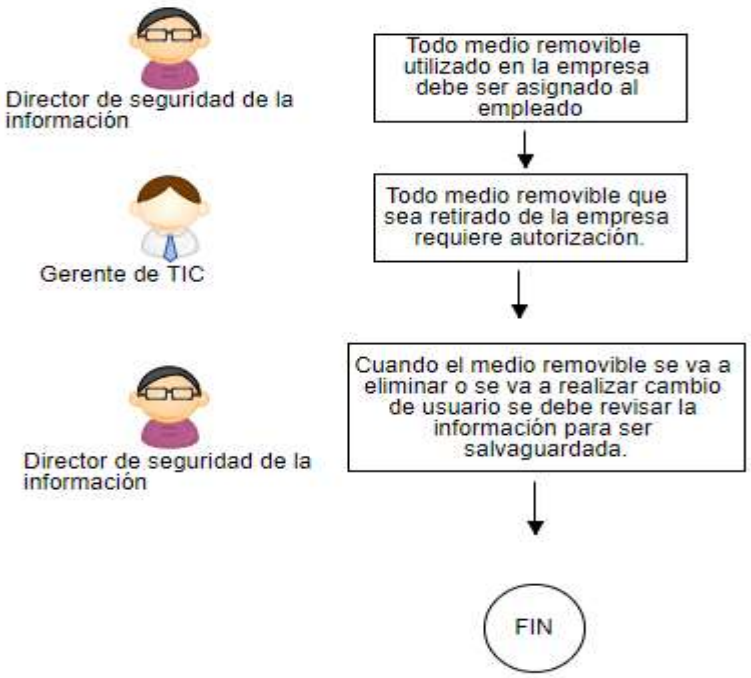
Tabla 12: PROCEDIMIENTO DE GESTIÓN DE MEDIOS REMOVIBLES

	PROCESO: TIC	Código	TIC- PRO- O5
		Versión	1
	PROCEDIMIENTO	Fecha	17/11/2017
		Clasificación	Privado
		Página 1	

Nombre del procedimiento	GESTIÓN DE MEDIOS REMOVIBLES
Objetivo	Definir procedimiento para la gestión de los medios removibles como cintas, discos, memorias USB, entre otros.
Alcance	Aplica para los subprocesos de Seguridad de la información y servicios tecnológicos y todos los empleados de la empresa.
Responsables	Director de seguridad de la información

Actividades	Líder de la actividad
Todo medio removible utilizado en la empresa debe ser asignado al empleado.	Director de seguridad de la información
Todo medio removible que sea retirado de la empresa requiere autorización. Nota: Todo medio que se retire y/o de la empresa debe ser reportado al guarda de seguridad quien realizará el registro de salida en la bitácora	Gerente de TIC
Cuando el medio removible se va a eliminar o se va a realizar cambio de usuario se debe revisar la información para ser salvaguardada.	Director de seguridad de la información

Flujograma



Fuente: El autor

Tabla 13: PROCEDIMIENTO DE GESTIÓN DE CONTROL DE ACCESO

	PROCESO: TIC	Código	TIC- PRO- O6
		Versión	1
	PROCEDIMIENTO	Fecha	17/11/2017
		Clasificación	Privado
		Página 1	

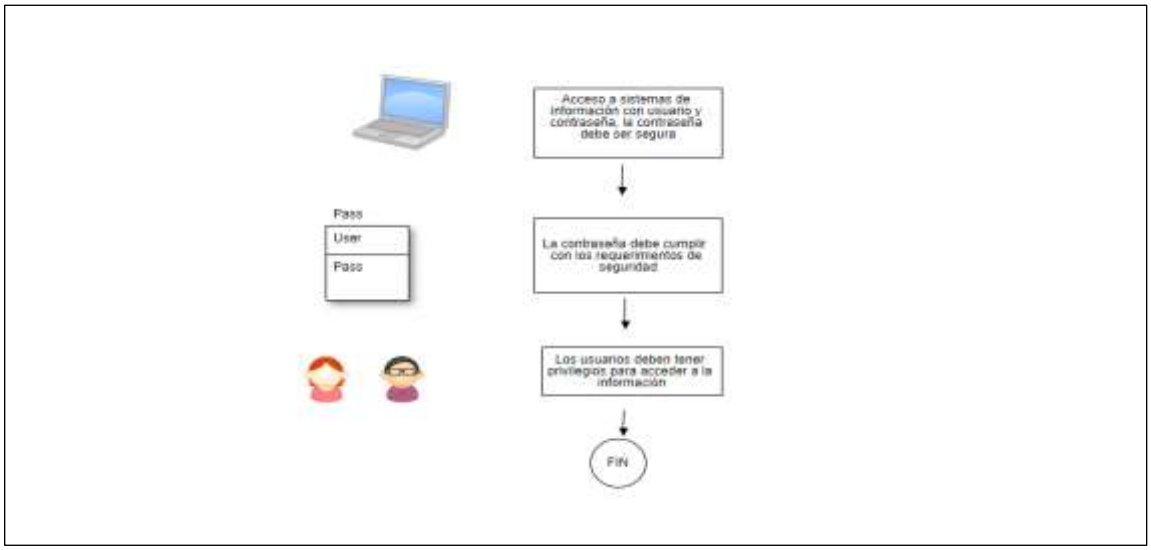
Nombre del procedimiento	GESTIÓN DE CONTROL DE ACCESO
Objetivo	Establecer medidas para el control de acceso a la información, aplicativos e instalaciones de la empresa.
Alcance	Aplica para todos los empleados y partes interesadas de la empresa.
Responsables	Director de seguridad de la información

Actividades	Líder de la actividad
CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN REGISTRO DE INICIO SEGURO El acceso a los aplicativos de la empresa se encuentra protegido con un inicio de sesión segura así: • No ingresa al aplicativo hasta que se haya valida el usuario y su contraseña. • Valida todas las entradas emitidas por el usuario, con el fin de minimizar el ingreso de personal no autorizado. • Después de dos inicios de sesión fallidos, el usuario se bloquea, el proceso de auditoría valida los intentos no exitosos. • Las contraseñas son cifradas	Director de seguridad de la información

GESTIÓN DE CONTRASEÑAS Las contraseñas son asignadas por el proceso de TIC y este recomienda a los usuarios: • No escribirlas en papel o almacenar en lugares visibles • No habilitar la opción “recordar clave en este equipo”. • No compartir las contraseñas • Utilice contraseña que no se asocien a usted, a sus gustos o familiares. • Cambia tus contraseñas regularmente. • No utilizar contraseña con variables (soporte1, soporte2, soporte3, qwertpoiuy, etc.).	Director de seguridad de la información
LIMITACIÓN DE TIEMPO DE CONEXIÓN La compañía no realiza bloqueos o restricciones a páginas Web.	Director de seguridad de la información
CONTROL DE ACCESO A LA INFORMACIÓN La empresa cuenta con un sistema de gestión de privilegios. El control de acceso a información física o digital, se realizará teniendo en cuenta los niveles. El acceso a la información compartida es por medio de carpetas. Solo la puede visualizar personal autorizado. El proceso de TIC, identifica la información y determina o la clasifica cuando la considera sensibles y les explica a los usuarios como deberían gestionarla desde ambientes tecnológicos aislados e independientes.	Director de seguridad de la información
COMPUTACIÓN Se entiende como dispositivos de cómputo todos aquellos que permitan tener acceso y almacenar información, desde lugares diferentes a las instalaciones. El uso de equipos de cómputo está restringido únicamente a los provistos por la organización y deberán contemplar las	Director de seguridad de la información

siguientes directrices: • Utilizar usuario y contraseña para el inicio de sesión. • Usar el antivirus provisto por el proceso de TIC. • No instalar software. • Uso de software licenciado y provisto por el proceso de TIC. • Realización de copias de seguridad periódicas. • Acatar los mecanismos de seguridad. • No dejar el equipo desatendido. • Guardar el equipo de cómputo en lugares adecuados. . • Mantener clasificada la información. • No active el bluetooth del computador.	

Flujograma



Fuente: El autor

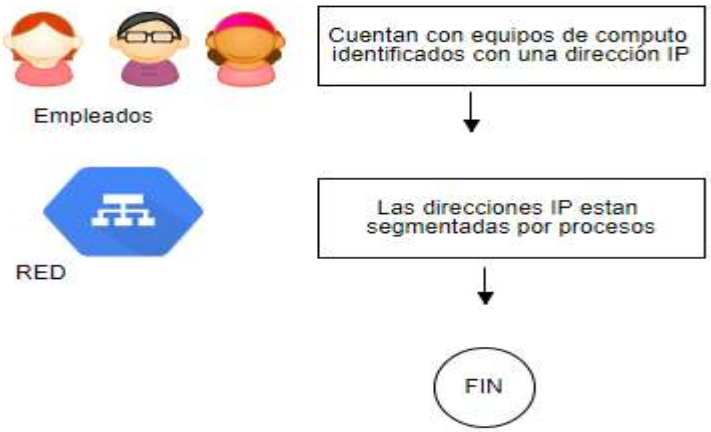
Tabla 14: PROCEDIMIENTO GESTIÓN DE SEGURIDAD EN LA RED

Estrategias Empresariales	**PROCESO: TIC**	Código	TIC- PRO-O7
		Versión	1
	PROCEDIMIENTO	Fecha	17/11/2017
		Clasificación	Privado
		Página 1	

Nombre del procedimiento	GESTIÓN DE SEGURIDAD EN LA RED
Objetivo	Realizar control de las redes de la empresa brindando la seguridad necesaria para proteger la información.
Alcance	Aplica para el tráfico de la red de la empresa.
Responsables	Jefe de infraestructura y comunicaciones

Actividades	Líder de la actividad
Realizar asignación de una dirección IP la cual identificará al trabajador y este solo tendrá acceso a las aplicaciones autorizadas, si no es parte de la empresa se conectará a un Access Point que solo tendrá acceso a Internet	Jefe de infraestructura y comunicaciones
Los equipos e IP están segmentadas por procesos, para realizar la configuración y permitir el acceso a navegación se debe registrar la MAC del equipo. Las redes de la empresa se encuentra separadas por VLANS para cada uno de los procesos de la empresa y se identifican de acuerdo con el mapa de proceso de la compañía, a cada una se le asigna un segmento de red.	Jefe de infraestructura y comunicaciones

Flujograma



Fuente: El autor

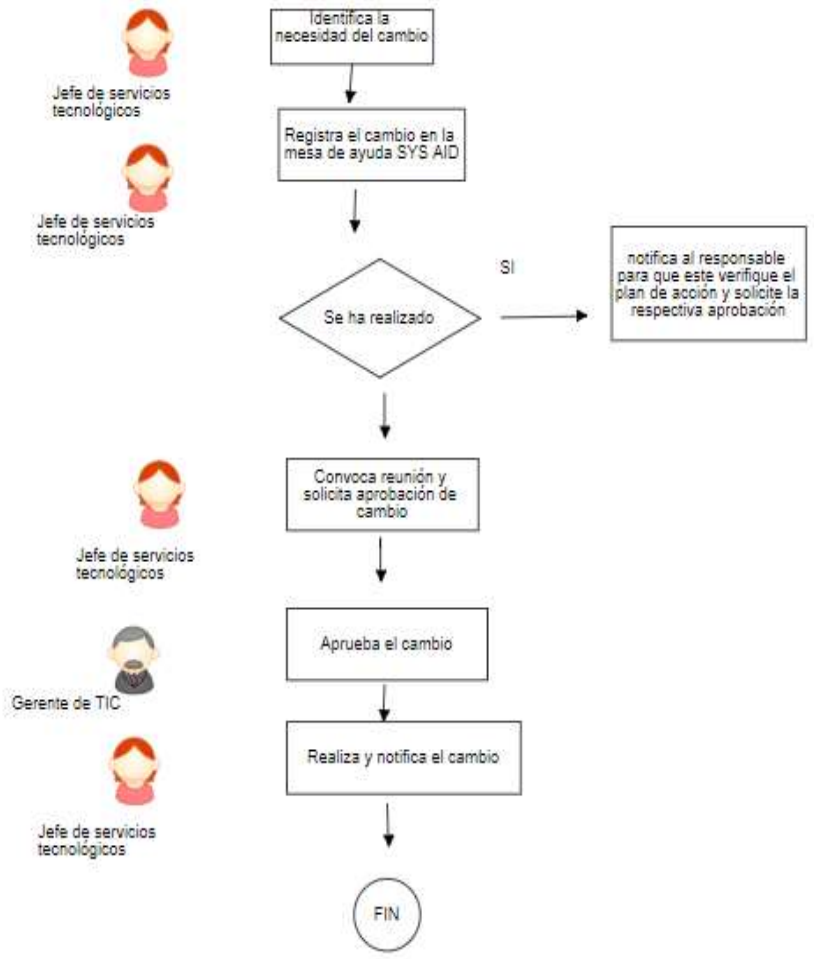
Tabla 15: PROCEDIMIENTO DE GESTIÓN DE CAMBIOS

	PROCESO: TIC	Código	TIC- PRO-O8
		Versión	1
	PROCEDIMIENTO	Fecha	17/11/2017
		Clasificación	Privado
		Página 1	

Nombre del procedimiento	GESTIÓN DE CAMBIOS	
Objetivo	Controlar el registro, clasificación, evaluación, aprobación e implementación de todos los cambios propuestos que afectan la prestación del servicio.	
Alcance	Este procedimiento cubre todos los cambios en la prestación del servicio desde la identificación de la necesidad del cambio ya sea por parte del cliente o interesados internos hasta la implementación satisfactoria del mismo.	
Responsables	Gerente de TIC	
Actividades		Líder de la actividad
Identifica la necesidad de cambio o valida documentación enviada por las partes interesadas sobre el cambio a implementar.		Jefe de servicios tecnológicos
Registrar por medio de SYSAID el cambio que se debe realizar, las personas involucradas, el tiempo de ejecución, los recursos requeridos.		Jefe de servicios tecnológicos
Si el cambio se ha implementado antes se debe notificar al responsable para que este verifique el plan de acción y solicite la respectiva aprobación Si no se ha realizado el cambio antes se debe convocar una reunión para llevar a cabo un comité de cambios, con todos los interesados que se pueden ver afectados por el plan de acción a implementar. Posteriormente se genera el plan de trabajo diligenciando el formato TIC-F-03 Plan de Trabajo y se realiza la propuesta de cambios el cual será adjunto vía ticket.		Jefe de servicios tecnológicos

Solicita aprobación para el cambio	Jefe de servicios tecnológicos / Gerente de TIC
registra el cambio por medio del formato TIC-F-04 Gestión de cambio y lo adjunta al ticket para poder crear base de conocimiento el cual se almacenará en la opción soluciones de la herramienta.	Jefe de servicios tecnológicos

Flujograma



Fuente: El autor

Tabla 16: PROCEDIMIENTO DE GESTIÓN DE GESTIÓN DE LA CAPACIDAD

	PROCESO: TIC	Código	TIC- PRO-O9
		Versión	1
	PROCEDIMIENTO	Fecha	17/11/2017
		Clasificación	Privado
		Página 1	

Nombre del procedimiento	GESTIÓN DE GESTIÓN DE LA CAPACIDAD
Objetivo	Medir la capacidad y el desempeño de la infraestructura que actualmente se encuentra en la empresa con el fin de garantizar el cumplimiento de las demandas de los recursos tecnológicos.
Alcance	En este documento se incluyen los pasos básicos descritos por la Biblioteca de Infraestructura de Tecnologías de Información ITIL[65] para realizar una correcta gestión de la capacidad.
Responsables	Gerente de TIC Director de TIC

Actividades	Líder de la actividad
Plan de Capacidad Análisis de Rendimiento Actual Se debe realizar un análisis del rendimiento actual de los componentes críticos y determinar la situación actual de dichos componentes. El análisis debe incluir la siguiente información: Recursos incluidos en el análisis Resumen de la capacidad de los recursos para satisfacer las demandas actuales; clasificando la información por categorías de recurso. Principales problemas en el rendimiento actual de los recursos Análisis de la Demanda del Negocio	Gerente de TIC Director de TIC

[65] WIKI. ITIL {En línea}. {10 mayo 2017}, disponible en internet https://wiki.es.it-processmaps.com/index.php/Portada

Se debe analizar la demanda que tiene la organización considerando: • Servicios de negocio incluidos en el análisis de rendimiento. • Tasas de utilización actual de los servicios de TI. • Para cada servicio identificar las necesidades de incremento en las cargas de trabajo, requerimientos de procesamiento y rendimiento. Lo anterior debe proyectarse en el corto, mediano y largo plazo. Identificación de las demandas futuras de capacidad Se deben identificar las demandas futuras de capacidad y monitoreo, así como los requerimientos para poder proveerlos, indicando como mínimo los siguientes elementos: • Servicios de TI proyectados • Para cada servicio de TI, indicar la proyección de capacidad y rendimiento. • Indicar la capacidad y rendimiento proyectado para los recursos que soportan el servicio de TI. • Requisitos técnicos, financieros y humanos para soportar la demanda requerida. Monitorización de los Recursos de la Infraestructura de TI Ejecutar Herramientas de Monitoreo Se debe monitorizar la capacidad y desempeño de los componentes que soportan los servicios, teniendo en cuenta los índices de capacidad y desempeño previamente identificados. Identificar Desviaciones y Afectación en los Niveles de Servicio Con base a los resultados del monitoreo, se deben identificar y documentar las variaciones a los niveles de rendimiento esperados. Se debe determinar si estas variaciones generan incidentes	

y el grado de afectación a los niveles de servicio acordados, de ser así, se deben generar las medidas correctivas respectivas y realizar un plan de mejora. Propuesta de Mejora Dicha propuesta de mejora debe considerar al menos los siguientes factores: • Servicio de negocio, servicio de TI y recursos relacionados • Descripción de la propuesta de mejora • Plazo de implementación • Costo asociado • Condiciones especiales (si aplica) Actualizar el plan de capacidad Se debe actualizar el plan de capacidad especificando los nuevos umbrales de rendimiento. Supervisión de la Capacidad Toda la información obtenida en las actividades anteriormente descritas se debe almacenar y registrar. A este registro se le conoce como Base de Datos de la Capacidad (CDB).	

Flujograma

Fuente: El autor

12. IMPLANTAR

12.1 DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad o SoA, es un documento en el cual se detallan los 114 controles de la Norma NTC ISO 27002:2013 y la actividad, documento y/o formato que realizó la empresa para aplicarlo y cumplir lo establecido. Además, se documentan las exclusiones o controles que no se van a implementar puesto que no son requeridas por la empresa, estas exclusiones deben tener una justificación. En el diseño la empresa aplicó 66 de 114 controles, esto equivale al 58%. De los 66 controles aplicados se establecieron 7 exclusiones las cuales se detallan a continuación:

Tabla 17: Exclusiones declaración de aplicabilidad

Sección	Objetivo de control/Control	Control Actual	Justificación de exclusión
A.6.1.5	Seguridad de la información en la gestión de proyectos	EXCLUSIÓN	La empresa no cuenta con un proceso de gestión de proyectos
A.6.2.1	Política para dispositivos móviles	EXCLUSIÓN	Los dispositivos móviles no se utilizan para la gestión de actividades laborales
A.6.2.2	Teletrabajo	EXCLUSIÓN	La empresa no tiene aprobado la opción para realizar teletrabajo
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	EXCLUSIÓN	Las aplicaciones de la empresa no corren por una red publica
A.14.2.1	Política de desarrollo seguro	EXCLUSIÓN	La empresa no cuenta con un proceso de desarrollo
A.14.2.5	Principios de construcción de los sistemas seguros	EXCLUSIÓN	La empresa no cuenta con un proceso de desarrollo
A.14.2.6	Ambiente de desarrollo seguro	EXCLUSIÓN	La empresa no cuenta con un proceso de desarrollo

Fuente: El autor

La empresa continuará con la implementación del sistema de gestión de seguridad de la información (SGSI), con el fin de subir los niveles de madurez y documentar el 42% de controles restantes. La declaración de aplicabilidad o SoA establecido por la empresa se relaciona en el Anexo G:

13. ANALISIS DE LOS RESULTADOS

De acuerdo con el análisis GAP inicialmente realizado se estableció el estado actual de la empresa en materia de seguridad de la información, al presentar un índice de madurez inicial, se logró evidenciar que la empresa tiene un nivel muy bajo en cuanto a la implementación de controles y políticas que le permitan prestar un servicio integral a sus empresas cliente. De esto se concluyó que no existía una planeación estratégica que fuera estructurada por una guía o siguiendo un lineamiento normativo que direccionara adecuadamente el trabajo desarrollado. Este fue el insumo para el desarrollo de cada una de las etapas del trabajo.

Al indagar sobre las partes interesadas, se obtuvo que el impacto e influencia que tienen los socios y clientes representan el 90% para los intereses de la empresa, por lo que las estrategias que sean definidas deben girar en torno al cumplimiento de los requisitos de estos y en generar valor para afianzar confianza en la empresa.

De acuerdo con las necesidades de la empresa y sus partes interesas se estableció el alcance del sistema de seguridad de la información a desarrollar, obteniendo como resultado que, como el componente tecnológico es fundamental para la prestación de los servicios que ofrece la empresa y tiene una influencia directa sobre el desarrollo de las actividades en cada uno de los procesos que la conforman, el proceso TIC resulta crítico y por lo tanto objeto del alcance del proyecto.

Estas actividades dieron claridad a la gerencia para el establecimiento de la política del sistema, la cual se diseñó en función de los objetivos estratégicos de la empresa y de cómo se pretende generar compromiso al interior y reflejar confiabilidad hacia el exterior.

La gestión de riesgos e identificación de activos arrojo como resultado que, de 14 activos identificados, los activos SIIGO producción y SIIGO contingencia resultan críticos para las actividades de la empresa, sobre estos se validaron los controles implementados encontrando los activos críticos no contaban con controles, por lo que se hizo necesario instruir a los líderes de proceso en el diseño, valoración y monitoreo de controles específicos que permitan fortalecer las debilidades encontradas.

Como resultado del análisis de esos riesgos, se definieron cinco controles:

a. Realizar aseguramiento y backup de la configuración de la base de datos, servidores y aplicativos.

b. Establecer monitoreos a la base datos, servidores con el fin de controlar y monitorear, para que esta tenga los umbrales o niveles de consumos de recursos adecuados.

c. Configurar Backup automáticos full e incremental a la información almacenada en la base de datos.

d. Realizar contrato con un tercero especializado para el almacenamiento externo de la copia de seguridad.

e. Establecer cronogramas para las pruebas de restauración de las copias de seguridad de la información.

De estos, cuatro son responsabilidad del proceso de TIC (a, b, c y e) y uno a cargo de la Líder de gestión humana (d), con ellos a parte de mitigar los riesgos y cubrir los controles necesarios, se logra cumplir el 100% de la información documentada propuesta para este proyecto, la cual la exige la norma, esta es la base principal para la implementación del sistema de gestión de seguridad de la información.

Por último, se documentó la declaración de aplicabilidad, la cual mostro que de los 114 controles que se encuentran referenciados en la norma, la empresa queda con un total de 66 en cumplimiento, lo que representa un 58%. Sin embargo, y con el desarrollo de este proyecto, los documentos entregados y las capacitaciones realizadas, se dejan las bases para que la empresa cumpla con el 100% y deje instaurado su sistema de seguridad de la información.

16. CONCLUSIONES

El diagnóstico del estado de madurez de la empresa permitió consolidar la situación real frente a lo requerido por la normatividad, esto fue la base que soportó el desarrollo del proyecto y el compromiso de la gerencia para culminar el 100% de los controles y mantener un sistema de gestión de seguridad de la información.

Se logró el diseño de la estructura del sistema de seguridad de la información, identificando las responsabilidades, objetivos y alcance, que fueron aprobados por la gerencia de la empresa y que se incluirá en la planeación estratégica del proceso de TIC.

La metodología de identificación de activos y gestión de riesgos planteada, fue apropiada por los responsables del proceso TIC, de manera que con el apoyo que se brido por parte del proyecto, se establecieron los controles a implementar, se reforzaron los que ya se tenían en el proceso y se direccionó de forma planificada la gestión sobre los activos de información.

Lo anterior, permitió estructurar, de acuerdo con la metodología y actividades descritas a lo largo del presente documento, el sistema de seguridad de la información para Estrategias Empresariales de Colombia S.A.S, que cumple con lo establecido por la norma NTC ISO 27001:2013, y en el cual se consolidan los criterios necesarios que debe seguir la empresa como ruta estratégica para la prestación de sus servicios, generar valor agregado a sus clientes y expandirse en el mercado.

Para los riesgos identificados con la metodología ISO 27005:2008, (ver literal 10.1) se establecieron los controles para los que su nivel de calificación fue muy alto, con los líderes de proceso, de manera que cada uno se apropió de la metodología, para darle continuidad a su gestión y mejoramiento continuo.

Al realizar la identificación de las partes interesadas, la empresa estableció prioridades en el servicio, direccionando la planificación estratégica de sus actividades en función de esas partes, priorizándolas y teniendo en cuenta su grado de influencia y requerimientos para el logro de los objetivos propuestos al interior del proceso tecnológico.

Diseñar el análisis de riesgos, alcance, política, objetivos, información documentada y la declaración de aplicabilidad de acuerdo con lo establecido en la Norma NTC ISO 27001:2013, ayudan a realizar las actividades de forma controlada, para que

así los empleados velen por que los activos mantengan su confidencialidad, disponibilidad e integridad. Este diseño es la base fundamental para que empresa la empresa cuide la información y continúe la implementación y certificación.

La información documentada elaborada entrega las bases para el desarrollo de las actividades de forma controlada y secuencial, definiendo los responsables y los soportes que se debe generar en cada paso, esta se elaboró de acuerdo con los debes de la Norma NTC ISO 27001:2013.

La declaración de aplicabilidad cubre los 114 controles de la Norma NTC ISO 27002:2013 para proteger la empresa, activos, partes interesadas. Esta se basa en un enfoque holístico y cubriéndola de extremo a extremo. Logrando que todos los procesos realicen sus actividades de forma controlada.

El sistema de gestión de seguridad de la información le traerá beneficios a la empresa, desde la planificación estratégica, hasta la ejecución de las actividades de manera controlada y direccionando el trabajo bajo un estándar reconocido que le asegura la confidencialidad, integridad y disponibilidad de la información.

17.BIBLIOGRAFÍA

- ICONTEC, Instituto Colombiano de Normas Técnicas. Nueve claves para el éxito – una visión general de la implementación de la norma NTC-ISO/IEC 27001. 2016. P127

- ICONTEC, Instituto Colombiano de Normas Técnicas. Compendio de seguridad de la información, segunda edición. 2015. P260

- ICONTEC, Instituto Colombiano de Normas Técnicas. Gestión del riesgo en la seguridad de la información. 2015. P68

- ICONTEC, Instituto Colombiano de Normas Técnicas Guía para la implementación de un sistema de gestión de seguridad de la información. 2014. P81

- ICONTEC, Instituto Colombiano de Normas Técnicas. Gestión del riesgo principios y directrices. 2011.P29

- ISO, International Organization for Standardization Information technology -- Security techniques. Information security management systems Overview and vocabulary. 2016. P37

- PMG-SSI. Ciclo Deming. {En línea}. {10 mayo 2017}, disponible en internet: <http://www.pmg-ssi.com/2015/06/iso-27001-ciclo-de-deming/>

- STANDARDS.ISO. Glosarios ISO 27000:2014. {En línea}. {10 mayo 2017}, disponible en internet: http://standards.iso.org/ittf/PubliclyAvailableStandards/c063411_ISO_IEC_27000_2014.zip>

- ISO27000. Controles Anexo A NTC- NORMA ISO 27001:2013. {En línea}. {10 mayo 2017}, disponible en internet: <http://www.iso27000.es/download/ControlesISO27002-2013.pdf>

- WELIVESECURITY. Metodología Magerit. {En línea}. {10 mayo 2017}, disponible en internet: <https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/>

- ADMINISTRACIÓN ELECTRONICA. Mapa de calor Magerit. {En línea}. {10 mayo 2017}, disponible en internet :

<https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WQ5UBmc2zIU>

- ISO27000. Gestión de medios removibles. {En línea}. {10 mayo 2017}, disponible en internet: <http://www.iso27000.es/iso27002_8.html>

- ISO27002.WIKI. ZOHO. Política de seguridad de la información. {En línea}. {10 mayo 2017}, disponible en internet: <https://iso27002.wiki.zoho.com/5-1-Pol%C3%ADtica-de-seguridad-de-la-informaci%C3%B3n.html>

- PMG-SSI. Clasificación de activos de seguridad de la información. {En línea}. {10 mayo 2017}, disponible en internet: <http://www.pmg-ssi.com/2015/05/como-clasificar-los-activos-de-seguridad-en-un-sgsi/>

- PMG-SSI. Gestión de acceso. En línea}. {10 mayo 2017}, disponible en internet: <http://www.pmg-ssi.com/2016/08/iso-27001-como-controlar-el-control-de-acceso/>

- IDU. Declaración de aplicabilidad. {En línea}. {10 mayo 2017}, disponible en internet: <https://www.idu.gov.co/documents/20181/251887/FO-TI-27+Formato+Declaracion+de+Aplicabilidad++V_1.0+-+Diligenciado+Dic2015.pdf/1138b1b6-6f0c-41cf-85b1-7383c5f15f54>

- SIGEA. Análisis GAP. {En línea}. {10 mayo 2017}, disponible en internet: http://www.sigea.es/assessment27001.pdf

- MINTIC. Controles de seguridad de la información. {En línea}. {10 mayo 2017}, disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

- INTEDYA. Gestión de puertos USB. {En línea}. {10 mayo 2017}, disponible en internet: <http://www.intedya.com/internacional/54/consultoria-gestion-de-la-seguridad-de-la-informacion-isoiec-27001.html>

- SIC. Protección de datos personales. {En línea}. {10 mayo 2017}, disponible en internet: <http://www.sic.gov.co/proteccion-de-datos-personales>

- SIC. Protección de datos personales – Decreto 1377 de 2013. {En línea}. {10 mayo 2017}, disponible en internet: http://www.sic.gov.co/sites/default/files/normatividad/DECRETO%2B1377%2BDEL%2B27%2BDE%2BJUNIO%2BDE%2B2013.pdf

- SIC. Protección de datos personales – Guía de responsabilidad demostrada. {En línea}. {10 Mayo 2017}, disponible en internet:

<http://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada>

- ISO27002.WIKI. ZOHO. Gestión de incidentes de seguridad de la información. {En línea}. {10 mayo 2017}, disponible en internet: <https://iso27002.wiki.zoho.com/13Incidentes.html>

- DELTAASESORES. Ley 1273 de 2009. {En línea}. {10 mayo 2017}, disponible en internet: <http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia>

- ISO27000.Sistema de gestión de seguridad de la información. {En línea}. {10 mayo 2017}, disponible en internet: http://www.iso27000.es/download/doc_sgsi_all.pdf

- GESTION-CALIDAD. Información documentada. {En línea}. {10 mayo 2017}, disponible en internet: <http://gestion-calidad.com/informacion-documentada-iso-27001-2013>

- ISOTOOLS. Tratamiento de riesgos. {En línea}. {10 mayo 2017}, disponible en internet: <http://www.isotools.com.co/iso-27001-evaluacion-tratamiento-riesgos-6-pasos/>

- SEGURIDADPARATODOS. Seguridad informática o seguridad de la información. {En línea}. {10 mayo 2017}, disponible en internet: <http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html>

- INCIBE. Contingencia TIC vs continuidad de negocio. {En línea}. {10 mayo 2017}, disponible en internet: <https://www.incibe.es/protege-tu-empresa/blog/contingencia-vs-continuidad>

- INCIBE. Mini SGSI. {En línea}. {10 mayo 2017}, disponible en internet: <https://www.incibe.es/protege-tu-empresa/blog/minisgsi>

- ADVISERA. Anexo A. {En línea}. {10 mayo 2017}, disponible en internet: <https://advisera.com/27001academy/es/knowledgebase/resumen-del-anexo-a-de-la-norma-iso-270012013/>

- ALCALDIABOGOTA. Ley 603. {En línea}. {10 mayo 2017}, disponible en internet: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960>

- AGPD. Ley de protección de datos personales España {En línea}. {10 mayo 2017}, disponible en internet: <

http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/index-ides-idphp.php>

- DAVISVISION. HIPAA {En línea}. {10 mayo 2017}, disponible en internet: < http://www.davisvision.com/Que-es-la-HIPAA/>
- MSAFFIRIO. NIVEL DE MADUREZ {En línea}. {10 mayo 2017}, disponible en internet https://msaffirio.wordpress.com/2008/06/21/escala-de-madurez-%E2%80%93-process-maturity-model/
- WIKI. ITIL {En línea}. {10 mayo 2017}, disponible en internet https://wiki.es.it-processmaps.com/index.php/Portada

ANEXOS

ANEXO A: 114 controles del Anexo A

Ítem	Controles del anexo A	RE	SI	NO	NA	PA		Objetivos/control
Ítem	Controles	RE	SI	NO	NA	PA	Meta Control	Cumplimiento Control
A.5..	**Política de Seguridad de la Información**	2	0	1	0	1	**100%**	**25%**
A.5.1.	Gestión de la Dirección para la Seguridad de la Información	2	0	1	0	1	100%	25%
A.5.1.1	Políticas de Seguridad de la Información	PA				✔		
A.5.1.2	Revisión de las políticas de seguridad de la Información	NO		✔				
A.6..	**Organización de la Seguridad de la Información**	7	1	6	0	0	100%	14%
A.6.1.	**Organización Interna**	5	0	5	0	0	100%	0%
A.6.1.1	Roles y responsabilidades en Seguridad de la Información	NO		✔				
A.6.1.2	Separación de deberes	NO		✔				
A.6.1.3	Contacto con las autoridades	NO		✔				
A.6.1.4	Contacto con grupos de interés especial	NO		✔				

Ítem	Controles del anexo A	RE	SI	NO	NA	PA		Objetivos/control
A.6.1.5	Seguridad de la información en proyectos	NO		✔				
A.6.2.	**Dispositivos móviles y teletrabajo**	2	1	1	0	0	100%	**50%**
A.6.2.1	Política de Dispositivo Móvil	NO		✔				
A.6.2.2	Teletrabajo	SI	✔					
A.7..	**Seguridad en los Recursos Humanos**	5	5	1	0	0	100%	83%
A.7.1.	**Antes de asumir el empleo**	2	2	0	0	0	100%	100%
A.7.1.1	Selección	SI	✔					
A.7.1.2	Términos y condiciones de empleo	SI	✔					
A.7.2.	**Durante la ejecución del empleo**		2	1	0	0	100%	**67%**

Ítem	Controles del anexo A	RE	SI	NO	NA	PA		Objetivos/control
A.7.2.1	Responsabilidades de la dirección	NO		✔				
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	SI	✔					
A.7.2.3	Proceso disciplinario	SI	✔					
A.7.3.	**Terminación y cambio de empleo**	1	1	0	0	0	100%	100%
A.7.3.1	Terminación o cambio de responsabilidades de empleo	SI	✔					
A.8..	**Gestión de los activos**	10	0	6	0	4	**100%**	20%
A.8.1.	**Responsabilidad por los activos**	4	0	1	0	3	100%	38%
A.8.1.1	Inventario de Activos	PA				✔		
A.8.1.2	Propiedad de los activos	PA				✔		
A.8.1.3	Uso aceptable de los activos	PA				✔		
A.8.1.4	Devolución de activos	NO		✔				
A.8.2.	**Clasificación de la Información**	3	0	3	0	0	100%	0%
A.8.2.1	Clasificación de la información	NO		✔				
A.8.2.2	Etiquetado y manejo de la información	NO		✔				
A.8.2.3	Manejo de activos	NO		✔				
A.8.3.	**Manejo de los Medios**	3	0	2	0	1	100%	17%

Ítem	Controles del anexo A	RE	SI	NO	NA	PA		Objetivos/control
A.8.3.1	Gestión de los medios removibles	PA				✔		
A.8.3.2	Disposición de los medios	NO		✔				
A.8.3.3	Transferencia de los medios físicos	NO		✔				
A.9..	**Control de Acceso**	13	5	8	0	0	100%	36%
A.9.1.	**Requisitos del Negocio para el Control de Acceso**	2	0	2	0	0	100%	0%
A.9.1.1	Política de control del acceso	NO		✔				
A.9.1.2	Acceso a redes y a servicios en red	NO		✔				
A.9.2.	**Gestión de Acceso de Usuarios**	6	3	3	0	0	100%	**50%**
A.9.2.1	Registro de usuarios y cancelación del registro de usuarios	NO		✔				
A.9.2.2	Suministro de acceso de usuarios	SI	✔					
A.9.2.3	Gestión de derechos de acceso privilegiado	SI	✔					
A.9.2.4	Gestión de información de autenticación secreta de usuarios	NO		✔				
A.9.2.5	Revisión de los derechos de acceso de usuarios	NO		✔				
A.9.2.6	Retiro o ajuste de los derechos de acceso	SI	✔					
A.9.3.	**Responsabilidades de los usuarios**	1	1	0	0	0	100%	100%
A.9.3.1	Uso de información de autenticación secreta	SI	✔					
A.9.4.	**Control de acceso a sistemas y aplicaciones**	4	1	3	0	0	100%	25%

Ítem	Controles del anexo A	RE	SI	NO	NA	PA		Objetivos/control
A.9.4.1	Restricción de acceso a la información	SI	✔					
A.9.4.2	Procedimiento de ingreso seguro	NO		✔				
A.9.4.3	Sistema de gestión de contraseñas	NO		✔				
A.9.4.4	Uso de programas utilitarios privilegiados	NO		✔				
A.10..	**Criptografía**	2	0	0	0	2	100%	**50%**
A.10.1.	**Controles Criptográficos**	2	0	0	0	2	100%	**50%**
A.10.1.1	Política sobre uso de controles criptográficos	PA				✔		
A.10.1.2	Gestión de llaves	PA				✔		
A.11..	**Seguridad Física y del Entorno**	15	0	8	2	5	100%	30%
A.11.1.	**Áreas Seguras**	6	0	2	1	3	100%	**42%**
A.11.1.1	Perímetro de seguridad física	PA				✔		
A.11.1.2	Controles de acceso físicos	PA				✔		
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	NO		✔				
A.11.1.4	Protección contra amenazas externas y ambientales	PA				✔		
A.11.1.5	Trabajo en áreas seguras	NO		✔				
A.11.1.6	Áreas de despacho y carga	NA			✔			
A.11.2.	**Equipos**	9	0	6	1	2	100%	22%
A.11.2.1	Ubicación y protección de los equipos	PA				✔		
A.11.2.2	Servicios de suministro	NA			✔			

Ítem	Controles del anexo A	RE	SI	NO	NA	PA		Objetivos/control
A.11.2.3	Seguridad del cableado	PA				✔		
A.11.2.4	Mantenimiento de equipos	NO		✔				
A.11.2.5	Retiro de activos	NO		✔				
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	NO		✔				
A.11.2.7	Disposición segura o reutilización de equipos	NO		✔				
A.11.2.8	Equipos de usuarios desatendido	NO		✔				
A.11.2.9	Política de escritorio limpio y pantalla limpia	NO		✔				
A.12..	**Seguridad de las Operaciones**	11	1	2	2	6	100%	**43%**
A.12.1.	**Procedimientos Operacionales y Responsabilidades**	4	1	0	2	1	100%	88%
A.12.1.1	Procedimientos de operación documentados	NA			✔			
A.12.1.2	Gestión de cambios	PA				✔		
A.12.1.3	Gestión de capacidad	NA			✔			
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	SI	✔					
A.12.2.	**Protección contra códigos maliciosos**	1	0	0	0	1	100%	**50%**
A.12.2.1	Controles contra códigos maliciosos	PA				✔		
A.12.3.	**Copias de respaldo**	1	0	0	0	1	100%	**50%**
A.12.3.1	Respaldo de la información	PA				✔		
A.12.4.	**Requisitos y seguimiento**	1	0	1	0	0	100%	0%
A.12.4.4	Sincronización de relojes	NO		✔				
A.12.5.	**Control de software operacional**	1	0	1	0	0	100%	0%

Ítem	Controles del anexo A	RE	SI	NO	NA	PA		Objetivos/control
A.12.5.1	Instalación de software en sistemas operativos	NO		✔				
A.12.6.	**Gestión de la Vulnerabilidad Técnica**	2	0	0	0	2	100%	**50%**
A.12.6.1	Control de las vulnerabilidades técnicas	PA				✔		
A.12.6.2	Restricciones sobre la instalación de software	PA				✔		
A.12.7.	**Consideraciones de la Auditoría de los sistemas de Información**	1	0	0	0	1	100%	**50%**
A.12.7.1	Controles de auditorías de sistemas de información	PA				✔		
A.13..	**Seguridad de las Comunicaciones**	**1**	0	1	0	0	100%	0%
A.13.1.	**Gestión de la Seguridad de las Redes**	0	0	**0**	**0**	**0**	100%	0%
A.13.2.	**Transferencia de Información**	**1**	0	**1**	**0**	**0**	100%	0%
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	NO		✔				
A.14..	**Adquisición, Desarrollo y Mantenimiento de Sistemas**	13	5	2	1	5	100%	**65%**
A.14.1.	**Requisitos de seguridad de los Sistemas de Información**	3	**0**	**0**	**0**	**3**	100%	**50%**
A.14.1.1	Análisis y especificación de los requisitos de seguridad de la información	PA				✔		
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	PA				✔		
A.14.1.3	Protección de transacciones de los Servicios de las aplicaciones	PA				✔		
A.14.2.	**Seguridad en los Proceso de Desarrollo y Soporte**	9	**5**	**1**	**1**	**2**	100%	78%
A.14.2.1	Política de desarrollo seguro	SI	✔					

Ítem	Controles del anexo A	RE	SI	NO	NA	PA		Objetivos/control
A.14.2.2	Procedimiento de control de cambios en sistemas	SI	✔					
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	NO		✔				
A.14.2.4	Restricciones en los cambios a los paquetes de software	SI	✔					
A.14.2.5	Principios de construcción de los sistemas seguros	PA				✔		
A.14.2.6	Ambiente de desarrollo seguro	PA				✔		
A.14.2.7	Desarrollo contratado externamente	NA			✔			
A.14.2.8	Pruebas de seguridad de sistemas	SI	✔					
A.14.2.9	Prueba de aceptación de sistemas	SI	✔					
A.14.3.	**Datos de Prueba**	1	**0**	**1**	**0**	**0**	100%	0%
A.14.3.1	Protección de Datos de Prueba	NO		✔				
A.15..	**Relaciones con los Proveedores**	5	0	4	0	1	100%	10%
A.15.1.	**Seguridad de la información en las relaciones con los proveedores**	3	**0**	**3**	**0**	**0**	100%	0%
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	NO		✔				
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	NO		✔				
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	NO		✔				
A.15.2.	**Gestión de la prestación de servicios de Proveedores**	2	**0**	**1**	**0**	**1**	100%	25%

Ítem	Controles del anexo A	RE	SI	NO	NA	PA		Objetivos/control
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	PA				✔		
A.15.2.2	Gestión de cambios en los servicios de los proveedores	NO		✔				
A.16..	**Gestión de incidentes de Seguridad de la Información**	7	3	4	0	0	100%	**43%**
A.16.1.	**Gestión de Incidentes y Mejoras en la seguridad de la Información**	7	**3**	**4**	**0**	**0**	100%	**43%**
A.16.1.1	Responsabilidades y procedimientos	NO		✔				
A.16.1.2	Reporte de eventos de seguridad de la información	NO		✔				
A.16.1.3	Reporte de debilidades de seguridad de la información	NO		✔				
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	SI	✔					
A.16.1.5	Respuesta a incidentes de seguridad de la información	SI	✔					
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	SI	✔					
A.16.1.7	Recolección de evidencia	NO		✔				
A.17..	**Aspectos de seguridad de la información de la Gestión de Continuidad de Negocio**	4	1	3	0	0	100%	25%
A.17.1.	**Continuidad de seguridad de la información**	3	**0**	**3**	**0**	**0**	100%	0%
A.17.1.1	Planificación de la continuidad de la seguridad de la información	NO		✔				

Ítem	Controles del anexo A	RE	SI	NO	NA	PA		Objetivos/control
A.17.1.2	Implementación de la continuidad de la seguridad de la información	NO		✔				
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	NO		✔				
A.17.2.	**Redundancias**	1	**1**	**0**	**0**	**0**	100%	100%
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	SI	✔					
A.18..	**Cumplimiento**	8	0	6	2	0	100%	25%
A.18.1.	**Cumplimiento de los requisitos legales y contractuales**	5	**0**	**3**	**2**	**0**	100%	40%
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	NO		✔				
A.18.1.2	Derechos de propiedad intelectual (DPI)	NA			✔			
A.18.1.3	Protección de registros	NA			✔			
A.18.1.4	Privacidad y protección de información de datos personales	NO		✔				
A.18.1.5	Reglamentación de los controles criptográficos	NO		✔				
A.18.2.	**Revisiones de seguridad de la información**	3	**0**	**3**	**0**	**0**	100%	0%
A.18.2.1	Revisión independiente de la seguridad de la información	NO		✔				
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	NO		✔				
A.18.2.3	Revisión del cumplimiento técnico	NO		✔				
	TOTAL	**114**	**21**	**52**	**7**	**24**	100%	36%

ANEXO B: Responsabilidades en el sistema de gestión de seguridad de la información

CARGO/ROL	RESPONSABILIDADES
Gerencias de la empresa	Dedicar tiempo (trimestral) y designar recursos para que los activos de la empresa se mantengan protegidos
	Mantener un inventario de los activos de información importantes
	Asegurarse de que se llevan a cabo todas las acciones correctivas
	Verificar si las acciones correctivas han eliminado la causa de no conformidades
	Realizar actividades continúas relacionadas con la sensibilización
Participante comité de Seguridad de la Información	Elaborar y actualizar la documentación del sistema de gestión de seguridad de la información.
	Velar por que se realicen los análisis de riesgos, planes de contingencia y prevención de desastres en pro de velar por la seguridad de la información.
	Realizar análisis de los incidentes de seguridad de la información reportados.
	Tomar decisiones disciplinarias en los eventos que se encuentre involucrado un empleado y que hayan afectado o violado una de las políticas de seguridad de la información.
	Proponer acciones disciplinarias contra los empleados que realizaron la violación de la seguridad.
	Proponer los objetivos de seguridad de la información.
	Proponer mejoras en la seguridad y las acciones correctivas.
	Proponer el presupuesto y otros recursos necesarios para la protección de la información.
	Definir las cláusulas de seguridad que deben ser parte de un acuerdo.
	Realizar revisión posterior al incidente de los planes de recuperación.
Gerente de TIC	Velar que los empleados cumplan las políticas, procedimientos y normas de seguridad.
	Suministrar apoyo técnico en los asuntos que afecte o violen la seguridad, por ejemplo: (infección de virus, explotación de vulnerabilidades, hackers, entre otros.
	Documentar los incidentes y eventos de seguridad evidenciados y comunicar a las áreas implicadas con fin de que se establezcan las acciones correctivas y preventivas.

CARGO/ROL	RESPONSABILIDADES
	Deshacerse de los medios y equipos fuera de uso, de una forma segura
	Definir qué tipo de canales de comunicación son aceptables y que no son
	Proponer modelo para la autenticación, contraseñas seguras y métodos criptográficos, etc.
	Establecer controles con el fin de que los empleados naveguen de forma segura en internet.
Coordinador de Seguridad	Dirigir las investigaciones que den a lugar los incidentes de fraude o hurto de información y seguridad de la información, realizar apoyo para la definición de acciones correctivas y preventivas.
	Permanecer en contacto permanente con las autoridades y grupos de interés especial
Asistente de contratación	Verificar los antecedentes disciplinarios de los nuevos empleados.
Jefe de servicios	Recibir los requerimientos para la creación de usuarios en los diferentes aplicativos de la empresa
	Supervisar que los empleados utilicen de forma adecuada los recursos tecnológicos
	Controlar el software de la empresa
	Garantizar los mantenimientos preventivos a los servidores y a los equipos del área administrativa según definición en los cronogramas establecidos por el área de TIC
	Informar a su jefe inmediato las actividades sospechosa o eventos de seguridad de la información
	Coordinar pruebas
	Revisar los registros de actividades de los usuarios con el fin de reconocer comportamientos sospechosos
Jefe de comunicaciones	Autorizar los accesos de los equipos a las aplicaciones necesarias por cada empleado previamente definidos por cada gerente de área
	Monitorear el uso de los recursos de red
	Revisar el log de accesos
	Garantizar los mantenimientos preventivos a la red de la empresa según definición en los cronogramas establecidos por el área de TIC para la red de comunicaciones de la empresa.
	Informar a su jefe inmediato las actividades sospechosa o eventos de seguridad de la información
	Preparar equipos de comunicación que se utilizarán en caso de una emergencia / desastre

CARGO/ROL	RESPONSABILIDADES
Asistente de Soporte	Controlar los activos de hardware de la empresa, los equipos deben estar codificados para su identificación y control. Debe mantener una matriz con el inventario actualizado.
	Asignar o retirar hardware a los empleados previamente solicitados por cada gerente de área
	Supervisar los cuidados físicos de los recursos informáticos
	Garantizar los mantenimientos preventivos a los equipos de los puntos de contacto según definición en los cronogramas establecidos por el área de TIC
	Informar a su jefe inmediato las actividades sospechosa o eventos de seguridad de la información
Director Financiero	Garantizar la seguridad en las instalaciones físicas, en los controles de acceso que garanticen que personas internas o externas no vulneren la seguridad locativa de la empresa
Director de Gestión Humana	Garantizar que los empleados cuenten con acuerdos de confidencialidad debidamente establecidos en la organización de acuerdo al marco normativo vigente, a la formación y concientización del personal en el cumplimiento de las políticas de seguridad establecidas por la empresa
	Realizar de cursos de iniciación sobre temas de seguridad para los nuevos empleados
Junta directiva y Gerencia General	Facilitar que el comité de seguridad cumpla con sus funciones para garantizar la seguridad de la información, de proveer y autorizar los recursos humanos y económicos que sean necesarios para asegurar las vulnerabilidades que puedan ser encontradas y debidamente justificadas por el comité como acciones de mejora al sistema
Empleados	Cumplir con las políticas de seguridad de la información definidas por la empresa.
	No divulgar información privilegiada de la empresa
	No podrá mantener sobre el escritorio información en papeles o en medios de almacenamiento que correspondan a la empresa
	No intentar tener acceso a aplicaciones que no tenga autorización para ingresar
	No vulnerar la seguridad física, locativa o de red de la empresa
	No realizar suplantación de identidad de usuarios ingresando con usuarios y claves que no le correspondan

CARGO/ROL	RESPONSABILIDADES
	No realizar acceso a oficinas que no se encuentren con personal del área correspondiente
	No entregar sus accesos a personal no autorizado
	No utilizar los activos y/o recursos informáticos para actividades diferentes a las contratadas
	Cuidar su contraseña y no compartirla con terceros
	Utilizar contraseña robusta de mínimo 10 caracteres alfa numérica que no tenga relación con el usuario, prohibir su reutilización.
	Reportar los incidentes de seguridad identificados.
Auditores Internos del SGSI	Participar activamente en los ciclos de auditorías internas del S.G.S.I planificadas.
	Contribuir para que las políticas de seguridad de la información definidas por la empresa sean cumplidas
Asistente Jurídico	Preparar pruebas para una acción legal después de un incidente
Director de seguridad	Difundir el alcance, política y objetivos del Sistema de Gestión de Seguridad de la Información a todo el personal de la empresa.
	Editar, distribuir y controlar la documentación del sistema de gestión de seguridad de la información
	Asegurar la revisión sistemática de la documentación de todo el sistema de gestión de seguridad de la información
	Asegurar la transmisión de información sobre acciones correctivas, preventivas y su aplicación
	Informar a la Gerencia los resultados de auditorías internas, externas, acciones correctivas y de mejora
	Preparar los cuestionarios de auditorías
	Definir y analizar los registros del sistema de gestión, las responsabilidades y periodos de conservación
	Coordinar los procesos de socialización y capacitación del Sistema de Gestión de Seguridad de la Información
	Elaborar y actualizar las políticas, normas, pautas y procedimientos relacionados a seguridad de la información y telecomunicaciones

CARGO/ROL	RESPONSABILIDADES
	Documentar los incidentes y eventos de seguridad evidenciados y comunicar a las áreas implicadas para que establezcan las acciones correctivas
	Elaborar la lista de partes interesadas relacionados con la seguridad de la información.
	Elaborar la lista de requisitos de las partes interesadas
	Ser responsable de revisar y actualizar los documentos principales
	Enseñar a los empleados la forma de realizar la identificación y valoración de riesgos
	Coordinar el proceso de valoración de riesgos
	Preparar el plan de formación y sensibilización para la seguridad de la información
	Comunicar los beneficios de la seguridad de la información
	Informe sobre los resultados de medir
	Informe requisitos importantes de las partes interesadas
	Notificar a la alta dirección sobre los principales riesgos
	Asesorar a los altos ejecutivos en todas las cuestiones de seguridad
	Realizar la evaluación de riesgos para las actividades a ser subcontratados
	Realizar verificación de antecedentes de los candidatos a socios de outsourcing
	Recibir información sobre los incidentes de seguridad
	Coordinar la respuesta a incidentes de seguridad
	Analizar los incidentes con el fin de prevenir su repetición
	Coordinar el proceso de análisis de impacto en el negocio y la creación de planes de respuesta
	Realizar actividades continuas relacionadas con la sensibilización

ANEXO C: Política de seguridad de la información

	POLITICA: TIC	Código	TIC- PO-O1
		Versión	1
	POLITICA DE SEGURIDAD DE LA INFORMACIÓN	Fecha	17/10/2017
		Clasificación	Privado
		Página 1	

Nombre del procedimiento	POLITICA DE SEGURIDAD DE LA INFORMACIÓN
Objetivo	Determinar los lineamientos para proteger la información de la empresa, basándose en los requisitos legales, tecnológicos y normativos, con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información
Alcance	Aplica a toda la empresa, empleados, contratistas, aprendices, que tenga acceso a la información sensible de la empresa.
Responsables	Gerente de TIC
Política	
La dirección de Estrategias Empresariales de Colombia S.A.S., reconoce la importancia de salvaguardar la información y se compromete en la implementación y mantenimiento de un sistema de gestión de seguridad de la información (SGSI), para asegurar la confidencialidad, integridad y disponibilidad de la información generada por el desarrollo de su objeto social o incluye aquella que sea enviada, adquirida o cedida. La empresa protege su información creada, procesada, transmitida o resguardada por sus procesos de operación, con el fin de minimizar impactos financieros, operativos o legales debido a un uso inadecuado de esta. La empresa protege su información de las amenazas originadas por parte de sus empleados, contratistas y aprendices. La empresa implementa control de acceso a la información, aplicativos, recursos de red, portales y sistemas de información internos y externos o con accesos remotos. La empresa garantiza una adecuada gestión de los eventos de seguridad. La empresa garantiza la continuidad de las operaciones La empresa garantiza el cumplimiento de las obligaciones legales, regulatorias contractuales.	

Responsabilidades proceso TIC
Establecer, mantener y divulgar las políticas y procedimientos de servicios de tecnología, incluida esta política de seguridad de información. Mantener la seguridad de la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos. Informar a la Dirección los eventos de seguridad de la información. Aplicar y hacer cumplir la Política de Seguridad de la Información. Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo de acuerdo con las directrices emitidas de parte de la Dirección.
Responsabilidades de los propietarios de la información
Clasificar la información que está bajo su administración y/o generación. Determinar los tiempos de retención de la información. Determinar y evaluar de forma permanente los riesgos asociados a la información, así como los controles implementados para el acceso.
Responsabilidades de empleados, contratistas, aprendices
Utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas. Proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido. Evitar la divulgación no autorizada o el uso indebido de la información. Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración. Usar software autorizado que haya sido adquirido legalmente por la empresa. Aplicar y cumplir con la presente Política.

ANEXO D: Metodología gestión de riesgos:

Objetivo

Definir la metodología para la evaluación y tratamiento de los riesgos de la información en la empresa, de acuerdo con la norma ISO/IEC 27001:2013.

Alcance

La metodología a implementar va desde la identificación de los activos relevantes para el funcionamiento del negocio, hasta la asociación de riesgos y su tratamiento.

Responsabilidad

La aplicación de la metodología depende de la participación de diferentes roles los cuales se relacionan a continuación:

Identificación de activos relevantes para el SGSI	Gerentes y Líderes de proceso	Mínimo una vez al año.
Valorar los activos	Gerentes y Líderes de proceso	Mínimo una vez al año.
Identificación de riesgos	Toda la compañía	Permanente
Identificación de vulnerabilidades	Director de seguridad	Mínimo una vez al año.
Identificación de amenazas	Director de seguridad	Mínimo una vez al año.
Valoración y clasificación del riesgo	Director de seguridad	Mínimo una vez al año.
Selección de controles	Director de seguridad	Mínimo una vez al año.
Aprobar plan de tratamiento	Gerencia	Mínimo una vez al año.
Revisiones a la gestión del riesgo	Auditoría interna	De acuerdo con planeación

Contenido

La metodología cuenta con un enfoque sistemático para la gestión de riesgos de los activos de información identificados y poder diseñar, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) de la empresa.

1. Etapas de la gestión de riesgos

La metodología de gestión de riesgo pasa por las siguientes actividades:

a. Análisis de riesgos:

Entrevistas al personal de la organización para obtener información. Los objetivos de esta etapa son:

1. Identificar y evaluar los activos de información.
2. Identificar el conjunto de amenazas y su relación con las vulnerabilidades detectadas sobre los activos.
3. Cuantificar el impacto de la materialización de amenazas.

b. Selección de controles:

Realizada el análisis y calificación de riesgos, se realizan citas con los líderes del proceso para identificar los controles y calificar el riesgo después de la validación de la efectividad del control.

2. Análisis de riesgos

Un activo de información es todo aquello que tiene valor en términos de confidencialidad, integridad y disponibilidad para la empresa y por tanto debe ser valorado para identificar su importancia y riesgos.

La clasificación de los activos de información está determinada por su tipo y clase:

Tipo de activo	Clase de activo
Activos de Información Puros	Información Digital
	Información Física
	Activos de Información intangibles

Tipo de activo	Clase de activo
	Bases de datos
Activos de Tecnologías de Información	Servicios de información
	Software
	Hardware de TI
	Controles ambientales
Activos de Información Recurso Humano	Empleados
	No Empleado

3. **Cálculo del Valor del Activo de Información.**

El paso a seguir después de la identificación de los activos de información en cada proceso es definir que variables deben considerarse en el cálculo del valor del activo de información.

El valor del activo está determinado por la suma de las siguientes variables:

- Confidencialidad
- Integridad
- Disponibilidad
- Valor económico

Para la valoración de los activos se utiliza una escala de 1 a 5[66] sobre cada una de las variables mencionadas anteriormente.

4. **Valor Económico del Activo (VE):**

Valor del Activo*:* Está determinado por el valor de la confidencialidad, integridad, disponibilidad y el valor económico.

Valoración	Rango	
1	**Muy Bajo**	**[$1 - $ 2.000.000]**

66 Siendo 1 el valor más bajo y 5 el valor más alto en el activo evaluado.

Valoración	Rango	
2	**Bajo**	**($ 2.000.000 - $ 4.000.000]**
3	**Medio**	**($4.000.000 - $ 6.000.000]**
4	**Alto**	**($6.000.000 - $ 8.000.000]**
5	**Muy Alto**	**(8.000.000 - >8.000.000]**

5. **Confidencialidad (C):**

Valoración	Rango	Descripción
1	**Muy Bajo**	La información puede ser utilizada por cualquier usuario.
2	**Bajo**	La información puede ser utilizada por personal de la empresa y proveedores
3	**Medio**	La información puede ser utilizada por jefes
4	**Alto**	Solo es posible el acceso la información puede ser utilizada por directores y gerentes
5	**Muy Alto**	Solo es posible es acceso por los Gerentes y junta directiva

6. **Integridad (I):**

Valoración	Rango	Descripción
1	**Muy Bajo**	La información puede ser modificado siempre y por cualquier usuario

2	**Bajo**	La información puede ser modificada por cualquier empleado de la compañía
3	**Medio**	La información puede ser modificada por jefes
4	**Alto**	La información puede ser modificada con autorización de directores y gerentes
5	**Muy Alto**	La información puede ser modificada con de la junta directiva o Gerencia

7. Disponibilidad (D):

Valoración	Rango	Descripción
1	**Muy Bajo**	Si el activo no puede ser utilizado por una semana no se afecta la empresa
2	**Bajo**	Si el activo no puede ser utilizado por tres días no se afecta la empresa
3	**Medio**	Si el activo no puede ser utilizado por un día no se afecta la empresa
4	**Alto**	Si el activo no puede ser utilizado por cuatro horas no se afecta la empresa
5	**Muy Alto**	El activo debe estar disponible siempre

8. Valor del activo (VA)

El valor del activo de información está dado por:

Valor Activo = Confidencialidad + Integridad + Disponibilidad + Valor Económico del activo

Nota: de acuerdo con la distribución, el máximo y mínimo de las valoraciones estimadas se establecerán los rangos para aplicar la clasificación de los activos según esta variable.

Clasificación	Rangos del valor del activo
Muy Alto	(15-20]
Alto	(13-15]
Medio	(11-13]
Bajo	(7-11]
Muy bajo	[4-7]

9. Identificar las Amenazas de los Activos de Información

Las amenazas pueden ser de origen natural o humano y en caso de materializarse pueden afectar uno o todos los activos.

La siguiente tabla presenta las amenazas identificadas:

Amenazas		
Acceso no autorizado	Derramar líquidos sobre el equipo	Goteras o fugas de agua
Acceso no autorizado al código	Destrucción de los repositorios de datos	Negligencia del personal
Ataque por denegación de servicio	Ente regulador de propiedad intelectual	Negligencia o errores de proveedores
Auditorías externas	Errores de sincronización en cambios	Personal autorizado
Aumento de las llamadas inesperado	Errores de usuario / Factores ambientales	Personal no autorizado
Aumento del tráfico	Errores de usuarios	Robo
Ausencia de personal	Errores o negligencia de usuarios	Tormenta eléctrica
Cambio sin registrar	Exceso de temperatura	Vandalismo
Daño de equipo o medio origen de almacenamiento	Falla en el proveedor de internet	Virus informático

10. Identificar las Vulnerabilidades en los Activos de Información

Las vulnerabilidades de los activos son la probabilidad de que una amenaza se materialice. Para identificar las amenazas se debe realizar una encuesta con los empleados y validar la posibilidad de que las amenazas se materialicen.

11. Clasificar los Riesgos según las Vulnerabilidades y Amenazas

Los riesgos identificados y relacionados a las vulnerabilidades y amenazas de los activos de información están clasificados así:

Tipo Riesgo
Lógico
Físico

Tipo Riesgo
Locativo
Legal
Personal
Organizacional
Baja por mantenimiento

12. Identificación de vulnerabilidades

a. Lógicas

Son aquellos que vulneran la integridad de los activos de información de la empresa, el software, las bases de datos, los accesos a la información, que pueden ser causados por códigos maliciosos, cualquier tipo de manipulación o error humano que altere o elimine datos. A continuación, se hace mención de algunas vulnerabilidades posibles.

Contraseñas

Vulnerabilidad	Amenaza	Riesgo
No se conocen políticas para el manejo de contraseña	**Que sean cifradas por terceros**	**Ingreso al sistema o correo y hurten la información importante de la empresa.**
Mala configuración de los servicios en red		
Vulnerabilidad	**Amenaza**	**Riesgo**
Mala configuración del sistema por parte del administrador	**Puede ser utilizada para cualquier tipo de ataque**	**Se dificulta la prestación del servicio**
Validación de entrada		
Vulnerabilidad	**Amenaza**	**Riesgo**
La entrada que procesa un sistema no es comprobada	**Defectos de programación**	**Desbordamiento de buffer**
Error en la gestión de recursos		
Vulnerabilidad	**Amenaza**	**Riesgo**
Error en la gestión de recursos	**Consumo excesivo en los recursos del sistema**	**El sistema deja de responder provocando denegaciones del servicio**
Virus		
Vulnerabilidad	**Amenaza**	**Riesgo**

No tener un antivirus actualizado	**El equipo puede ser afectado**	**Perder información**
Correos no deseados		
Vulnerabilidad	**Amenaza**	**Riesgo**
No se tiene control de los mensajes que ingresan al correo	**Correos spam**	**Ser víctima de algún tipo de fraude por internet o virus**
Fuga de información		
Vulnerabilidad	**Amenaza**	**Riesgo**
Mala configuración del administrador de aplicación web dejando público el registro de errores	**El atacante puede ver las fallas exactas del sistema**	**Obtener el control parcial o total del sitio.**
Mala contratación de personal		
Vulnerabilidad	**Amenaza**	**Riesgo**
No conocer el debido manejo de los computadores	**Una mala gestión de procedimiento en el software**	**Perdida de información**
Ubicaciones de servidores		
Vulnerabilidad	**Amenaza**	**Riesgo**
Mala ubicación de servidores	**Alteración física por ubicación locativa**	**Perdida de información de la empresa**
Incumplimiento de las normas de instalación de la red		
Vulnerabilidad	**Amenaza**	**Riesgo**
Inadecuada instalación del cableado físico de las redes de datos	**Falla de diseño**	**Problemas de transmisión de datos, operatividad o indisponibilidad de los recursos de red.**
Sistema de alimentación ininterrumpida		
Vulnerabilidad	**Amenaza**	**Riesgo**
No se tienen Ups para un respaldo de energía	**Falta de energía**	**Perdida de información**

Fuente:

http://www.inteco.es/Formacion/Amenazas/Vulnerabilidades/

b. Físicas

Son aquellas que afectan la vida útil de los equipos que pueden ser causados por robo, falta de cuidados por parte del personal, o cualquier tipo de accidente causal de este daño.

Ingerir alimentos		
Vulnerabilidad	**Amenaza**	**Riesgo**
Tomar bebidas cerca del equipo	**Derramar el líquido sobre el equipo**	**Daño total o parcial del equipo**
Áreas de paso		
Vulnerabilidad	**Amenaza**	**Riesgo**
El equipo está un área de paso	**Error humano**	**Daño del equipo**
Alarmas de seguridad		
Vulnerabilidad	**Amenaza**	**Riesgo**
Control de alarmas	**Personas no autorizadas o ingresos forzosos**	**Robo de los equipos**
Determinar un almacenaje		
Vulnerabilidad	**Amenaza**	**Riesgo**
Tener un lugar específico para almacenar CD o memorias con información importante de la empresa	**Pérdida o abandono de los dispositivos**	**Perder información**
Conocer el entorno en el cual está ubicada la empresa		
Vulnerabilidad	**Amenaza**	**Riesgo**
No tener presente las estadísticas de robos de la ciudad	**No saber implementar niveles de seguridad adecuados**	**Robo de los equipos**
Concientización del personal para mantener la limpieza en su puesto de trabajo		
Vulnerabilidad	**Amenaza**	**Riesgo**
Política que obligue al empleado a mantener limpio y ordenado su puesto de trabajo	**Polvo y líquidos cercanos a los equipos y dispositivos**	**Perdida de hardware**
Establecer mantenimientos periódicos		
Vulnerabilidad	**Amenaza**	**Riesgo**
No tener un control periódico en el mantenimiento	**Fallas en el equipo**	**Pérdida total del equipo**
Los equipos críticos se encuentran almacenados en cuartos cerrados con acceso restringido y/o a personal autorizado.		
Vulnerabilidad	**Amenaza**	**Riesgo**

No tener un control en la entrada de cuarto de servidores, routers.	**Modificación de los datos**	**Pérdida de información**
Los equipos críticos se encuentran almacenados en cuartos cerrados con acceso restringido y/o a personal autorizado.		
Vulnerabilidad	**Amenaza**	**Riesgo**
No tener un control en la entrada de cuarto de servidores, routers.	**Robo de los equipos**	**Pérdida de los equipos**

Fuente:

auditoriasistemasucb.pbworks.com/f/MI+EXPO+SEGURIDAD+FISICA.ppt
http://www.fasor.com.sv/whitepapers/whitepapers/Monitoreo/Como_monitorear_amenazas_fisicas_en_centro_de_datos.pdf

http://www.inteco.es/Formacion/PYMES/Seguridad_fisica/Comunicaciones_y_Accesos/

c. Locativas

Son aquellas que hacen un entorno inadecuado para la seguridad e integridad de los equipos o documentos importantes de la compañía.

Equipamiento

Vulnerabilidad	Amenaza	Riesgo
Escritorios o mesas inestables	**Caída o daño de los equipos**	**Daño al equipo**

c. Legales

Son aquellos que afectan al no tener en cuenta las cláusulas y acuerdos estipulados en contratos.

No tener evidencias

Vulnerabilidad	Amenaza	Riesgo
No tener evidencias de los acuerdos firmados	**Inconformidad del cliente**	**Obtener una demanda**
Derechos de autor		
Vulnerabilidad	**Amenaza**	**Riesgo**
No registrar las creaciones de la empresa	**La copia de una página que revele información específica de un cliente**	**Problemas legales**
Datos		
Vulnerabilidad	**Amenaza**	**Riesgo**

No tener control en el acceso de la información de los clientes	**Inadecuado manejo de los datos e información de los clientes**	**Demanda por divulgación no permitida por el cliente**
Dominio		
Vulnerabilidad	**Amenaza**	**Riesgo**
Guardar contraseñas en el computador	**Que un tercero utilice la contraseña**	**Robo de dominio**
Impuestos		
Vulnerabilidad	**Amenaza**	**Riesgo**
Incumplimiento de normas o falta de pagos oportunos de impuestos	**Revisión del ente competente**	**Sanción o riesgo de cierre**

Fuente:
http://www.inteco.es/Formacion/Legislacion/Propiedad_Intelectual/

d. Naturales

Vulnerabilidad	**Amenaza**	**Riesgo**
No tener medidas de contingencia de catástrofes	**Catástrofe natural**	**Ausencia de personal y Perdida de equipos**
Vulnerabilidad	**Amenaza**	**Riesgo**
No tener número de extintores necesarios	**Incendio**	**Perdidas físicas**
Vulnerabilidad	**Amenaza**	**Riesgo**
El edificio es una construcción sismo resistente	**Terremoto o temblor**	**Ausencia del personal y perdida locación**

Fuente:
http://www.construmatica.com/construpedia/Construcciones_Sismoresistentes_en_la_Construcci%C3%B3n_para_el_Desarrollo

Determinar el impacto en los Activos de Información

El impacto está calificado por el responsable del activo de información, quien tiene mayor claridad de cuánto daño generaría la materialización de las amenazas sobre las vulnerabilidades en la empresa.

Nivel de Impacto (IMP):

Valoración	Clasificación	Intervalo
1	Muy Bajo	[$ 1 - $ 2.000.000]
2	Bajo	($ 2.000.000 - $ 4.000.000]
3	Medio	(4.000.000 - $ 6.000.000]
4	Alto	(6.000.000 - $ 8.000.000]
5	Muy Alto	($8.000.000 - >$8.000.000]

Determinar la probabilidad de Ocurrencia (P (a, v))

- **La probabilidad:** se calcula de acuerdo con la experiencia y el conocimiento de los gerentes de las áreas de proceso, se estableció en una escala de 1 a 5 la probabilidad de los riesgos identificados:

Calificación	
5	Muy Alto
4	Alto
3	Medio
2	Bajo
1	Muy Bajo

Determinar Valor de Riesgo (VR)

El marco de referencia utilizado en la evaluación del riesgo para los activos es la Norma NTC- ISO 27005:2008[67].

Para la valoración y evaluación de los riesgos se tendrán en cuenta las siguientes variables definidas anteriormente:

- **Valor del activo (VA)**.
- **Probabilidad P(a,v).**
- **Valor Impacto** (**IMP).**[68]

Se usa la siguiente formula:

[67] ICONTEC "estándar Internacional ISO/IEC 27005:2008 Information Technology – Security techniques – Specification for an Information Security Managment System"

[68] ICONTEC "estándar Internacional ISO/IEC 27005:2008 Information Technology – Security techniques – Specification for an Information Security Managment System"

$$VR = P(a,v) * IMP * VA \ (2)$$

El cálculo total del valor del riesgo asociado a un activo es determinado por la **ecuación (2)**.

Gestión de riesgos

A partir de las estimaciones del valor del riesgo realizadas se establece un análisis de distribución de frecuencias para clasificar los riesgos.

Clasificación Riesgo	Rango	
Muy Alto	301	500
Alto	201	300
Medio	121	200
Bajo	61	120
Muy Bajo	4	60

Tratamiento de los riesgos

Los riesgos que se trataran son los que su calificación este en **rangos críticos** son *Alto* y *Muy Alto*:

Alto (201 - 300) – Muy Alto (301 - 500)

Estos rangos fueron escogidos por considerarse que su materialización afecta la continuidad de las operaciones de la empresa. Las acciones establecidas para el tratamiento de los riesgos son:

- Transferir a empresas aseguradoras, terceros siempre y cuando el control no sea mayor al costo de la materialización del evento, al implementar el control el riesgo residual debe estar en los niveles de aceptación de la compañía tras su implementación.
- Mitigar: la empresa establece controles para que el riesgo se establezca o mantengan en niveles aceptables para la empresa.

- Aceptar: El riesgo es aceptado por la empresa cuando su control es mayor al costo de la materialización del evento.

Criterios para la aceptación de riesgos

Los riesgos que su calificación está en la lista que se relaciona a continuación se consideran que su impacto y probabilidad de ocurrencia no afecta la seguridad de la información de la empresa:

Muy Bajo (4-60) – Bajo (61-120) – Medio (121-200)

.

Selección de controles

Los controles que se establezcan a los riesgos deben garantizar que su riesgo residual se encuentre en los rangos aceptables, en este se documentarán en el *Plan de tratamiento de riesgos SGSI (formato TIC-F-01_Matriz de riesgos)*

Revisiones periódicas de la evaluación y el tratamiento de riesgos

Los riesgos deben evaluarse una vez al año o cada que la empresa tenga cambios en los procesos, su tecnología.

Informes de gestión de riesgos

Cada vez que se realice una revisión de la gestión de riesgos deberá presentarse un informe de la situación encontrada, y las acciones de tratamiento requeridas para los riesgos identificados cómo críticos.

ANEXO E: Matriz de riesgos de SGSI

	MATRIZ DE RIESGOS SGSI					CÓDIGO	TIC - F - 01							
						VERSIÓN	1.0							
						FECHA	11/10/2017							
Código	Activo	Área/Proceso	Responsable	Tipo de Activo	Clase Activo_Inf	Etiquetado	Vr Económico del Activo	Integridad	Confidencialidad	Disponibilidad	Vr. Del Activo	Clasificación del VA	Impacto	Clasificación del Impacto
1	SERVIDOR OCS INVENTORY	TIC	Jefe de infraestructura y comunicaciones	Activos de infraestructura	Hardware de TI	PRIV	5	2	3	3	13	Medio	3	Medio
2	SERVIDOR LINUX OPENFIRE	TIC	Jefe de infraestructura y comunicaciones	Activos de infraestructura	Hardware de TI	PRIV	5	2	3	3	13	Medio	3	Medio
3	SERVIDOR AUDITORIA	TIC	Jefe de infraestructura y comunicaciones	Activos de infraestructura	Hardware de TI	PRIV	5	2	3	3	13	Medio	3	Medio
4	SERVIDOR BINAPS	TIC	Jefe de infraestructura y comunicaciones	Activos de infraestructura	Hardware de TI	PRIV	5	2	3	3	13	Medio	3	Medio
5	SERVIDOR SYSAID - MESA DE AYUDA	TIC	Jefe de infraestructura y comunicaciones	Activos de infraestructura	Hardware de TI	PRIV	5	2	3	3	13	Medio	3	Medio

		MATRIZ DE RIESGOS SGSI				CÓDIGO					TIC - F - 01			
						VERSIÓN					1.0			
						FECHA					11/10/2017			
6	SERVIDOR ELASTIX	TIC	Jefe de infraestructura y comunicaciones	Activos de infraestructura	Hardware de TI	PRIV	5	2	3	3	13	Medio	3	Medio
7	SERVIDOR VMWARE 1	TIC	Jefe de infraestructura y comunicaciones	Activos de infraestructura	Hardware de TI	PRIV	5	2	3	3	13	Medio	3	Medio
8	SEVIDOR DIRECTORIO ACTIVO	TIC	Jefe de infraestructura y comunicaciones	Activos de infraestructura	Hardware de TI	PRIV	5	2	3	3	13	Medio	3	Medio
9	Equipo jefe de infraestructura y comunicaciones	TIC	Jefe de infraestructura y comunicaciones	Activos de infraestructura	Hardware de TI	PRIV	2	2	3	3	10	Bajo	3	Medio
10	Equipo jefe de desarrollo	TIC	Jefe de desarrollo	Activos de Tecnologías de Información	Hardware de TI	PRIV	2	2	3	3	10	Bajo	3	Medio
11	Equipo Director de seguridad	TIC	Director de seguridad	Activos de Tecnologías de Información	Hardware de TI	PRIV	2	2	3	3	10	Bajo	3	Medio
12	Equipo jefe ERP	TIC	Jefe de ERP	Activos de Tecnologías de Información	Hardware de TI	PRIV	2	2	3	3	10	Bajo	3	Medio
13	SERVIDOR SIIGO PRODUCCION	TIC	DBA	Activos de Información Puros	Servicios de Información	PRIV	5	5	5	5	20	Muy alto	5	Muy alto
14	SERVIDOR SIIGO CONTINGENCIA	TIC	DBA	Activos de Información Puros	Activo de información Intangible	PRIV	5	5	5	5	20	Muy alto	5	Muy alto

ANEXO F: Plan de tratamiento

De acuerdo con la calificación de los activos en la fase anterior, se evidenció que los activos críticos son SERVIDOR SIIGO PRODUCCION, SERVIDOR SIIGO CONTINGENCIA, por lo cual se establecieron los controles que se relacionan en este anexo.

CODIGO	CONTROL	ACTIVIDADES	REFERENCIA ANEXO A ISO 27001:2013	RESPONSABLE	PRIORIDAD	FECHA DE IMPLEMENTACIÓN
CTRL01	Realizar aseguramiento y backup de la configuración de la base de datos, servidores y aplicativos	Implementar políticas en el directorio activo	A.9.1	Coordinador de comunicaciones	ALTA	30/12/2017
CTRL02	Establecer monitoreos a la base datos, servidores con el fin de controlar y monitorear, para que esta tenga los umbrales o niveles de consumos de recursos adecuados.	Implementar software de detección, para establecer monitoreo 7X24X365	A.12.2.1	Coordinador de comunicaciones	ALTA	30/12/2017
CTRL03	Configurar Backup automáticos full e incremental a la información almacenada en la base de datos.	Crear copias automáticas para los respaldos que generen alerta	A.12.3.1	Coordinador de comunicaciones	ALTA	30/12/2017
CTRL04	Realizar contrato con un tercero especializado para el almacenamiento externo de la copia de seguridad.	Firmar contrato con Seguridad XYZ para recolección y almacenamiento de respaldo	A.12.3.1	Directora administrativa	ALTA	30/12/2017

CTRL06	Establecer cronogramas para las pruebas de restauración de las copias de seguridad de la información.	Documentar e implementara cada seis meses restauración de los respaldos	A.12.3.1	Coordinador de comunicaciones	ALTA	30/12/2017

ANEXO G: Declaración de aplicabilidad

	PROCESO: TIC	Código	TIC- PRO- 10
		Versión	1
	PROCEDIMIENTO	Fecha	20/11/2017
		Clasificación	Privado
			Página 1

Declaración de aplicabilidad	Convenciones para los controles: RL: Requerimiento legal, OC: Obligación contractual, RN: Requerimiento del negocio, MP: Mejores prácticas

Controles ISO 27001:2013			**Control Actual**	**Justificación de exclusión**	**Controles**				**Documento**	**Responsable del control**
Dominio	**Sección**	**Objetivo de control/Control**			**RL**	**OC**	**RN**	**MP**		
Políticas de la Seguridad de la	A.5.1.1	Políticas para la seguridad de la	Se realizó el diseño de la política de seguridad de la información					x	Política de Seguridad	Director de seguridad de la información

información		información.								
	A.5.1.2	Revisión de las políticas de seguridad de la información.	Al implementar la política de seguridad de la información, se revisará cada año o cada que se realicen cambios significativos, para garantizar que es adecuada, eficaz y eficiente					x	Política de Seguridad	Director de seguridad de la información
Organización de la seguridad de la información	A.6.1	**Organización interna**.								
	A.6.1.1	Roles y responsabilidades para la seguridad de la información	Los roles y responsabilidades relacionados con la seguridad					x	Responsabilidades en el sistema de gestión de seguridad de la información	Líder de gestión humana
	A.6.1.2	Separación de deberes	Organigrama del proceso TIC					x	organigrama - Mapa de procesos - Procedimiento gestión de talento humano	Líder de gestión humana
	A.6.1.3	Contacto con las autoridades	Directorio TIC					x	Directorio TIC	Gerente de TIC

	A.6.1.4	Contactos con grupos de interés especiales	Directorio TIC					x	Directorio TIC	Gerente de TIC
	A.6.1.5	Seguridad de la información en la gestión de proyectos	EXCLUSIÓN	La empresa no cuenta con un proceso de gestión de proyectos					N/A	N/A
	A.6.2	**Dispositivos móviles y teletrabajo**								
	A.6.2.1	Política para dispositivos móviles	EXCLUSIÓN	Los dispositivos móviles no se utilizan para la gestión de actividades					N/A	N/A

				laborales						
	A.6.2.2	Teletrabajo	EXCLUSIÓN	La empresa tiene aprobado la opción para realizar teletrabajo					N/A	N/A
Seguridad de los recursos humanos	A.7.1	**Antes de asumir el empleo**								
	A.7.1.1	Selección	Procedimiento gestión de talento humano			x			Procedimiento gestión de talento humano	Líder de gestión humana
	A.7.1.2	Términos y condiciones laborales	En el Contrato laboral se especifican los términos y condiciones del contrato laboral y las responsabilidades con relación a la seguridad de la información.			x			Contrato laboral	Líder de gestión humana
	A.7.2	**Durante la ejecución del empleo**								

	A.7.2.1	Responsabilidades de la dirección	Los roles y responsabilidades relacionados con la seguridad				x		Responsabilidades en el sistema de gestión de seguridad de la información	Líder de gestión humana
	A.7.2.2	Toma de conciencia, educación y formación y concientización en la seguridad de la información.	El director de seguridad realizara capacitación del SGSI					x	Formatos de capacitación	Líder de gestión humana
	A.7.2.3	Proceso disciplinario	La empresa cuenta con un proceso disciplinario					x	Reglamento interno	Líder de gestión humana
	A.7.3	**Terminación y cambio de empleo**								
	A.7.3.1	Terminación o cambio de responsabilidades de empleo	En el contrato se especifica las causales de terminación del contrato			x			Contrato laboral	Líder de gestión humana
Gestión de activos	A.8.1	**Responsabilidad por los activos**								

	A.8.1.1	Inventario de activos	Procedimiento compras procedimiento de activos					x	Procedimiento compras	Líder de gestión humana
	A.8.1.2	Propiedad de los activos	Procedimiento compras					x	Procedimiento compras	Líder de gestión humana
	A.8.1.3	Uso aceptable de los activos	Procedimiento compras					x	Procedimiento compras	Líder de gestión humana
	A.8.1.4	Devolución de activos	Procedimiento compras					x	Procedimiento compras	Líder de gestión humana
	A.8.3	**Manejo de medios**								
	A.8.3.1	Gestión de los medios removibles	Procedimiento gestión de medios removibles					x	Procedimiento compras	Director de seguridad de la información
Control del acceso	**A.9.1**	**Requisito del negocio para el control de acceso**								
	A.9.1.1	Política de control de acceso	procedimiento control de acceso				x		Procedimiento de control de acceso	Director de seguridad de la información
	A.9.1.2	Acceso a redes y servicios en red	procedimiento control de acceso					x	Procedimiento de control de acceso	Director de seguridad de la información
	A.9.2	**Gestión del acceso de usuarios**								

	A.9.2.1	Registro y cancelación del registro de usuarios	procedimiento control de acceso					x	Procedimiento de control de acceso	Director de seguridad de la información
	A.9.2.2	Suministro de acceso de usuarios	procedimiento control de acceso					x	Procedimiento de control de acceso	Director de seguridad de la información
	A.9.2.3	Gestión de derechos de acceso privilegiado	procedimiento control de acceso					x	Procedimiento de control de acceso	Director de seguridad de la información
	A.9.2.4	Gestión de información de autenticación secreta de usuarios (contraseñas)	procedimiento control de acceso					x	Procedimiento de control de acceso	Director de seguridad de la información
	A.9.2.5	Revisión de los derechos de acceso de los usuarios	procedimiento control de acceso					x	Procedimiento de control de acceso	Director de seguridad de la información

	A.9.2.6	Retiro o ajuste de los derechos de acceso de usuarios	procedimiento control de acceso					x	Procedimiento de control de acceso	Director de seguridad de la información
	A.9.3	**Responsabilidades de los usuarios**								
	A.9.3.1	Uso de información de autenticación secreta (contraseñas)	procedimiento control de acceso				x		Procedimiento de control de acceso	Director de seguridad de la información
	A.9.4	**Control de acceso a sistemas y aplicaciones**								
	A.9.4.1	Restricción de acceso a la información	procedimiento control de acceso					x	Procedimiento de control de acceso	Director de seguridad de la información
	A.9.4.2	Procedimientos de ingreso seguro	procedimiento control de acceso					x	Procedimiento de control de acceso	Director de seguridad de la información

	A.9.4.3	Sistema de gestión de contraseñas	procedimiento control de acceso					x	Procedimiento de control de acceso	Director de seguridad de la información
	A.9.4.4	Uso de programas utilitarios privilegiados	procedimiento control de acceso					x	Procedimiento de control de acceso	Director de seguridad de la información
	A.9.4.5	Control de acceso al código fuente de los programas	procedimiento control de acceso					x	Procedimiento de control de acceso	Director de seguridad de la información
Seguridad física y del entorno	A.11.1	**Áreas seguras**								
	A.11.1.1	Perímetro de seguridad física	Gestión de seguridad física				X		Gestión de seguridad física	Director de seguridad de la información
	A.11.1.2	Controles de acceso físico	Gestión de seguridad física				X		Gestión de seguridad física	Director de seguridad de la información
	A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Gestión de seguridad física				X		Gestión de seguridad física	Director de seguridad de la información

	A.11.1.4	Protección contra amenazas externas y ambientales	Gestión de seguridad física				X		Gestión de seguridad física	Director de seguridad de la información
	A.11.1.5	Trabajo en áreas seguras	Gestión de seguridad física				X		Gestión de seguridad física	Director de seguridad de la información
	A.11.1.6	Áreas de carga, despacho y acceso público	Gestión de seguridad física					X	Gestión de seguridad física	Director de seguridad de la información
Seguridad de las Operaciones	A.12.1	Procedimientos operacionales y responsabilidades								
	A.12.1.2	Gestión de cambios	Procedimiento de gestión de cambios					x	Procedimiento de gestión de cambios	Jefe de servicios tecnológicos
	A.12.1.3	Gestión de la capacidad	Procedimiento gestión de la capacidad				x		Procedimiento de gestión de capacidad	Director de seguridad de la información
Seguridad de la comunicaciones	**A.13.1**	**Gestión de la seguridad de las redes**								
	A.13.1.1	Control de redes	Gestión de la seguridad de la red					x	Gestión de la seguridad de la red	Director de seguridad de la información
	A.13.1.2	Seguridad de los servicios de red	Gestión de la seguridad de la red					x	Gestión de la seguridad de la red	Director de seguridad de la información

	A.13.1.3	Separación en las redes	Gestión de la seguridad de la red					x	Gestión de la seguridad de la red	Director de seguridad de la información
	A.13.2	**Transferencia de información**								
	A.13.2.1	Políticas y procedimientos de transferencia de información	Gestión de la seguridad de la red					x	Gestión de la seguridad de la red	Director de seguridad de la información
Adquisición, desarrollo y mantenimiento de sistemas	A.14.1	**Requisitos de seguridad de los sistemas de información**								
	A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	EXCLUSIÓN	Las aplicaciones de la empresa no corren por una red publica						
	A.14.2	**Seguridad en los procesos de desarrollo y soporte**								
	A.14.2.1	Política de desarrollo seguro	EXCLUSIÓN	La empresa no cuenta con un						

				proceso de desarrollo						
	A.14.2.2	Procedimientos de control de cambios en sistemas	Procedimiento de gestión de cambios					x	Procedimiento de gestión de cambios	Jefe de servicios tecnológicos
	A.14.2.5	Principios de construcción de los sistemas seguros	EXCLUSIÓN	La empresa no cuenta con un proceso de desarrollo						
	A.14.2.6	Ambiente de desarrollo seguro	EXCLUSIÓN	La empresa no cuenta con un proceso de desarrollo						
Gestión de los	A.16.1	**Gestión de los incidentes y las mejoras en la seguridad de la información**								

incidentes de la seguridad de la información	A.16.1.1	Responsabilidades y procedimientos	Procedimiento de gestión de incidentes					x	Procedimiento de gestión de incidentes	Director de seguridad de la información
	A.16.1.2	Reporte de eventos de seguridad de la información	Procedimiento de gestión de incidentes					x	Procedimiento de gestión de incidentes	Director de seguridad de la información
	A.16.1.3	Reporte sobre las debilidades de la seguridad	Procedimiento de gestión de incidentes					x	Procedimiento de gestión de incidentes	Director de seguridad de la información
	A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Procedimiento de gestión de incidentes					x	Procedimiento de gestión de incidentes	Director de seguridad de la información
	A.16.1.5	Respuesta a incidentes de seguridad de la	Procedimiento de gestión de incidentes					x	Procedimiento de gestión de incidentes	Director de seguridad de la información

		información								
	A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Procedimiento de gestión de incidentes					x	Procedimiento de gestión de incidentes	Director de seguridad de la información
	A.16.1.7	Recolección de evidencia	Procedimiento de gestión de incidentes					x	Procedimiento de gestión de incidentes	Director de seguridad de la información
gestión de la continuidad del negocio	A.17.1	**Continuidad de seguridad de la información**								
	A.17.1.1	Planificación de la continuidad de la seguridad de la información	Plan de continuidad del negocio					x	Plan de continuidad de negocio	Gerente TIC
	A.17.2.1	Disponibilidad de instalaciones de procesamiento de	Plan de continuidad del negocio					x	Plan de continuidad de negocio	Gerente TIC

		información								
cumplimiento	**A.18.1**	**Cumplimiento de los requisitos legales y contractuales**								
	A.18.1.3	Protección de los registros	Política de protección de datos personales		x				Política de protección de datos personales	Coordinador de calidad
	A.18.1.4	Privacidad y protección de información de datos personales	Política de protección de datos personales		x				Política de protección de datos personales	Coordinador de calidad
	A.18.1.5	Reglamentación de los controles criptográficos		Exclusión						
	A.18.2	Revisiones de seguridad de la información								

	A.18.2.1	Revisión independiente de la seguridad de la información	Resultados de auditorías internas				x	Se realizarán en junio de 2018	Directora de auditoría TIC
	A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Se realizará el análisis del cumplimiento de las políticas y normas de seguridad de los usuarios. La directora de auditoría TIC validará que los procedimientos se realicen cumpliendo con las políticas establecidas				x	Se realizarán en junio de 2018	Director de seguridad de la información
	A.18.2.3	Revisión del cumplimiento técnico	Se realizarán pruebas de conectividad y carga efectuadas sobre la aplicación para certificar la capacidad de procesamiento Se realizará análisis de vulnerabilidades de los sistemas, servers.				x	Se realizarán en junio de 2018	Gerente TIC - Director de seguridad de la información

ANEXO H: Carta autorización

Estrategias Empresariales

CERTIFICA:

Que, la ingeniera LILIANA ANDREA TORRES PÉREZ, identificada con cedula de ciudadanía número 38.556.608 expedida en Cali, labora en nuestra Compañía en el cargo de directora de auditoría TIC.

Que, como estudiante de la Universidad Nacional Abierta y a Distancia - UNAD, del programa especialización en seguridad informática, se le permitirá desarrollar el proyecto DISEÑAR UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LOS PROCESOS TIC Y COMERCIAL DE LA EMPRESA ESTRATEGIAS EMPRESARIALES DE COLOMBIA S.A.S

Se expide la presente a solicitud del interesado a los 29 días del mes de septiembre de 2017.

Cordialmente:

Yina Lorena Ortiz
Directora administrativa

Estrategias Empresariales de Colombia E&E S.A.S
NIT: 901008588-3

ESTRATEGIAS EMPRESARIALES DE COLOMBIA E&E S.A.S
NIT. 901008588-3
CALLE 22N # 6AN - 24 EDIFICIO SANTA MONICA CENTRAL
CONTACTO. 312 8132117 / 314 6828584
CALI - VALLE