DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE RECURSOS INFORMÁTICOS DE LA CONTRALORÍA DEPARTAMENTAL DEL META, SEGÚN LA NORMA ISO 27001

OLGER YONATAN CAZARAN BUITRAGO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VILLAVICENCIO
2017

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE RECURSOS INFORMÁTICOS DE LA CONTRALORÍA DEPARTAMENTAL DEL META, SEGÚN LA NORMA ISO 27001

OLGER YONATAN CAZARAN BUITRAGO

Trabajo de grado para optar por el título de:
Especialista en Seguridad Informática

Director del Proyecto:
Ing. Mariano Esteban Romero Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
Villavicencio
2017

Las ideas y contenido expresados en el presente documento, son de exclusiva responsabilidad de sus autores y no comprometen la ideología de la Universidad Nacional Abierta y a Distancia UNAD

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Villavicencio, Febrero de 2018

CONTENIDO

Página.

LISTA DE TABLAS

Pag.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

El diseño del Sistema de Gestión de Seguridad de la Información para el área de gestión de recursos informáticos de la Contraloría Departamental del Meta, se fundamenta en la realización de un análisis cualitativo y cuantitativo de las amenazas, vulnerabilidades y riesgos de la dependencia, con el fin de mantener y proteger la disponibilidad, confidencialidad e integridad de los activos, con base en el ciclo de mejoramiento continuo que a postre de la presenta investigación determina el diseño y creación de políticas y procedimientos de seguridad para una correcta gestión de los riesgos que afectan a los activos de la dependencia.

La oficina de Gestión de Recursos Informáticos, es la dependencia que se encarga de prestar el servicio de soporte TI, copias de seguridad, gestión de la navegación de internet, administración de los sistemas de información entre otros en la Contraloría Departamental del Meta, los cuales ayudan al normal funcionamiento de los procesos misionales, así mismo es el área que se encarga de velar por los activos informáticos y la seguridad de la información de la entidad.

De esta manera al diseñar el SGSI, se pretende dejar fija bases para una futura implementación del SGSI en la dependencia, mediante el uso de las mejores prácticas de seguridad como la norma ISO/IEC 27001:2013 apoyado en la metodología de gestión de riesgos MAGERIT y de esta manera establecer un plan para la continuidad de los servicios.

Palabras Claves:

Sistema de Gestión de Seguridad de la Información, activos de información, vulnerabilidad, MAGERIT, ISO 27001, políticas de seguridad, gestión del riesgo.

INTRODUCCIÓN

El diseño de un SGSI para el área de informática de la Contraloría Departamental del Meta, busca establecer políticas y procedimientos que permitan certificar la seguridad de los activos de la entidad, contra amenazas que puedan afectar la integridad, disponibilidad y confidencialidad, de los mismos; de esta manera mediante un análisis de riesgos definido y estructurado sistemáticamente bajo la metodología MAGERIT, donde se desarrollarán controles que permitan minimizar el riesgo frente a materialización de amenazas en la dependencia.

Uno de los grandes interrogantes que se hacen los auditores y personal a cargo de la seguridad de la información, es ver como organizaciones fijan presupuestos para diferentes rubros sin tener en cuenta la seguridad de la información, dejando este tema a un tercer plano, exponiendo totalmente la seguridad de sus activos, con el agravante que ante un eventual ataque, la organización no tenga como recuperarse representado en efectos catastróficos.

Por lo anterior, al desarrollar el SGSI para el área de sistemas de la Contraloría Departamental del Meta basados en la norma ISO 27001:2013, busca consolidar las bases de seguridad, sentando un precedente para los demás procesos y dependencias de la entidad, exhortándolos a tomar medidas de seguridad para proteger los activos

1. EL PROBLEMA DE INVESTIGACIÓN

1.1 DESCRIPCIÓN

La oficina de gestión de recursos informáticos de la Contraloría Departamental del Meta, hace parte de los procesos de apoyo enmarcados en el mapa de proceso de la entidad, desde allí se gestiona y controla los recursos informáticos como: sistemas de información, soporte a usuarios, mantenimientos de equipos y contratación de servicios referentes al área de dependencia.

La infraestructura de red, la cual está a cargo de la oficina de sistemas exhibe insuficiencias en seguridad que pueden afectar la disponibilidad de los activos de red, específicamente el riesgo se presenta en razón a que no se tiene un plan de contingencia que permita superar eventuales fallos del servidor de dominio, servidor de internet, hosting, conmutadores y enrutadores, así mismo, no hay un proveedor de servicio de internet alternativo, que en efecto ante una falla en el servicio de comunicaciones, la dependencia no tendría como responder a las peticiones de navegación de los usuarios.

El gobierno nacional a través del Ministerio de las Tecnologías de la Información y la Comunicación, por medio de la estrategia de gobierno en línea busca que las entidades sean más transparentes, abiertas, que integren a los ciudadanos en la toma de decisiones, pero, sobre todo seguras.

Se han presentado situaciones de pérdida de información por daños en los discos duros o borrado accidental de los usuarios, situación que afecta la gestión administrativa de la dependencia y hacia el exterior de la entidad, de igual forma se efectuaron ataques al hosting web, donde uno tuvo éxito logrando cambiar el index de la página web, situación que afectó la disponibilidad del recurso.

La razón del porque aún existen vulnerabilidades y riesgos sin ningún control, radica en que no se han desarrollado políticas y procedimientos estandarizados que permitan mitigar y gestionar los riesgos de la Oficina de gestión de recursos informáticos.

1.2 FORMULACIÓN

¿Cómo gestionar la seguridad de la información del proceso de gestión de recursos informáticos de la Contraloría Departamental del Meta?

1.3 OBJETIVOS

1.3.1 Objetivo General Del Proyecto

Diseñar un SGSI, que permita restar la probabilidad de ocurrencia y mitigar el impacto de los riesgos asociados con las vulnerabilidades y amenazas existentes en la oficina de gestión de recursos informáticos de la contraloría departamental del Meta.

1.3.2 Objetivos específicos

- Identificar los activos de información y las amenazas que puedan afectar la seguridad de los activos de la oficina de gestión de recursos informàticos.
- Realizar la evaluación de los riesgos informáticos existentes en la oficina de gestión de recursos informáticos de la contraloría departamental del Meta.
- Establecer controles que permita mitigar las causas que originan los riesgos.
- Definir políticas de seguridad que permitan minimizar los riesgos a los que están expuestos los activos de información de la oficina de recursos informáticos.

1.4 JUSTIFICACIÓN

Para la Contraloría Departamental del Meta, la información es el activo más importante, de allí la necesidad de siempre mantenerla protegida, siendo que la información digital, día a día forma parte activa de la entidad en la toma de decisiones permitiendo alcanzar objetivos enmarcados en el plan estratégico de la entidad.

Para la oficina de gestión de recursos informáticos es de vital importancia, definir barreras de protección que permitan el bloqueo o reducción del impacto ante la materialización de amenazas, de esta manera se vela por el correcto funcionamiento de cada uno de los activos de la dependencia, partiendo desde su clasificación pasando por la definición y terminando con el establecimiento de políticas y procedimientos a través de un sistema de gestión de seguridad de la información

El diseño de un Sistema de Gestión de Seguridad de la Información, permite a la oficina de gestión de recursos informáticos de la Contraloría Departamental del Meta, que utilice las mejores prácticas para el aseguramiento de la información, en donde se concientiza a los funcionarios sobres los riesgos, amenazas y vulnerabilidades garantizando la confidencialidad, disponibilidad integridad y la continuidad del negocio ante la materialización de una amenaza, que pueda poner en riesgo la seguridad de la información de la oficina.

1.5 DELIMITACIÓN

El diseño del Sistema de Gestión de Seguridad de la Información se realizará en el proceso de gestión de recursos informáticos de la Contraloría Departamental del Meta, basado en la norma ISO/IEC 27001:2013, se tendrá en cuenta los activos de la entidad y el análisis y gestión de riesgo se realizará bajo la metodología MAGERIT.

2. MARCO REFERENCIAL

2.1 ANTECEDENTES

Para la compañía de seguros positiva de la ciudad de Bogotá, en el año 2016 el Ingeniero Julian Andres Ardila Navarrete, efectuó el diseño un SGSI basado en la norma ISO 27001, en donde encontró que la dirección de la compañía no estaba comprometida con la seguridad de la información, exponiendo a la compañía a riesgos innecesarios, con el diseño del SGSI propuesto por el ingeniero Ardila, dejó lista a la compañía para la implementación.

En el 2015 el Ingeniero Andrés Felipe Doria Corcho como trabajo para optar el grado de especialista en seguridad informática de la UNAD, realizó una investigación cuyo objetivo era el "diseño de un sistema de gestión de seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 en la oficina de sistemas de información y telecomunicaciones de la Universidad de Córdoba", en donde terminó con éxito su investigación concluyendo que la seguridad de la universidad mejoró, además de la integración de todos los empleados además propuso la implementación del gobierno TI, a través de la metodología COBIT.

Para la misma época los ingenieros Alexander Guzmán García y Carlos Alberto Taborda Bedoya, efectuaron una investigación con el fin de realizar el "diseño de un sistema de gestión de la seguridad informática para empresas del área textil en las ciudades de Itaguí, Medellin y Bogotá a través de la auditoria", en donde se evidenciaron los riesgos de las empresas de este sector, y se aprovecharon las bondades de las herramientas para realizar auditorías en seguridad informática.

En la Universidad Tecnológica de Pereira, como opción para optar el grado de Ingeniero de Sistemas en el año 2013, los estudiantes Juan David Aguirre

Cardona y Catalina Aristizabal Betancourt, diseñaron un SGSI para el grupo empresarial la ofrenda.

En la Contraloría Departamental del Meta, no se ha realizado el diseño de algún Sistema de Gestión de Seguridad de la información, pero si se desarrolló una política de seguridad para el uso de los recursos informáticos, que se cada corto para el fin completo

2.2 MARCO TEÓRICO CONCEPTUAL

2.2.1 Sistema de Gestión de Seguridad de la Información (SGSI)

2.2.1.1 ¿Qué es un SGSI?

Empecemos por definir que es la seguridad de la información, está es la que busca proteger la información de diversas amenazas o peligros a la que se expone, para ello debe cumplir con algunos requisitos como: confidencialidad, integridad y disponibilidad[1]:

- ✓ **Confidencialidad.** Un atentando contra la confidencialidad es cuando una persona que no es el destinatario, tiene acceso a los datos[2].
- ✓ **Integridad.** Mientras la información se transmite a través del protocolo de comunicación, un atacante podría interceptar el mensaje y realizar cambios en determinados bits del texto cifrado con la intención de alterar los datos del criptograma.[3]

[1] Mieres. Jorge, Ataques Informaticos debilidades de seguridad comúnmente explotadas (2009), Recuperado de: https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

[2] Ruiz,Jonnatan Revisión Documental Ataques Informaticos (2015), Recuperado de: http://www.academia.edu/31835413/REVISI%C3%93N_DOCUMENTAL_ATAQUES_INFORMATICOS

[3] Ruiz,Jonnatan Revisión Documental Ataques Informaticos (2015), Recuperado de: http://www.academia.edu/31835413/REVISI%C3%93N_DOCUMENTAL_ATAQUES_INFORMATICOS

- ✓ **Disponibilidad.** En este caso, un atacante podría utilizar los recursos de la organización, como el ancho de banda de la conexión DSL para inundar de mensaje el sistema víctima y forzar la caída del mismo, negando así los recursos y servicios a los usuarios legítimos del sistema.[4]

Estos dominios tienen un objetivo en común y es preservar la seguridad de la información; para ofrecer una idea más clara se entiende por información a todo conjunto de datos organizados de manera sistemática que tiene una organización, esta información puede estar almacenada y trasmitida de manera física y virtual.

Figura 1.SGSI

Fuente: El Autor

[4] Ruiz,Jonnatan Revisión Documental Ataques Informaticos (2015), Recuperado de: http://www.academia.edu/31835413/REVISI%C3%93N_DOCUMENTAL_ATAQUES_INFORMATICOS

2.2.1.2 Funcionalidad de un SGSI

Para toda organización, entidad o empresa la información en conjunto con los procedimientos, procesos, medios, administradores, usuarios y medios que la soportan hacen parte del activo más importante de la misma, si se elevan los niveles de confidencialidad, integridad y disponibilidad de la información se logrará mantener los estándares de competitividad, seguridad, imagen legal y rentabilidad en referencia con las demás organizaciones, generando con esto, alcance a los objetivos estratégicos que se materializan en beneficios económicos.

Toda organización incluidos sus Sistemas de Información, está expuesta a experimentar un sinnúmero de amenazas cada vez más especializadas, que en caso de materializarse pueden generar un impacto desastroso para la organización, llegando a someter activos críticos sin posibilidad de repararlos, estas amenazas se materializan a efectos de explotar cualquier vulnerabilidad existente, cabe destacar que estas amenazas pueden provenir desde fuentes externas o internas de manera dolosa o culposa.

Figura 2. Utilidad de un SGSI

Fuente: www.iso27000.es

2.2.1.3 ¿Que incluye un SGSI?

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma[5]:

Figura 3. Qué incluye un SGSI

Fuente: www.iso27000.es

Alcance del SGSI: Ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas)[6].

Política y objetivos de seguridad: De manera general se trata del documento que establece lineamientos de aplicabilidad en donde se establece el compromiso de la dirección y el enfoque que debe tener la organización en cuanto la gestión de la seguridad de la información

[5] IBID., ISO 27001.
[6] IBID., ISO 27001.

Procedimientos y mecanismos de control que soportan al SGSI: son todos los procedimientos que se desarrollan para el cumplimiento del SGSI.

Enfoque de evaluación de riesgos: allí se describe la metodología que se emplea para realizar la identificación de amenazas, activos y riesgos, las vulnerabilidades, impacto en los activos ante la materialización de amenazas en la afectación de los activos, también se definen los criterios para la aceptación del riesgo residual fijando los niveles de aceptación.

Informe de evaluación de riesgos: el resultado de aplicar la metodología de evaluación citada anteriormente.

Plan de tratamiento de riesgos: en él se identifica las acciones a tomar por parte de la dirección, se fijan responsabilidades y prioridades, se estiman costos, lo anterior en efecto de la evaluación de riesgos.

Procedimientos documentados: Todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.

Registros: soportan la evidencia de cada del resultado del SGSI en el cumplimiento de su objetivo y desarrollo de los procedimientos

2.2.1.4 ¿Cómo implementar un SGSI?

Para implementar un SGSI con base en la ISO 27001, se realiza a través del ciclo PHVA, inmerso en los sistemas de gestión de calidad.

Figura 4. Ciclo PHVA

Fuente: el Autor

2.2.1.4.1 Plan: Establecer el SGSI

- Se define el alcance del SGSI el cual debe ir alineado a la misión de la organización, en donde se tiene en cuenta los activos y la tecnológica, localización y términos del negocio.
- Política de seguridad: en donde se incluye el ámbito, términos generales de aplicación se consideran requerimientos, legales y contractuales además de estar alineada con la misión y la visión de la entidad, debe estar aprobada por la dirección de la entidad.
- Se define una metodología de evaluación del riesgo apropiada para el diseño del SGSI y la estrategia de la organización, además de incorporar los criterios en los que se acepta el riesgo y los niveles de aceptación de los mismos.

- Se identifican los riesgos, en donde en primera medida se identifican los activos de información que generen un valor para la organización, también en este documento se relacionan las amenazas que puedan afectas estos activos, y las vulnerabilidades que puedan ser explotadas por las amenazas identificadas.
- Se analizan y evalúan los riesgos en cuanto a la materialización de amenazas que puedan afectar los activos de la organización, explotando alguna vulnerabilidad lo que supone la pérdida de integridad, confidencialidad y disponibilidad de la información.
- Se identifican las opciones de tratamiento de riesgos a los riesgos encontrados.

Figura 5. Gestión de Riesgos

Fuente: http://www.iso27001security.com/html/27004.html

- Seleccionar los objetivos de control los cuales se encuentra definidos en el Anexo A de la ISO 27001, para el tratamiento de riesgos.

- Identificados los riesgos residuales del resultado del tratamiento, estos deben ser aprobados por la dirección.
- Se define un documento de aplicabilidad de la política.

2.2.1.4.2 Hacer

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información[7].
- Se implanta el plan de tratamiento de riesgos.
- Se implanta Los objetivos de control y controles seleccionados del resultado de la fase planificar.
- Se gestionan las operaciones SGSI.
- Se gestionan los recursos.
- Los procedimientos y controles se implantan en esta fase.

2.2.1.4.3 Verificar

- Se ejecutan los controles y procedimientos con el fin de detectar fallas del SGSI, en esta fase también se identifican las brechas e incidentes de seguridad para ayudar a la dirección a determinar si hay un cumplimiento de la política de seguridad y si se está garantizando la seguridad de la información de la organización con os estándares de eficiencia establecidos.
- Se mide la efectividad de los controles.
- Se realizaran de manera periódica auditorías internas al SGSI, para evaluar la efectividad del sistema.
- Se actualizan los planes de seguridad de la información.

[7] IBID., ISO 27001.

2.2.1.4.4 Actuar

- Se realizas las acciones preventivas y correctivas detectadas de la fase verificación,
- Se comunican las acciones a las partes interesadas, guardando cuidado con el nivel de detalle el cual debe ser óptimo.
- Las mejoras introducidas deben ayudar a alcanzar el objetivo.
- Se regresa nuevamente a la fase planear.

2.2.2 Seguridad informática

Define la seguridad informática como la encargada de garantizar los tres principios básicos en el manejo de la información como lo son la confidencialidad, integridad y disponibilidad utilizando para ello un conjunto de normas, métodos, herramientas y personal humano calificado para actuar ante cualquier tipo de amenaza[8].

2.2.3 Amenazas

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información. Debido a que la Seguridad Informática tiene como propósitos de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones[9].

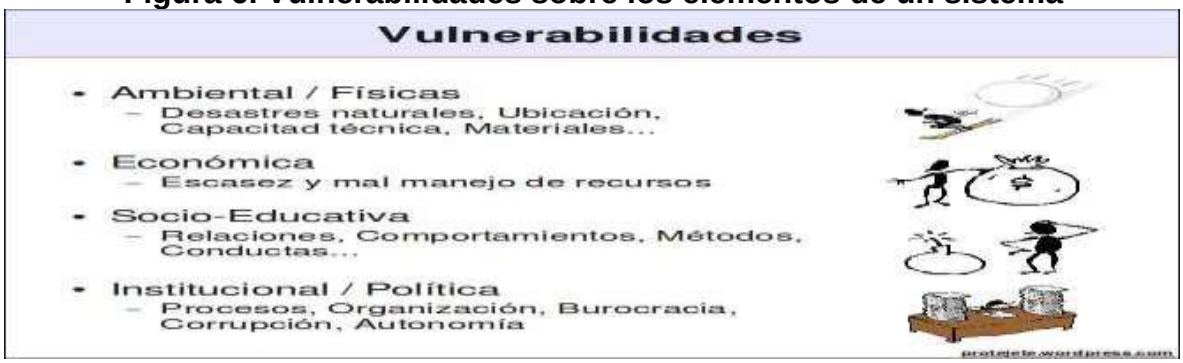
[8] Ingtux, ¿Qué es la Seguridad Informática?, Recuperado de: http://g3ekarmy.com/%C2%BFque-es-la-seguridad-informatica/

[9] Gestión de Riesgo en la Seguridad Informática recuperado de: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

2.2.4 Vulnerabilidades

La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacidad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño[10].

Figura 6. Vulnerabilidades sobre los elementos de un sistema



Fuente: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

2.2.5 Un evento de seguridad

Es aquella situación donde se presentan posibles fallas en el cumplimiento de las políticas y controles de la seguridad de la información, pero que no afectan el desarrollo de las actividades de la empresa y puede tratarse con una acción correctiva.

2.2.6 Un incidente de seguridad

Es aquel que pone en riesgo la seguridad de la información, ya sea de forma intencional o no y ocasiona interrupciones en el desarrollo de las actividades de la empresa.

[10] Gestión de Riesgo en la Seguridad Informática recuperado de la página web: https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

2.3 MARCO CONTEXTUAL INSTITUCIONAL

2.3.1 Descripción De La Empresa

2.3.1.1 Una entidad:

La Contraloría Departamental del Meta es una entidad del estado creada el 18 de octubre de 1960 bajo la ordenanza departamental 02 del mismo año, su función está orientada a ejercer la vigilancia de la gestión fiscal de la administración pública, de sus entidades descentralizadas, empresas de servicios públicos mixtas, privadas, y de los particulares que administren bienes y fondos del Estado. Dicho control será ejercido en forma posterior y selectiva de conformidad con los procedimientos, sistemas y principios establecidos en la Ley.[11]

2.3.1.2 Misión

La Contraloría Departamental del Meta vigila la gestión fiscal de sus sujetos de control y particulares que manejen fondos o bienes del Estado, de manera efectiva, transparente y visible, promoviendo la participación ciudadana en el control de los recursos públicos.[12]

2.3.1.3 Visión

En 2019, la Contraloría Departamental del Meta será visible por su gestión transparente, efectiva en el control fiscal y la participación ciudadana en la vigilancia de los recursos públicos.[13]

[11] http://www.contraloriameta.gov.co/
[12] http://www.contraloriameta.gov.co/
[13] http://www.contraloriameta.gov.co/

2.3.1.4 Política De Calidad

La Contraloría Departamental del Meta garantiza transparencia, eficacia, eficiencia y efectividad en el ejercicio del control fiscal a los recursos públicos del Departamento del Meta, con funcionarios competentes, mejoramiento continuo de los procesos y vinculación de la comunidad en la defensa del interés público, con el propósito de satisfacer las necesidades del cliente.[14]

2.3.1.5 Objetivos De Calidad

- Garantizar el control y vigilancia de la gestión fiscal
- Promover la participación de la ciudadanía en la vigilancia de la gestión pública y sus resultados
- Fortalecer la celeridad en el trámite de los procesos de responsabilidad fiscal
- Asegurar el funcionamiento e impulsar la modernización institucional[15]

[14] http://www.contraloriameta.gov.co/
[15] http://www.contraloriameta.gov.co/

2.3.1.6 Organigrama

Figura 7. Organigrama Contraloría Departamental del Meta

Fuente:http://www.contraloriameta.gov.co

2.3.2 Ubicación física

La Contraloría Departamental del Meta es una entidad del sector público del estado Colombiano encargado de la vigilancia de la gestión fiscal de la administración pública en el Departamento del Meta, tiene una única sede, la cual se encuentra ubicada en la dirección Cra 34 # 35-38 en la ciudad de Villavicencio.

El área de gestión de recursos informáticos es dependencia directa del despacho de contralor quien a su vez es representante legal de la entidad, lo que la posiciona en una dependencia transversal, prestando no sólo soporte sino haciendo parte y tomando partido de las decisiones misiones, estratégicas de la entidad, mediante el desarrollo de planes y programas que contribuyen con la ejecución del plan estratégico de la Contraloría.

El área de sistemas actualmente tiene entre sus funciones lo contemplado en el decreto 415 de 2016 que avista las siguientes:

- Liderar la gestión estratégica con tecnologías de la información y las comunicaciones mediante la definición, implementación, ejecución, seguimiento y divulgación de un Plan Estratégico de Tecnología y Sistemas de Información (PETI) que esté alineado a la estrategia y modelo integrado de gestión de la entidad y el cual, con un enfoque de generación de valor público, habilite las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo de su sector y la eficiencia y transparencia del Estado[16].
- Liderar la definición, implementación y mantenimiento de la arquitectura empresarial de la entidad y/o sector en virtud de las definiciones y lineamientos establecidos en el marco de referencia de arquitectura empresarial para la gestión de Tecnologías de la Información y las Comunicaciones (TIC) del Estado, la estrategia GEL y según la visión estratégica, las necesidades de transformación y marco legal específicos de su entidad o sector[17].
- Desarrollar los lineamientos en materia tecnológica, necesarios para definir políticas, estrategias y prácticas que habiliten la gestión de la entidad y/o sector en beneficio de la prestación efectiva de sus servicios y que a su vez faciliten la gobernabilidad y gestión de las Tecnologías de la Información y las Comunicaciones TIC. Así mismo, velar por el cumplimiento y actualización de las políticas y estándares en esta materia[18].

16 http://es.presidencia.gov.co/normativa/normativa/DECRETO%20415%20DEL%2007%20DE%20MARZO%20DE%202016.pdf

17 http://es.presidencia.gov.co/normativa/normativa/DECRETO%20415%20DEL%2007%20DE%20MARZO%20DE%202016.pdf

18 http://es.presidencia.gov.co/normativa/normativa/DECRETO%20415%20DEL%2007%20DE%20MARZO%20DE%202016.pdf

- Liderar la gestión, seguimiento y control de la ejecución de recursos financieros asociados al portafolio de proyectos y servicios definidos en el plan estratégico de Tecnologías y Sistemas de información[19].

En la dependencia hay asignado un profesional universitario de sistemas, el cual tiene entre sus funciones:

- Diseñar e implementar los sistemas de información de la entidad que contribuyan al logro de la misión institucional e implementar y mantener en forma oportuna la tecnología necesaria.
- Adoptar medidas de seguridad orientadas a mantener la integridad de los recursos informáticos.
- Garantizar la formulación, el cumplimiento, el control en la ejecución y la evaluación de los planes, programas y proyectos adoptados por la Contraloría.

Actualmente al área de sistemas presta los siguientes servicios a personal interno y externo.

2.3.3 Servicios Informáticos

Tabla 1. Servicios ofrecidos por la entidad

SERVICIO	DESCRIPCIÓN
Soporte Equipos Informáticos	Servicio en donde se realiza asistencia/soporte a los funcionarios de la entidad, previa solicitud diligenciada de manera virtual o en casos excepcionales de forma telefónica.

19 http://es.presidencia.gov.co/normativa/normativa/DECRETO%20415%20DEL%2007%20DE%20MARZO%20DE%202016.pdf

Tabla 2. (Continuación)

SERVICIO	DESCRIPCIÓN
Intranet	Sitio web interno de soporte estático a donde pueden ingresar solamente los funcionarios de la entidad, pues allí encuentran todos los procedimientos, formatos, políticas normatividad aplicables a los diferentes procesos.
Sitio Web	Sitio web de consulta por parte de los funcionarios de la entidad, allí se publica la gestión de la entidad en ejercicio de su función y misión.
Correo electrónico	Sistema de comunicación oficial digital, que permite la interacción institucional de los funcionarios de la entidad; por directriz de la dirección aduciendo problemas de seguridad, sólo se le creó cuentas a los líderes de proceso.
Spark	Sistema de mensajería instantánea en donde se pueden realizar conversaciones sincronizadas, envío y recepción de archivos, conferencias y demás.
Internet	Servicio de navegación por la internetwork lo que permite a los funcionarios la gestión administrativa facilitándoles la comunicación e interacción con la ciudadanía así mismo la navegación.

Fuente: Autor

2.3.4 Estructura de la Red LAN

La infraestructura de red de la entidad está compuesta por dispositivos tecnológicos que tienen un atraso funcional de 6 años, por lo cual no prestan un acorde a las demanda de las peticiones de los usuarios.

Se encuentran 76 computadores de escritorios, 13 portátiles, 5 impresoras de red, 3 servidores, 5 switch's y 3 hub's, por el nivel de complejidad y seguridad se detallan los 3 servidores.

Tabla 3. Servidores Instalados

Servidor	Sistema Operativo	Características Físicas	Servicios/servidores
Hp Proliant ML 160	Windows Server 2008 Estándar R1 64 Bits	• Ram 16 GB • Disco duro 1 TB • Procesador Intel Xeón 2.00 Ghz	• Dominio • Archivos • WUSUS • Sql Server 2008. • GLPI • Openfire
Hp Proliant ML 110	Debian 8 64 Bits	• Ram 2 Gb • Disco Duro 320 Gb. • Procesador Intel Pentium 3 Ghz	• Apache • Mysql • PHP • Sitio web de la entidad
Hp Dx2300	PFsense(FreeBSD)	• Ram 1 Gb • Disco Duro 80 Gb • Procesador Intel Core 2 Duo 1.8 Ghz	• Squid • Enrutamiento • Internet

Fuente:Autor

Además se cuenta con cableado estructurado que llega a un rack por cada piso, lo que facilita la administración ante el continuo cambios de puestos y puntos de red.

2.4 MARCO LEGAL

La Contraloría Departamental del Meta al ser una entidad descentralizada con autonomía administrativa, está regida por las siguientes normas y decreto nacionales y locales.

- Ley 330 de 1996, por la cual se desarrolla parcialmente el artículo 308 de la Constitución Política y se dictan otras disposiciones relativas a las Contralorías Departamentales.
- Ley 610 de 2000, por la cual se establece el trámite de los procesos de responsabilidad fiscal de competencia de las contralorías.
- Ley 1474 de 2011, por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- Decreto único reglamentario 1082 de 2015, por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Para el desarrollo de este proyecto es necesario tener soportes teóricos como son los estándares normativos, que sustenten el actuar de las entidades públicas del país en cuanto a la preservación de la seguridad de la información como lo es:

- La ley 1581 de 2012 protección de datos.
- Ley 1712 de 2014 transparencia y del derecho de acceso a la información pública nacional.

3. METODOLOGÍA

El desarrollo del siguiente proyecto, se realiza con base en el tipo de investigación descriptiva, en razón a que ya se tiene conocimiento del problema, y se espera plantear un SGSI a través de las variables y requerimientos de la ISO/IEC 27001.

3.1 TIPO DE INVESTIGACIÓN

El desarrollo del proyecto se ajusta al tipo de investigación descriptiva y analítica, en razón a que esta se desarrolla en el marco de: recolección de la información, descripción, registro de la información, análisis, interpretación y comprensión de los procesos; todo el análisis se hace sobre la gestión de la dependencia en donde se requiere detectar fallas y anomalías de seguridad de la información, para así plantear soluciones.

3.1.1 Descriptiva

Se usa al momento de buscar describir una realidad, que tiene como alcance todos sus componentes, y hace referencia al proceso preparatorio del trabajo científico, facilitando la ordenación de las observaciones presentadas en la conducta, los factores, procesos, procedimientos, características y otras variables de fenómenos y hechos, como conclusión este tipo de investigación no tiene explicación a su hipótesis.

3.2 DISEÑO DE INVESTIGACIÓN

Las entidades públicas del estado colombiano, con base en la estrategia de gobierno en línea impulsada por el ministerio de las TIC, el cual tiene como objetivo que Colombia sea el país más transparente y seguro, siendo así que promueve una política de datos abiertos en donde los entidades oficiales deben

publicar toda la información de gestión, salvo casos excepcionales en donde la información es clasificada o reservada.

Para darle cumplimiento a la estrategia de gobierno en línea en el componente seguridad de la información esta entidad quiere hacer una gestión más segura basada en la norma ISO 27001:2013.

Por lo anterior para el desarrollo del proyecto se utilizara esta metodología en colaboración con MAGERIT para clasificar los activos, amenazas y riesgo en donde se les realizara una evaluación y valoración para que finalmente se haga un tratamiento de riesgos y posteriormente creación de documento de aplicabilidad con base en la norma ISO 27001:2013.

Con MAGERIT se busca identificar los activos, las amenazas, los riesgos y las vulnerabilidades en la organización que permiten que las amenazas se materialicen impactado de manera negativa sobre lo activos identificados, se persigue una aplicación metódica de gestión de riesgos evitando así la improvisación y la subjetividad del analista.

Esta norma sirve de soporte y ayuda para implementar un sistema de gestión de riesgos de manera organizada y objetiva con procesos bien definidos.
Que se logra con MAGERIT.

1. Identificación de activos
2. Determinación de amenazas
3. Estimación de impactos
4. Determinación del riesgo
5. Determinación de las medidas de seguridad necesarias

3.3 POBLACIÓN

Aunque en la Contraloría Departamental del Meta hay 68 funcionarios dentro de su planta de personal, la oficina de gestión de recursos informáticos sólo cuenta con un funcionario de planta y un funcionario asignado temporalmente.

3.4 MUESTRA

De los 68 funcionarios de las diferentes dependencias de la entidad, para el desarrollo del proyecto en la oficina de gestión de recursos informáticos se toma: funcionario profesional de sistemas de planta, funcionario técnico con asignación temporal y el jefe directo de la dependencia.

3.5 FUENTES DE INFORMACIÓN

La información que se obtiene directamente de la oficina de gestión de recursos informáticos de la Contraloría Departamental del Meta, sus procesos, funciones de la dependencia, estado del arte, y resultados dela análisis de riesgos.

3.5.1 Información Primaria

A través de la vivencia del día a día en la dependencia y a partir del desarrollo de una encuesta, se logra determinar la problemática que aqueja a la dependencia en donde se ven involucrados los activos para poder determinar el análisis de riesgos, de igual manera se obtiene el procedimiento y las políticas de seguridad implementadas.

3.5.2 Información secundaria

Se tienen en cuenta información bibliográfica que se obtiene del desarrollo de la especialización, conceptos formados del estudio de las diferentes asignaturas así mismo información de la internetwork.

3.6 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Para la recolección de la información se realizó a través del acceso directo a las evidencias, por observación directa, y técnica de realización de encuesta.

3.6.1 Técnica de observación

Teniendo en cuentas las funciones y responsabilidades de la oficina de gestión de recursos informáticos se observó: ubicaciones de los rack de telecomunicaciones distribuidas en cada uno de los pisos, ubicación de los diferentes servidores, seguridad de los computadores, procedimiento de recursos informáticos y lugar de almacenamiento de las copias de seguridad.

3.6.2 Técnica de encuesta

Se realizó un cuestionario a los tres funcionarios involucrados con la oficina de gestión de recursos informáticos en donde: las preguntas eran cerradas con una única opción de respuesta, respuestas abiertas con sugerencias de cómo mejorar el sistema.

4. RESULTADOS

4.1 INVENTARIO DE ACTIVOS.

La Contraloría Departamental del Meta está comprometida con preservar la confidencialidad, integridad y disponibilidad de la información que en ella se gestiona, incluyendo medidas que la pueden soportar y fortalecer, se realiza la clasificación de los activos de información basados en la metodología de riesgos MAGERIT Libro II catálogo de elementos que los clasifica de la siguiente manera:

- **Servicios**: Satisface una necesidad de los usuarios, los servicios prestados por el sistema:
- **Datos/Información:** activo abstracto que es almacenado de manera física y virtual pueden estar agrupados en ficheros y base de datos.
- **Aplicaciones Informáticas:** activo software que sirve para procesar, gestionar, transportar y transformar los datos.
- **Equipos Informáticos:** trata del hardware que soporta las aplicaciones y los datos informáticos.
- **Soportes de Información:** son los dispositivos físicos con los cuales se pueden almacenar información.
- **Redes de Comunicaciones:** son los medios de transporte de la información.
- **Equipamiento auxiliar:** otro tipo de activo que sirven de soporte para los equipos informáticos sin estar directamente relacionado con los datos.
- **Instalaciones/Personal:** los lugares donde está la información y el personal que la administra.

En razón a que se tiene acceso total al proceso de sistemas de la entidad se hace una identificación de los activos, y se clasifica de acuerdo al tipo.

4.1.1.1 Servicios.

Son todos aquellos activos encargados de satisfacer las necesidades de los funcionarios de la dependencia entre estos tenemos.

- World wide web, el cual se encarga de ofrecerles el servicio de internet para los funcionarios.
- Correo electrónico, para la gestión de cuentas de correos electrónicos enviar y recibir correos.
- Soporte interno (a usuarios de la propia organización), en donde se ofrece la asistencia informática a los funcionarios de la entidad.
- Página web, Servicio de mantenimiento de la página web.
- Mensajería interna (a usuarios de la propia organización) Servicio de mensajería Interna.

4.1.1.2 Datos/Información

En pocas palabras son el eje central de la oficina de gestión de recursos informáticos ya que el diseño del sistema de gestión de seguridad gira en torno a esta, es un tipo de activo abstracto a diferencia de los demás activos.

- Ficheros, Contratos suscritos con los proveedores
- Copias de Respaldo Archivo de Copias de seguridad de la información

4.1.1.3 Aplicaciones Informáticas

Hace referencia al software encargado de gestionar el activo datos mediante operaciones informáticas.

- Sysman, Sistema de Información administrativo

- GLPI Sistema de Información para solicitar asistencia
- Bitdefender, antivirus el cual la gestión se realiza desde la nube.

4.1.1.4 Equipos informáticos

Se trata de los dispositivos hardware encargados de soportar las aplicaciones y los datos.

- Grandes equipos, servidor de bases de datos, servidores de dominio e internet
- Informática personal, computadores de la entidad
- Conmutadores, conmutadores de la entidad
- Centralita telefónica, Planta telefónica
- Impresoras, medios de impresión

4.1.1.5 Soportes de Información

- Discos, discos duro de respaldo de la información

4.1.1.6 Redes de Comunicaciones

- Red local, Lan de la entidad

4.1.1.7 Equipamiento Auxiliar

- Mobiliario, muebles, estantes de la entidad.

4.1.1.8 Instalación y Personas

- Rrack, Rack de Comunicaciones

- Administradores de sistemas, Profesional Universitario de Sistemas
- Proveedores, Proveedores

4.1.2 Informe de calificación de riesgos.

Una vez realizado el análisis de riesgos, se determina que hay activos de la Contraloría Departamental del Meta que hacen parte del grupo con riesgo alto, y el efecto sería catastrófico, lo que en efecto afectaría la seguridad de la información representados en grandes consecuencias para la entidad.

Denegación del servicio y fallo de los servicios de comunicaciones son las amenazas que pueden afectar al activo página web, otro de los activos al que se le debe prestar principal atención es el activo sysman, siendo este el Sistema de información para la gestión administrativa, que puede ser afectado por el acceso no autorizado representado en efectos catastróficos a la privacidad de la información de la entidad.

El servidor de datos y los computadores debido a que la entidad no tiene un servicio de vigilancia están en riesgo de pérdida por robo, para lo cual se deben tomar medidas de protección.

La entidad tiene un sistema de Copias de Seguridad que permite respaldar la información de gestión de los funcionarios, los primeros 5 días hábiles de cada mes, no obstante ese respaldo se está llevando en CD lo que dificulta el almacenamiento y la copia y consigo la degradación de la información, con el resultado de análisis de riesgos se recomienda cambiar el almacenamiento de los backups.

Por otra parte hay amenazas clasificadas dentro del grupo desastres naturales, que tienen que ver con fuego e inundación y que en caso de materializarse tendría

efectos catastróficos para la entidad, por fortuna la ubicación física de la entidad, no hay riesgo que estas amenazas se ejecuten.

4.2 EVALUACIÓN DE RIESGOS INFORMÁTICOS

4.2.1 Valoración Cualitativa de los Activos

Para realizar la valoración de los activos se tuvo en cuenta que no a todos se les debe generar el mismo peso, toda vez que cada uno cumple un función diferente y el riesgo de amenaza varía en razón de la misma, por lo tanto el impacto ante la materialización de una amenaza es diferente, se realizar la valoración cuantitativa en razón de las cinco dimensiones confiabilidad, integridad, autenticidad, disponibilidad y trazabilidad de acuerdo a la siguiente clasificación:

- 10, extremo se presenta cuando el daño es extremadamente grave
- 9, muy Alto se presenta cuando el daño es muy grave
- 6-8, se presenta cuando hay el daño es altamente grave
- 3-5, se presenta cuando el daño es importante
- 1-2, se presenta cuando el daño es menor
- 0, despreciable se presenta cuando el daño es importante para efectos prácticos.

De acuerdo al activo se le asignan las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, las cuales sirven para darle un valor de acuerdo a las consecuencias frente a la materialización de amenazas.

4.2.1.1 Valoración Cualitativa Servicios.

Comprende los activos clasificados World wide web, correo electrónico, Soporte, página web, y mensajería interna, en donde la mayor afectación se presenta en la página web involucrando la disponibilidad e integridad del activo, cuyo valor alcanza a daños graves, para los demás activos la afectación se presenta en los dominios de confidencialidad, integridad, y autenticidad en una menor proporción con daños importantes.

4.2.1.2 Valoración Cualitativa Datos/Información

Los activos Ficheros y copias de respaldo, debido a la forma como la dependencia realiza gestión sobre el activo el grado de afectación se cataloga como menor, en los dominios de confidencialidad integridad y disponibilidad.

4.2.1.3 Valoración Cualitativa Aplicaciones Informáticas

Los activos clasificados son Sysman, GLPI, Bitdefender, en promedio se presentan afectaciones con peso importante, viéndose involucrados especialmente los componentes de confidencialidad, integridad, disponibilidad y trazabilidad.

4.2.1.4 Valoración Cualitativa Equipos informáticos

Se trata de los dispositivos hardware encargados de soportar las aplicaciones y los datos como lo es grandes equipos, informática personal, conmutadores, centralita telefónica, impresoras, los grados de afectación varian entre daños importantes y menores los cuales afectan la integridad y disponibilidad de los activos.

4.2.1.5 Valoración Cualitativa Soportes de Información

Discos, discos duro de respaldo de la información al estar almacenados en una caja fuerte, la afectación es menor.

4.2.1.6 Valoración Cualitativa Redes de Comunicaciones

Red local, el grado de afectación es menor en donde el dominio afectado es la disponibilidad del activo.

4.2.1.7 Valoración Cualitativa Instalación y Personas

Rack, administradores de sistemas y proveedores, donde se presenta un grado de afectación al administrador del sistema en el dominio de disponibilidad.

Para realizar la identificación y valoración de amenazas se tiene en cuenta la frecuencia con las que estas ocurren, las cinco dimensiones de seguridad que denota Magerit y la escala de rango porcentual de impactos en los activos.

En donde:

- Frecuencia muy alta, se presentó al menos en el último día
- Frecuencia alta, se presentó en la última Semana
- Frecuencia media, se presentó en el último mes
- Frecuencia baja, se presentó en los últimos 6 meses
- Frecuencia muy baja, no Se presentó en el último año.

En donde la amenaza que más se presentó fue la de indisponibilidad de personal con una frecuencia alta, lo anterior aduce a que sólo hay una persona al frente de la oficina de sistemas para atender los diferentes requerimientos.

Con una frecuencia media es decir que se presentó en último mes, se evidenciaron las amenazas: caída del sistema por sobrecarga, corte del suministro eléctrico, errores del administrador y fallo de servicios de comunicaciones, resultados de no tener servicios de respaldo de energía, y problemas con el proveedor de internet además de su ancho de banda mínimo.

Ahora, se refleja un alto impacto frente a la materialización de amenazas de fallo de servicios de comunicaciones, errores del administrador y pérdida de equipos, las cuales afectan el servidor de base de datos, los computadores de la entidad y la página web; con mayor proporción se presenta en el dominio de confidencialidad y en una menor en el de integridad.

Con un impacto alto es decir del 75%, se presentan las amenazas caídas del sistema por sobrecarga, indisponibilidad del personal, fallo de servicios de comunicaciones y errores del administrador, en donde los activos principalmente afectados son sysman, servicio de mensajería interna y soporte a usuarios, afectando la disponibilidad e integridad de los activos.

Los riesgos frente a la materialización de amenazas que puedan afectar en gran medida la gestión de la dependencia, tiene que ver con:

- Accesos desatendidos a los cuartos de comunicaciones
- Falta de personal para la atención a los requerimientos.
- Ancho de banda de internet reducido.
- Contar con un solo ISP.
- Falta de unidades de respaldo o un plan de contingencia.

En el anexo a, se encuentra la valoración detallada de los riesgos y amenazas a los que se encuentran expuestos los activos del área de gestión de recursos informáticos de la Contraloría Departamental del Meta.

4.3 CONTROLES DE SEGURIDAD

Una vez se han identificado los activos de la entidad y las amenazas que estos representan a su seguridad, se definen salvaguardas con el fin de reducir el riesgo teniendo en cuenta los activos que se van a proteger y de acuerdo a la metodología Magerit, las cuales se clasifican en:

:

- Preventivas: disuasorias y eliminatorias
- Acotan la degradación: minimizadoras, correctivas y recuperativas
- Consolidan el efecto de las demás: monitorización, de detección, de concienciación y administrativas

Como control preventivo se deben crear políticas de seguridad de la información con el fin de preservar la integridad, confidencialidad y disponibilidad del: antivirus, conmutadores, ficheros, pagina web, red lan, servidores y computadores.

Como control eliminatorio para evitar que los equipos sean afectados por virus se deben desinstalar las licencias vencidas, en donde cada vez que cumple el tiempo límite de validez de las licencias, se toman cerca de tres meses el cambio, de igual manera proteger el rack de comunicaciones instalando controles de acceso mínimos, se recomienda físicos.

En cuanto a controles recuperativos, se pueden implementar en los activos servicios, datos, aplicaciones informáticas y equipos informáticos, para lo cual es necesario:

- Canal o soporte redundante para el servicio de internet, mensajería interna, pagina web, de igual doble soporte para los contratos.
- Se debe mejorar el sistema de copias de seguridad para los activos, servidor de base de datos e internet, computadores información de gestión de los funcionarios, de manera que se pueda asegurar la integridad de las mismas.

Hay salvaguardas de monitorización para los activos correo e internet, en razón a que son activos cuyo uso no depende de la gestión del área de informática, y es uno de los focos principales de riesgo de seguridad, donde se pueden materializar amenazas , como accesos no autorizados, descarga de virus y robos de información

4.4 SGSI PARA EL ÁREA DE SISTEMAS DE LA CONTRALORÍA DEPARTAMENTAL DEL META

4.4.1 Establecer El SGSI

4.4.1.1 Alcance

El contenido de este SGSI, comprende la seguridad de la información de los procesos y subprocesos que ha establecido la organización para el área de Gestión de los Recursos Informáticos de la Contraloría Departamental del Meta.

4.4.1.2 Política del Sistema de Gestión de Seguridad.

La información es un recurso valioso para el área de Gestión de los Recursos Informáticos de la Contraloría Departamental del Meta , dependencia apoyada en la misión, visión y objetivos estratégicos de la Contraloría, expresa su compromiso en la minimización de los riesgos a los cuales está expuesta la

información que maneja, impulsando una cultura de seguridad y calidad en todos sus procesos, gestionando los incidentes de seguridad que se puedan presentar con el fin de garantizar la seguridad y continuidad de los procesos principales del área.

Recursos Informáticos propende por la evaluación, vigencia y conformación de esta política, al igual que los demás elementos del SGSI.

Los activos de información estarán clasificados e identificados a fin de establecer los niveles adecuados de protección.

El funcionario encargado de la dependencia debe garantizar la protección de la información, a la cual tenga acceso para evitar pérdida, daño o uso no autorizado.

La dependencia implementará controles que permitan salvaguardar los activos de información, para evitar accesos no autorizados, alteraciones o uso indebido de los recursos, garantizando la continuidad de la prestación de los servicios internos y usuarios.

4.4.1.3 Organización de la Seguridad de la Información

Desde la oficina del despacho de la Contraloría Departamental del Meta, se define el propósito de crear los espacios necesarios para la capacitación y la asignación de recursos pertinentes y suficientes para velar por el dominio y conocimiento de las políticas de seguridad de la información contenidas en la norma ISO 27001 para el área de recursos informáticos.

4.4.1.3.1 Responsables en la seguridad de la información.

La seguridad de la información de la dependencia está a cargo del jefe de Sistemas cuyas funciones son:

- Implantar y administrar sistemas informáticos en el entorno mono y multiusuario de manera segura
- Proponer y coordinar cambios para mejorar la explotación del sistema informático y las aplicaciones con los controles previstos en el SGSI
- Administrar los usuarios y contraseñas de los empleados en la plataforma tecnológica de la empresa
- Velar por la seguridad del sistema operativo bloqueando sitios web que puedan afectar la integridad del sistema
- Generar copias de seguridad incrementales diarias y completas semanales de las bases de datos de la empresa
- Realizar las pruebas de funcionalidad a las copias de seguridad.
- Verificar el licenciamiento de software instalado en la plataforma tecnológica de la empresa
- Efectuar el mantenimiento preventivo, correctivo y adaptativo de los equipos de cómputo.

4.4.1.3.2 Acuerdos de Confidencialidad

La oficina de recursos informáticos gestionó la incorporación en los contratos, cláusulas de confidencialidad y no divulgación de la información, determinando el alcance del incumplimiento a esta política, su responsabilidad civil y penal al que hubiere lugar de acuerdo con lo establecido en la Ley 1273 de 2009 y 1581 de 2012.

Los funcionarios, contratistas y terceros que tengan vínculos con la oficina de gestión de recursos informáticos aceptan los acuerdos de confidencialidad y no divulgación, que establecen los compromisos de cumplir con los lineamientos de seguridad de la información, dando un manejo adecuado a la información y salvaguardando su confidencialidad.

4.4.1.3.3 Contactos con las autoridades

La oficina de gestión de recursos informáticos reconoce, identifica y establece contacto con las autoridades como Policía Judicial, CTI, en temas de informática forense y grupos especializados en seguridad de la información, para investigar los incidentes de seguridad de la información para determinar las responsabilidades civiles y penales.

Para mejorar el sistema de seguridad de la dependencia, el funcionario de la oficina de sistemas mantiene contacto con grupos de profesionales especializados, el programa presidencial Gobierno en Línea del Ministerio de las Tecnologías, las asociaciones de ingenieros especialistas en seguridad de la información, y foros especializados.

4.4.1.3.4 Revisión independiente de la seguridad de la información

La Auditoria es una actividad independiente y objetiva de asesoría que le permite medir a la empresa el grado de cumplimiento con el sistema de Gestión de Seguridad de la Información, para mantenerlo, controlarlo y operarlo conforme a las necesidades establecidas en las políticas del SGSI. Para verificar el cumplimiento del SGSI, se realizan dos actividades de auditoría en el año y cuando se requiera, se puede realizar revisiones totales o parciales al proceso, determinando los hallazgos no conformes y las observaciones con miras a la planificación de acciones correctivas.

Las auditorías internas son realizadas por funcionario o terceros que cumplan los requisitos establecidos, siguiendo los lineamientos de independencia, objetividad, libre de cualquier perjuicio o conflicto de intereses, y que no audite su propio trabajo.

4.4.1.3.5 Partes externas y coordinación de la seguridad de la información

La auditoría a los servicios que requieren tercerización de servicios permite establecer medidas de revisión y control en cada uno de los procesos relacionados al SGSI, con miras a determinar el grado de cumplimiento en seguridad, confianza, confidencialidad, integridad y disponibilidad de los servicios ofrecidos por la empresa. La oficina de gestión de recursos informáticos socializa las Políticas de Seguridad de la Información a través de sensibilizaciones y capacitaciones con las partes externas, en los procesos relacionados al SGSI. Para conocer el grado de alineación existente entre el SGSI y partes externas se realiza auditoria de control a dichos servicios. Permitiendo generar el mapa de riesgos con sus objetivos de control y controles relacionados.

4.4.1.4 Gestión de Activos

Todos los activos, de la oficina de gestión de recursos informáticos están claramente identificados, plaquetiados, rotulados y asignados al responsable de la oficina.

El conocimiento, uso y propiedad de los activos de información en la dependencia, le permite generar valor agregado a la administración efectuando, control y protección a sus procesos, contando con el pleno conocimiento de lo que la dependencia posee para el desarrollo de su gestión administrativa, evitando así el

incumplimiento de responsabilidades, la violación a los derechos de autor y de las responsabilidades derivadas por la pérdida o daño de los mismos.

El profesional de sistemas es el responsable de clasificar, elaborar y mantener actualizado un inventario de activos de información, con el fin de garantizar la disponibilidad, integridad y confidencialidad de estos. Que permita fácilmente ser identificado en serie, nombre, fecha de inventario, versión (software).

El archivo de la oficina de gestión de recursos informática está organizado conforme con el sistema general de archivo (ley 594 de 2000), y se encuentra actualizado, plenamente etiquetado y almacenado.

4.4.1.4.1 Clasificación de la Información

La información es uno de los activos más importantes que tiene la oficina de gestión de recursos informáticos. El proceso de Clasificación le permite consolidar su buen nombre con terceros, proveedores y clientes, por el manejo seguro que le hace a su información pues tal acción permite demostrar el cumplimiento de regulaciones internas y gubernamentales. La información se clasifica de acuerdo a su importancia, a su valor, al dueño, al custodio y a los usuarios de la misma.

El profesional de sistemas aprueba la clasificación de la información en términos de su valor, requisitos legales sensibilidad e importancia de la información para la empresa así.

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.20

[20] Ley 1712 de 2014, recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 de 2014.[21]

Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la ley 1712 de 2014.[22]

4.4.1.4.2 Etiquetado y manejo de Información

De acuerdo al procedimiento de la oficina de gestión de recursos informáticos se realiza bajo el esquema del Sistema de Información Documental que clasifica su nivel de confidencialidad acorde con las tablas de retención documental y la Ley 594 del 2000.

4.4.1.5 Seguridad de los recursos humanos

Con el fin de crear un ambiente laboral que garantice un adecuado manejo de los activos de información, desde la oficina de gestión de recursos informáticos se gestionó el principio según el cual, todos los funcionarios, contratistas y terceros son responsables de conocer y aplicar las políticas de seguridad de la información.

[21] Ley 1712 de 2014, recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882
[22] Ley 1712 de 2014, recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882

Todos los funcionarios deben velar por la protección y buen uso de los activos de información de la empresa, informando oportunamente los incidentes de seguridad que afecten la seguridad de la información.

4.4.1.5.1 Roles y Responsabilidades

Se gestionó desde la dependencia la inclusión en el manual de funciones de la entidad, las funciones y responsabilidades sobre el uso y manejo seguro de la información para los cargos de la dependencia.

4.4.1.5.2 Selección del personal

Para el cargo de profesional universitario de la oficina de gestión de recursos informáticos se establece los criterios de selección de personal, en remplazo en caso tal que el profesional tenga que ausentarse de su cargo, en donde se define el perfil para el cargo respectivo en cuanto a experiencia, formación y educación.

Para los contratos de prestación de servicios profesionales y de apoyo a la gestión, la selección del contratista se realizara teniendo en cuenta los requisitos de idoneidad y experiencia para la prestación del servicio, en cuanto a procesos de suministro de tecnología esta se realizar por el los modelos de contratación establecidos en el decreto 1082 de 205.

4.4.1.5.3 Formación y concientización sobre la seguridad de la información

Los funcionarios y de ser necesario el personal contratista de la oficina de gestión de recursos informáticos, recibirán formación adecuada, para el cumplimiento de sus funciones y responsabilidades con el Sistema de Gestión de Seguridad de la Información. Esta contempla los requisitos de seguridad, responsabilidades

legales, el correcto uso de los recursos, entre otros, de igual manera la socialización se extiende al resto de funcionarios de la entidad.

Los programas de formación y concienciación se desarrollaran de acuerdo al plan integral de capacitación de la entidad en las funciones, responsabilidades y habilidades de los funcionarios.

4.4.1.5.4 Proceso disciplinario

En el momento de presentarse un incidente de seguridad, el profesional universitario del área de sistemas, iniciaría la correspondiente indagación preliminar a fin de establecer la veracidad de los hechos y definir las acciones a que haya lugar, teniendo en cuenta la gravedad del incidente y su impacto en la dependencia.

4.4.1.5.5 Devolución de activos

Al momento del retiro de funcionario de la entidad, este mismo debe devolver los todos sus activos de información, para así ser descargados del archivo de activos, retirando los accesos físicos y lógicos, como requisito para la firma de paz y salvos, lo anterior se gestiona desde la dependencia de almacén.

4.4.1.6 Seguridad física y del entorno.

4.4.1.6.1 Perímetro de seguridad física

La oficina de gestión de recursos informáticos ha definido en su espacio físico, áreas que contiene información y servicios que procesan información como seguras utilizando perímetros modulares para controlar el acceso de personal no autorizado, señalizándolos visiblemente.

4.4.1.6.2 Control de Acceso Físico

La dependencia tiene definido los mecanismos para el control de acceso físico a los diferentes rack de telecomunicaciones, donde se procese o almacene información sensible, al igual que donde se encuentren equipos e infraestructura de comunicaciones, permitiendo el ingreso únicamente a personal autorizado y debidamente identificado.

4.4.1.6.3 Seguridad de Oficinas, Recintos e Instalaciones

Durante las horas en las que no se labora, la entidad ha contratado el servicio de vigilancia, proceso que se lleva a cabo mediante detectores de movimiento y monitoreo del sistema de cámaras instaladas en las diferentes lugares específicos de la contraloría, el sistema cuenta con línea de comunicación directa con el servicio de vigilancia en caso de que se presente alguna anomalía.

4.4.1.6.4 Protección contra amenazas externas y ambientales

La entidad tiene contratado con la empresa aseguradora de riesgos profesionales POSITIVA para identificar las amenazas físicas y naturales a las que está expuesta la contraloría incluida la dependencia de gestión de recursos informáticos. De igual forma la empresa ha contratado pólizas de aseguramiento con la compañía LA PREVISORA contra todo riesgo para empleados, instalaciones, riesgos a terceros, bienes y personal en caso de accidentes laborales.

Se redactó un informe de riesgos y amenazas con el fin de gestionar capacitación para los empleados en el manejo de tales riesgos y amenazas. Se realiza

periódicamente sesiones de capacitación con la aseguradora y entidades como el Cuerpo de Bomberos y la defensa civil así como la realización de simulacros de evacuación.

4.4.1.6.5 Seguridad de los Equipos

Los equipos que pertenecen a la infraestructura de tecnología de Información de la dependencia y la entidad, tales como computadores, servidores, equipos de comunicaciones, cableado de energía eléctrica y comunicaciones, UPS, planta telefónica, dispositivos de almacenamiento y demás que sirven como soporte de la información de la empresa, están ubicados y protegidos minimizando los riesgos por pérdida, daño, robo, accesos no autorizados o interrupción de las actividades. Igualmente se cuenta con pólizas de seguro contra ambientales tales como las producidas por agua, fuego, explosivos.

La empresa se asegura que la infraestructura de servicios de Tecnologías de información este protegida contra fallas en el suministro de energía y demás anomalías relacionadas con ésta, implementando un sistema de alimentación ininterrumpida (UPS) de manera individual que garantice el funcionamiento continuo de los sistemas computacionales que así lo requiera.

No está permitido consumir alimentos, beber o fumar en el puesto de trabajo.

4.4.1.6.6 Mantenimiento de equipos

El profesional universitario de la dependencia es quien en primeria instancia realiza mantenimiento correctivo, preventivo y adaptativo de la infraestructura tecnológica instalada. En segunda instancia y cuando así lo amerite, la entidad terceriza el servicio de mantenimiento continuo y adecuado de equipos mediante contrato de prestación de este servicio con una empresa idónea que asegura la

continua disponibilidad e integridad de los mismos, de igual manera de manera general por cada vigencia se realiza la contratación del mantenimiento preventivo y correctivo de equipos de cómputo.

4.4.1.6.7 Seguridad de los Equipos Fuera de las Instalaciones y Retiro de Activos

Los equipos o software no se retiran de las instalaciones de la Contraloría Departamental del Meta, sin previa autorización del profesional de sistemas, secretaria general y almacenista, informando sus fines y razones de salida con registro escrito teniendo en cuenta que estos no pueden quedar desatendidos en lugares públicos, deben tener las medidas de seguridad necesarias para ser transportados.

La persona responsable del retiro de equipos asegura que en todo momento éstos están continuamente vigilados, controlados y manipulados por personal autorizado, manteniendo las medidas de seguridad necesarias para ser transportados evitando robo y daño.

En caso de robo o pérdida, se deberá reportar profesional de sistemas, secretaria general y almacenista e instaurar la respectiva denuncia ante la autoridad competente.

Los equipos portátiles se deben llevar como equipaje de mano y camuflado cuando sea posible, durante los viajes y todas las precauciones necesarias a fin de garantizar la confidencialidad, integridad y disponibilidad de los activos de información.

En caso de dar de baja un equipo, se asegura que se haya realizado borrado seguro de información y software licenciado en los medios de almacenamiento.

4.4.1.7 Gestión de operaciones y comunicaciones

4.4.1.7.1 Documentación de los Procedimientos de Operación

Los procedimientos operativos relacionados con los servicios de comunicaciones y procesamiento de la información de la oficina de gestión de recursos informáticos, se mantendrán documentados, actualizados y disponibles con el fin de garantizar el correcto funcionamiento de la plataforma tecnológica.

4.4.1.7.2 Gestión del Cambio

El profesional universitario de la oficina de gestión de recursos informáticos controla los cambios en los servicios y los sistemas de procesamiento de la información, evaluando aspectos técnicos y de seguridad, y verifica su correcta implementación.

4.4.1.7.3 Gestión de la Capacidad del Sistema

A través de la dependencia de sistemas se realiza seguimiento y evaluación a la infraestructura tecnológica a fin de identificar el uso de los recursos, su proyección o escalabilidad. Permitiendo adquirir nuevos recursos de ser necesario una vez identificadas las necesidades, para asegurar el óptimo desempeño del sistema.

4.4.1.7.4 Aceptación del sistema

La oficina de gestión de recursos informáticos tiene definido el protocolo de implementación de sistemas de información nuevos, actualizaciones o nuevas versiones ejecutando pruebas suficientes para la aceptación antes de su integración.

4.4.1.7.5 Protección Contra Códigos Maliciosos y Móviles

La oficina de gestión de recursos informáticos para la protección de la infraestructura tecnológica, ha implementado software de seguridad, como antivirus, antispam, antispyware, debidamente licenciado para proteger su plataforma tecnológica de códigos maliciosos y móviles no autorizados. También realiza actividades para concientización de los empleados sobre estas amenazas.

Desde la dependencia se autoriza el uso de estas herramientas y garantiza que éstas no sean deshabilitadas, al igual que su actualización permanente.

No está permitido sin la autorización de la dependencia de Sistemas, desinstalar o deshabilitar las herramientas de seguridad que provee la empresa, ni el uso de código móvil ni el ingreso de tecnología móvil a la red de datos, para generar, compilar, propagar, ejecutar o introducir código de programación que este diseñado para producir daño a la infraestructura tecnológica o su rendimiento.

4.4.1.7.6 Copias de Respaldo

Desde la dependencia se ha definido en el procedimiento de generación de copias de seguridad de la información para el desarrollo de las actividades misionales de la empresa, contenida en medios tecnológicos. Será almacenada periódicamente de forma que se asegure su identificación, protección, integridad y disponibilidad. Igualmente se cuenta con un plan de recuperación de copias de seguridad, que permite actuar en caso de que ocurra alguna falla o error.

Cada funcionario al momento de la terminación de la relación laboral con la entidad independiente del tipo de contratación deberá entregar copia de seguridad de la información generada en la realización de sus funciones, como requisito para

la expedición de paz y salvo de la oficina de sistema y posterior liquidación de su contrato.

Este procedimiento aplica para salvaguarda de la información en la Contraloría Departamental del Meta.

El procedimiento definido para la generación de copias de seguridad se establece a continuación:

- Se identifica las bases de datos, aplicativos del sistema información de gestión de los funcionarios de lo cual se requiere de copias de seguridad
- El respaldo se información se efectuará en el medio disponible en la empresa DVD, Discos duros externos, CD o Blu-Ray.
- Se realizan copias de seguridad incremental diaria de aquella información que se actualiza frecuentemente y de alto valor para la institución, a las 10:00 p.m en formato comprimido.
- Se realizan copias de seguridad mensual de la configuración de servidor, de los respaldos incrementales diarios y de la información de gestión de los funcionarios
- Los respaldos mensuales se conservan por los menos dos años.
- Se conserva una copia del último mes de cada año como históricos.
- Se realiza cada seis meses simulación de recuperación de las copias de seguridad.
- Todas las copias de seguridad serán etiquetadas con las siguientes especificaciones: tipo de copia (mensual, diaria), rango de la copia . Se debe especificar el contenido (Logs, scripts de configuración, bitácoras, datos).
- Se realiza las pruebas de funcionalidad a las copias de seguridad.

- Se hace registro de estas acciones en el formato de registro de generación de copias de seguridad que contiene; código de la copia, nombre de la copia, responsable, lugar de archivo, medio de archivo, tiempo de archivo y disposición. Permitiendo así la trazabilidad de los registros de copias de seguridad.

4.4.1.8 Manejo de Medios

El uso de medios de almacenamiento removibles tales como CDs, DVDs, memorias usb, discos duros externos, entre otros, en la infraestructura tecnológica de la empresa, se autoriza para aquellos empleados que lo requieran de acuerdo al cumplimiento de sus funciones.

Los funcionarios de las otras dependencias deben asegurar física y lógicamente los dispositivos con el fin de no poner en riesgo la disponibilidad, integridad, y confidencialidad de la información.

4.4.1.8.1 Uso de Internet

Desde la oficina de gestión de recursos informáticos se proporciona el servicio de internet, con el fin de mejorar el rendimiento y eficiencia en las actividades que se realizan, encaminadas al cumplimiento de la misión y la visión institucional.

El uso de esta herramienta debe hacerse de manera responsable, ética, no abusiva, sin afectar la productividad de la empresa, sin atentar contra las leyes vigentes y sin poner en riesgo la confidencialidad, integridad y disponibilidad de la plataforma tecnológica.

No está permitido desde la red interna el acceso a páginas con contenido que atente contra la moral, la ética, los lineamientos de seguridad y la normatividad vigente.

El servicio de internet está destinado a fines laborales, haciendo buen uso del mismo, por lo cual no se permite el ingreso a páginas poco fiables, descargas de juegos, música, vídeos, aplicaciones, programas y demás que afecte la gestión de la red.

Si de alguna manera se ve afectado el ancho de banda, la velocidad y perjudicada la red por virus será necesario el registro de sitios visitados por los funcionarios, donde ellos serán avisados de tal situación, para su posterior tratamiento e investigación a que diere lugar.

4.4.1.8.2 Uso del Correo electrónico

El correo electrónico es una herramienta que agiliza los trámites, cuida el medio ambiente al eliminar la papelería utilizada para fines de distribución, conocimiento y asegura su confidencialidad, integridad y disponibilidad, permitiendo almacenar los testigos de recibido y lectura, asegurando que las personas de interés estén informadas a un mínimo costo.

Desde la oficina de gestión de recursos informáticos, se proporciona a los líderes de proceso, cuentas de correo electrónico institucionales con el fin de consolidar la imagen institucional y el sentido de pertenencia. Para lo cual debe dársele un uso racional, responsable, ético y acorde con las funciones desempeñadas.

El usuario debe cambiar periódicamente la contraseña, la cual debe tener como mínimo seis caracteres alfanuméricos.

Es responsabilidad del funcionario, el uso y manejo de la cuenta de correo y así como la privacidad de la contraseña.

Las solicitudes de información de la dependencia deben realizarse única y exclusivamente desde la cuenta del correo institucional, no está permitido realizar envío de información institucional desde cuentas de correo personales.

La cuenta de correo institucional solo podrá ser utilizar para fines laborales, por tanto el envío de correo masivo, mensajes de contenido religioso, político, propagandístico o que afecte la sensibilidad o reputación de las personas y quede entredicho el buen nombre de la entidad, queda prohibido y se hará la respectiva investigación a que diera lugar.

En caso de requerir el envío de correos masivos, archivos de música y videos es necesaria la autorización del profesional de sistemas.

4.4.1.8.3 Uso de los recursos tecnológicos

La instalación y configuración de software y hardware está a cargo del profesional universitario de Sistemas. Los usuarios no se encuentran facultados para realizar este tipo de actividades.

El profesional universitario de Sistemas debe revisar y mantener de manera periódica las aplicaciones instaladas a fin de verificar el licenciamiento de las mismas.

4.4.1.8.4 Monitoreo del Uso de los Sistemas

El profesional universitario de Sistemas debe asegurar que se generan los registros de eventos de las aplicaciones que hacen parte de la plataforma

tecnológica, con el fin de identificar usos no autorizados e incidentes de seguridad de la información.

El monitoreo y revisión de estos registros (Logs) se realizan de acuerdo al nivel de riesgos a los cuales está expuesta la plataforma tecnológica de la entidad.

4.4.1.9 Control de Acceso

4.4.1.9.1 Política de Control de Acceso Lógico

La oficina de gestión de recursos informáticos, define que para el acceso a la plataforma tecnológica o algunos de sus componentes o aplicaciones, todos los usuarios deben estar identificados y autorizados por el profesional de gestión de recursos informáticos, previa solicitud del profesional del talento humano, quien es el encargado de llevar los controles pertinentes. La identificación única de los usuarios, permite que queden vinculados y sean responsables de sus acciones.

4.4.1.9.2 Gestión de Usuarios

Para el control de los usuarios, la oficina de gestión de recursos informáticos, establece un procedimiento para la alta, modificación y baja de usuarios en los sistemas, con el objeto de permitir el acceso a usuarios nuevos o que han cambiado de funciones y denegar el acceso a usuarios que han dejado la entidad o han cambiado de dependencias.

La dependencia encargada de realizar estos cambios, de acuerdo a las solicitudes realizadas por el responsable de cada dependencia.

4.4.1.9.3 Gestión de Contraseñas para Usuarios

Desde la oficina de gestión de recursos informáticos se realiza la gestión para que los funcionarios tengan acceso a la plataforma tecnológica, donde deben tener asignado un usuario y contraseña para el uso de los recursos y aplicativos, teniendo en cuenta que las contraseñas deben tener un manejo confidencial.

Los funcionarios deben aplicar buenas prácticas de seguridad en la selección y uso de las contraseñas.

4.4.1.9.4 Equipo Desatendido, Escritorio y Pantalla Despejada.

Para la oficina de gestión de recursos informáticos, es muy importante el buen manejo de la información tanto digital como física y teniendo en cuenta que los procesos misionales el cual maneja información de los presuntos responsables fiscales, razón por la cual la entidad es visitada frecuentemente por personal de la ciudadanía, entes de control y proveedores, se requiere tener especial cuidado y atención con la información de carácter confidencial y restringido.

Es responsabilidad de todos los funcionarios, que tengan asignado un equipo de cómputo, bloquear la sesión de su equipo cuando se ausente de su puesto de trabajo y se reactivará ingresando la contraseña del usuario. Al terminar la jornada laboral se deben cerrar las aplicaciones y apagar los equipos de cómputo de manera adecuada.

La información sensible que se encuentre en papel o en medios magnéticos debe ser protegida y no dejarse a la vista, especialmente cuando no se esté utilizando, para lo cual debe asegurarse bajo llave en gabinetes u otros sitios seguros.

Los documentos confidenciales o restringidos que se envíen a las impresoras, deben retirarse inmediatamente.

4.4.1.9.5 Separación de las Redes e Identificación de los Equipos

La plataforma tecnológica bajo supervisión de la oficina de gestión de recursos informáticos, se encuentra separada de otras redes de datos que prestan servicios a la comunidad en general.

Los equipos que se conecten a la plataforma tecnológica están identificados y autorizados por el profesional universitario de sistemas, el cual establece los controles pertinentes.

4.4.1.9.6 Adquisición de Sistemas de Información

La oficina de gestión de recursos informáticos, adelanta la contratación para la adquisición de productos tecnológicos necesarios para el desarrollo y mantenimiento de la plataforma tecnológica, evaluando las características técnicas, definiendo acuerdos sobre licencias de uso, propiedad de los códigos y derechos de propiedad intelectual.

Antes de poner en funcionamiento las aplicaciones, se realizan pruebas para detectar fallos que puedan atentar contra la seguridad de la información de la empresa.

4.4.1.10 Gestión de los incidentes de seguridad de la información

4.4.1.10.1 Reporte de Eventos o Incidentes

Es deber de todos los funcionarios, reportar a la oficina de Sistemas toda situación que genere un evento o incidente de seguridad que atente contra el normal desarrollo de las actividades de la empresa, allí se evaluará la situación y dará el tratamiento requerido.

Desde la secretaría general se reportará las situaciones ante las autoridades competentes cuando haya implicaciones legales ya sean penales o civiles.

4.4.1.10.2 Manejo de Incidentes de Seguridad

Los incidentes de seguridad, deben ser registrados en documento físico o digital indicando el tipo de incidencia, fecha y hora de la incidencia, fecha de reporte, persona que realiza el reporte, persona a quien comunica la incidencia, descripción detallada de la incidencia, efectos y posibles consecuencias, acciones adoptadas para subsanar las consecuencias.

El profesional de sistemas será el responsable de evaluar el incidente o designar el personal idóneo para realizar estas funciones. Para el desarrollo de estas labores puede requerirse el apoyo de otras dependencias o empresas externas.

Una situación donde se presente un incidente o evento de seguridad permite identificar oportunidades de mejora y aprender de estos fallos.

4.4.1.11 Gestión de la continuidad del negocio

La oficina de gestión de recursos informáticos contará con un plan de continuidad de las actividades más críticas, que permita reanudar sus actividades ante la presencia de interrupciones prolongadas en la prestación de los servicios, ya sea por fallos o desastres naturales.

De acuerdo al análisis de riesgos, se identificarán los eventos con alto impacto en la dependencia, probabilidad de ocurrencia y sus consecuencias. Para implementar planes que permitan reanudar las actividades.

Los planes deberán estar documentados, probados, actualizados de acuerdo con las características de la empresa y deben ser de conocimiento de los empleados, de tal manera que sean conscientes de sus roles y responsabilidades.

4.4.1.12 Cumplimiento

La oficina de gestión de recursos informáticos debe cumplir con el marco normativo Colombiano y para ello la dependencia identifica los requerimientos normativos aplicables y contractuales pertinentes para los sistemas de información.

La dependencia propenderá por el cumplimiento de los derechos de propiedad intelectual y sobre el uso de productos de software patentados, y realizará revisiones periódicas a fin de que se cumpla esta reglamentación.

Hace parte de los derechos de propiedad Intelectual, la información que se genere como propia del conocimiento de la dependencia, códigos fuente.

El profesional universitario de sistemas es el encargado de velar por la correcta aplicación y control de las licencias de productos de software y hardware, así como el número de usuarios permitidos. Está prohibido el uso de productos ilegales o sin licencia.

La dependencia tiene definidos acuerdos contractuales con los proveedores que realizan arrendamiento de software, donde se señalan los acuerdos de protección de la propiedad intelectual.

Es deber de todos los funcionarios velar por el buen manejo y protección de los datos e información personal, de la cual puedan tener conocimiento por el ejercicio de sus funciones.

5. DIVULGACIÓN

El presente proyecto se dará a conocer a la comunidad académica por los medios dispuestos por la UNAD con el fin de presentar el desarrollo y resultados obtenidos de este.

Actualmente la UNAD cuenta con repositorios, en su biblioteca Bibliotecas, la cual es la herramienta que se usará para la divulgación.

6. CONCLUSIONES

Día a día se ve reflejado como las TIC, hacen parte fundamental del diario vivir de cualquier organización, en procesos que involucran la satisfacción a los usuarios, mejorar la prestación de sus servicios, y en el caso de las entidades del estado, reflejar transparencia, igualdad, equidad y participación ciudadana, no obstante el uso de las TIC por las entidades trae inmerso riesgos y exposiciones de seguridad que la mayoría de las veces, las desconocen la parte directiva ocasionando que no se fijen presupuesto para proteger la información.

El desarrollo de esta investigación permitió conocer los beneficios que incorpora un sistema de gestión de seguridad de la información para el área de sistemas de la Contraloría Departamental del Meta, además de gestionar los riesgos basados en la metodología MAGERIT y aplicación de la ISO/IEC 27001:2013, que mediante el ciclo PHVA o mejoramiento continuo y en su fase de diseño se pudo establecer la documentación base de aplicación de la norma; aunado a lo anterior ya inmersos en desarrollo del proyecto, se pudo conocer los dominios controles y objetivos de control del anexo A mediante un análisis diferencial, se pudo diseñar políticas de seguridad generales involucrando a la parte directiva de la entidad.

Siguiendo con el diseño del sistema de gestión de seguridad de la información, se logró realizar la clasificación delos activos de información determinando el nivel de riesgo de cada uno de ellos resultado de la aplicación de la metodología MAGERIT.

Dentro de las vulnerabilidades encontradas, se presenta que no hay un control de acceso efectivo de manera física para ingresar al rack principal y la entidad, en razón a que no se cuenta con servicio de vigilancia y las chapas de las puertas no se encuentran en funcionamiento

En conclusión de manera general se determina que el diseño de un SGSI en el área de sistemas de la Contraloría Departamental del Meta, genera beneficios a largo plazo, lo que garantiza el cumplimiento de la gestión de la entidad y aquellos procesos que trabajan por la protección de la información y los activos relacionados. Contribuyendo para fortalecer la continuidad del negocio.

7. RECOMENDACIONES

El desarrollo del presente proyecto para que obtenga lo beneficios y resultados reales, se recomienda el total compromiso de parte directiva de la Contraloría Departamental del Meta, y no como un simple impulso y gestión del profesional universitario del área recursos informáticos, si no que involucre a los diferentes procesos como planeación y comunicaciones, despacho del contralor, secretaría general y funcionaros de toda la entidad y de esta manera alinear los objetivos TI con los de la entidad.

Así mismo se recomienda realizar jornadas de capacitación y sensibilización sobre temas de seguridad de la información más precisamente sobre la implementación de un SGSI, además de ubicar las políticas en una parte pública para que cualquier persona en la entidad pueda acceder a ellas sin ningún inconveniente.

Por otra parte, el diseño de un SGSI no debe quedar en la fase de diseño, siguiendo el ciclo de mejora continua, la entidad tiene que continuar con la etapa de implementación, para después completar el ciclo y de esta manera gestionar todos los riesgos a los que está expuesta la dependencia de sistemas en todos sus activos.

BIBLIOGRAFÍA

UNAD, Repositorio Institucional Unad, Recuperado de: http://repository.unad.edu.co/simple-search?query=seguridad+informatica Portal ISO, (2005), Recuperado de: http://www.iso27000.es/sgsi.html

INTECO, Instituto Nacional de Tecnología de la Comunicación. España. [Online]. Disponible en: http://www.inteco.es/Formacion/SGSI/Conceptos_Basicos/Modelos_PDCA_SGSI/

CONTRERAS N. (2011). Enfoque de la Seguridad de la Información, Instituto Tecnológico Nacional de Argentina.

UNAD, Repositorio Institucional Unad, Recuperado de:

http://repository.unad.edu.co/simple-search?query=seguridad+informatica

UGAS, L. (2002). Seguridad en organizaciones con tecnologías de información. Telématique: Revista Electrónica de estudios Telemáticos: Vol. 1 (1), pp. 1-9. Base de datos eUreka.

MIERES. Jorge, Ataques Informáticos debilidades de seguridad comúnmente explotadas (2009), Recuperado de: https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS DE ESPAÑA. MAGERIT versión 3 (idioma español): Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. 2012. Libro I, II y III.

SUÁREZ SIERRA, Lorena. Guía Integradora de la asignatura Sistema de Gestión de Seguridad Informática. UNAD - Especialización en Seguridad Informática. 2015. 10 p.

SUAREZ, L. Modulo Sistema de Gestión de la Seguridad de la Información SGSI, Universidad Nacional Abierta y a Distancia UNAD , 2013.

PORTAL DE ADMINISTRACIÓN ELECTRÓNICA - MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS DE ESPAÑA - SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS. Artículo: MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VSxjRvBx6U1.

ANEXO A IDENTIFICACIÓN Y DETERMINACIÓN ANÁLISIS Y GESTIÓN DE RIESGOS

IDENTIFICACIÓN Y DETERMINACIÓN ANÁLISIS Y GESTIÓN DE RIESGOS DE CONTRALORÍA DEPARTAMENTAL DEL META.

Valoración Cualitativa de los Activos

Para realizar la valoración de los activos se tuvo en cuenta que no a todos se les debe generar el mismo peso, toda vez que cada uno cumple un función diferente y el riesgo de amenaza varía en razón de la misma, por lo tanto el impacto ante la materialización de una amenaza es diferente, se realizar la valoración cuantitativa en razón de las cinco dimensiones confiabilidad, integridad, autenticidad, disponibilidad y trazabilidad de acuerdo a la siguiente tabla:

Tabla 4. Criterios de valoración

Valor		Criterio
10	Extremo	Daño Extremadamente Grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Efectos prácticos

Fuente:Tomado del Magerit V3 libro 2 Catalogo de elementos

De acuerdo al activo se le asignan unas dimensiones que sirven para darle un valor de acuerdo a las consecuencias frente a la materialización de amenazas.

Tabla 5. Dimensiones Activos

Dimensión	Código
Disponibilidad	D
Integridad	I
Confidencialidad	C
Autenticidad	A
Trazabilidad	T

Fuente: El autor

Valoración Cualitativa Servicios

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimensión				
				C	I	A	D	T
[www]	world wide web	[S_Internet]	Servicio de internet para los funcionarios	6	6	6		
[email]	Correo electrónico	[S_correo]	Gestión de cuentas de correos electrónicos	6	6	7		
[int]	interno (a usuarios de la propia organización)	[S_U_soporte]	Asistencia informática a los funcionarios de la entidad.	6	6	6		
[anon]	anónimo (sin requerir identificación del usuario)	[S_U_página_web]	Servicio de mantenimiento de la página web.			6	7	
[int]	interno (a usuarios de la propia organización)	[S_U_spark]	Servicio de mensajería Interna			5	7	

Valoración Cualitativa Datos/Información

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimension				
				C	I	A	D	T
[files]	Ficheros	[D_contratos]	Contratos suscritos con los proveedores	6	4	7		

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimension				
				C	I	A	D	T
[backup]	Copias de Respaldo	[D_Copias de Seguridad]	Archivo de Copias de seguridad de la información	5			5	

Valoración Cualitativa Aplicaciones Informáticas

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimension				
				C	I	A	D	T
[sub]	desarrollo a medida (subcontratado)	[A_Sysman]	Sistema de Información administrativo		6	6	7	
[std]	estándar (off the shelf)	[A_GLPI]	Sistema de Información para solicitar asistencia		5	5	6	
[av]	anti virus	[A_antivirus]	Bitdefender instalación en la nube.				6	

Valoración Cualitativa Equipos informáticos

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimension				
				C	I	A	D	T
[host]	Grandes equipos	[E_servidor]	Servidor de bases de datos, servidores de dominio e internet	6	6		6	
[pc]	informática personal	[E_computadores]	Computadores de la entidad	6	6		6	

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimension				
				C	I	A	D	T
[switch]	conmutadores	[E_switch]	Conmutadores de la entidad				5	
[pabx]	centralita telefónica	[E_planta]	Planta telefónica		5		5	
[print]	medios de impresión	[E_impresoras]	impresoras				5	

Valoración Cualitativa Soportes de Información

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimension				
				C	I	A	D	T
[disk]	discos	[S_copias]	Discos duro de respaldo de la información		6		6	

Valoración Cualitativa Redes de Comunicaciones

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimension				
				C	I	A	D	T
[LAN]	Red local	[R_lan]	Lan de la entidad				6	

Valoración Cualitativa Equipamiento Auxiliar

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimension				
				C	I	A	D	T

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimension				
				C	I	A	D	T
[Furniture]	Mobiliario	[M_mobiliario]	Muebles, estantes de la entidad.		5		6	

Valoración Cualitativa Instalación y Personas

Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Dimension				
				C	I	A	D	T
[local]	cuarto	B_rack	Rack de Comunicaciones		5		6	
[adm]	administradores de sistemas	B_sistemas	Profesional Universitario de Sistemas				6	
[prov]	proveedores	B_proveedores	Proveedores				6	

Identificación de Amenazas

Para realizar la identificación y valoración de amenazas se tiene en cuenta realiza la frecuencia con las que estas ocurren, las cinco dimensiones de seguridad que denota Magerit y la escala de rango porcentual de impactos en los activos.

Tabla 6 Escala de rango de frecuencia de amenazas

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	Se presentó en el último día	100

Vulnerabilidad	Rango	Valor
Frecuencia alta	Se presentó en la última Semana	70
Frecuencia media	Se presentó en el último més	50
Frecuencia baja	Se presentó en los últimos 6 meses	10
Frecuencia muy baja	No Se presentó en el último año.	5

Fuente: Tomada del módulo de sistemas de gestión de la seguridad informática

Tabla 7. Dimensiones de Seguridad

Dimensiones de Seguridad	Código
Confidencialidad	C
Autenticidad	A
Integridad	I
Disponibilidad	D
Trazabilidad	T

Fuente:El Autor

Tabla 8 Escala de rango porcentual de impactos en los activos para cada dimensión de seguridad.

Impacto	Valor Cuantitativo
Muy Alto	100%
Alto	70%
Medio	50%
Bajo	20%
Muy bajo	5%

Fuente: Tomada del módulo de sistemas de gestión de la seguridad informática

En la siguiente tabla se procede a identificar las amenazas para el inventario de activos realizado, de igual manera se identifica el impacto ante la materialización de la amenaza.

Tabla 9. Identificación amenazas e impacto

Nombre grupo de activo Magerit	Nombre activo de acuerdo a la empresa	Amenaza	Frecuencia de la Amenaza	Impacto para cada dimensión de seguridad %				
				C	I	A	D	T
World wide web	Servicio de internet para los funcionarios	Fallo de servicios de comunicaciones	**50**				**75%**	
		Caída del sistema por sobrecarga	**50**				**75%**	
		Desastres industriales	5				75%	
Correo electrónico	Gestión de cuentas de correos electrónicos	Errores de mantenimiento / actualización de programas (software)	5		20%		5%	
		Fuga de información	5	75 %				
interno (a usuarios de la propia organización)	Asistencia informática a los funcionarios de la entidad.	Indisponibilidad del personal	70		20%		75%	
		Ingeniería social	5	75 %				
anónimo (sin requerir identifica	Servicio de mantenimiento de la página	Denegación de servicio	10		50%		100%	5%
		Acceso no autorizado	5	75 %	50%	75%		

Nombre grupo de activo Magerit	Nombre activo de acuerdo a la empresa	Amenaza	Frecuencia de la Amenaza	Impacto para cada dimensión de seguridad %				
				C	I	A	D	T
ción del usuario)	web.	Fallo de servicios de comunicaciones	50				100%	
interno (a usuarios de la propia organización)	Servicio de mensajería Interna	Errores del administrador	50		50%		100%	
		Acceso no autorizado	5			75%		
		Fallo de servicios de comunicaciones	50				75%	
Ficheros	Contratos suscritos con los proveedores	Degradación de los soportes de almacenamiento de la información	5		50%		50%	
		Datos incompletos de los Usuarios	5		20%			20%
Copias de Respaldo	Archivo de Copias de seguridad de la información	Degradación de los soportes de almacenamiento de la información	5		20%		75%	
		Acceso no autorizado	5	20 %	20%	50%	20%	

Nombre grupo de activo Magerit	Nombre activo de acuerdo a la empresa	Amenaza	Frecuencia de la Amenaza	Impacto para cada dimensión de seguridad %				
				C	I	A	D	T
desarrollo a medida (subcontratado)	Sistema de Información administrativo	Acceso no autorizado	5	20 %	75%	100 %		20%
		Errores del administrador	50		50%		75%	
estándar (off the shelf)	Sistema de Información para solicitar asistencia	Errores del administrador	5		50%		75%	
		Acceso no autorizado	5	20 %	20%	50%	20%	
anti virus	Bitdefender instalación en la nube.	Errores del administrador	5		20%		50%	
Grandes equipos	Servidor de bases de datos, servidores de dominio e internet	Pérdida de equipos	5				100%	
		Corte del suministro eléctrico	50		50%		50%	
informática personal	Computadores de la entidad	Pérdida de equipos	5				100%	
		Corte del suministro eléctrico	50		50%		50%	
conmutadores	Conmutadores de la entidad	Fuego	5				20%	
		Pérdida de equipos	5				50%	

Nombre grupo de activo Magerit	Nombre activo de acuerdo a la empresa	Amenaza	Frecuencia de la Amenaza	Impacto para cada dimensión de seguridad %				
				C	I	A	D	T
centralita telefónica	Planta telefónica	Errores del administrador	5		20%		20%	
		Corte del suministro eléctrico	50		50%		50%	
medios de impresión	impresoras	Corte del suministro eléctrico	50		50%		50%	
		Pérdida de equipos	5				50%	
discos	Discos duro de respaldo de la información	Degradación de los soportes de almacenamiento de la información	5		50%		100%	
Red local	Lan de la entidad	Desastres naturales	5				50%	
Mobiliario	Muebles, estantes de la entidad.	Fuego	5				50%	
cuarto	Rack de Comunicaciones	Desastres naturales	5				50%	
		Fuego	5				50%	
administradores de sistemas	Profesional Universitario de Sistemas	Extorsión	5				50%	
		Ingeniería social	5				50%	

Nombre grupo de activo Magerit	Nombre activo de acuerdo a la empresa	Amenaza	Frecuencia de la Amenaza	Impacto para cada dimensión de seguridad %				
				C	I	A	D	T
proveedores	Proveedores	Extorsión	5				50%	
		Ingeniería social	5				50%	

De acuerdo a los resultados de la identificación de las amenazas y el impacto que tiene para la dependencia, la materialización de una de ellas y la frecuencia con la que ocurren, se decide a través de los siguientes controles mitigar las amenazas con alto riesgo como lo son:

- Fallo de servicios de comunicaciones
- Caída del sistema por sobrecarga
- Indisponibilidad del personal
- Errores del administrador

CONTROLES DE SEGURIDAD

Salvaguardas

Una vez se han identificado los activos de la entidad y las amenazas que estos representan a su seguridad, se definen salvaguardas con el fin de reducir el riesgo teniendo en cuenta los activos que se van a proteger.

Tabla 10. Clasificación Salvaguardas

Efecto	Tipo
Preventivas: reducen la probabilidad	[PR] preventivas [DR] disuasorias

Efecto	Tipo
	[EL] eliminatorias
Acotan la degradación	[IM] minimizadoras [CR] correctivas [RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización [DC] de detección [AW] de concienciación [AD] administrativas

Fuente: El Autor

Tipo de Activo	Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des Salvaguarda
Servicios	[www]	World wide web	[S_Internet]	Servicio de internet para los funcionarios	[MN] de monitorización	Registro de descarga
					[PR] preventivas	Políticas de seguridad
					[RC] recuperativas	Canal redundante
					[AW] de concienciación	Capacitación al personal en el manejo de la información.
					[AD] administrativas	Puesta en marcha

Tipo de Activo	Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des Salvaguarda
						del Plan Director
	[email]	Correo electrónico	[S_correo]	Gestión de cuentas de correos electrónicos	[MN] de monitorización	Registro de descarga
					[PR] preventivas	Políticas de seguridad
					[RC] recuperativas	Canal redundante
					[AW] de concienciación	Capacitación al personal en el manejo de la información.
					[AD] administrativas	Puesta en marcha del Plan Director
	[int]	interno (a usuarios de la propia organización)	[S_U_soporte]	Asistencia informática a los funcionarios de la entidad.	[PR] preventivas	Políticas de seguridad
					[RC] recuperativas	Canal redundante
					[AW] de concienciación	Capacitación al personal

Tipo de Activo	Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des Salvaguarda
						en el manejo de la información.
					[AD] administrativas	Puesta en marcha del Plan Director
	[anon]	anónimo (sin requerir identificación del usuario)	[S_U_página_web]	Servicio de mantenimiento de la página web.	[MN] de monitorización	Registro de descarga
					[PR] preventivas	Políticas de seguridad
					[RC] recuperativas	Canal redundante
					[AW] de concienciación	Capacitación al personal en el manejo de la información.
					[AD] administrativas	Puesta en marcha del Plan Director
	[int]	interno (a usuarios	[S_U_spark]	Servicio de mensajería	[MN] de monitorización	Registro de

Tipo de Activo	Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des Salvaguarda
		de la propia organización)		Interna		Accesos
					[PR] preventivas	Políticas de seguridad
					[RC] recuperativas	Canal redundante
					[AW] de concienciación	Capacitación al personal en el manejo de la información.
					[AD] administrativas	Puesta en marcha del Plan Director
Datos/Información	[files]	Ficheros	[D_contratos]	Contratos suscritos con los proveedores	[PR] preventivas	Políticas de seguridad
					[RC] recuperativas	Canal redundante
					[AW] de concienciación	Capacitación al personal en el manejo de la

Tipo de Activo	Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des Salvaguarda
						información.
					[AD] administrativas	Puesta en marcha del Plan Director
	[backup]	Copias de Respaldo	[D_Copias de Seguridad]	Archivo de Copias de seguridad de la información	[PR] preventivas	Políticas de seguridad
					[AW] de concienciación	Capacitación al personal en el manejo de la información.
					[AD] administrativas	Puesta en marcha del Plan Director
Aplicaciones Informáticas	[sub]	desarrollo a medida (subcontratado)	[A_Sysman]	Sistema de Información administrativo	[PR] preventivas	Políticas de seguridad
					[AW] de concienciación	Capacitación al personal en el manejo de la

Tipo de Activo	Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des Salvaguarda
						información.
					[RC] recuperativas	Copias de Seguridad
	[std]	estándar (off the shelf)	[A_GLPI]	Sistema de Información para solicitar asistencia	[PR] preventivas	Políticas de seguridad
					[AW] de concienciación	Capacitación al personal en el manejo de la información.
					[RC] recuperativas	Copias de Seguridad
	[av]	anti virus	[A_antivirus]	Bitdefender instalación en la nube.	[AW] de concienciación	Capacitación al personal en el manejo de la información.
					[MN] de monitorización	Registro de Uso y Descarga

Tipo de Activo	Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des Salvaguarda
					[EL] eliminatorias	Desistalar lincencias vencidas
					[PR] preventivas	Políticas de seguridad
Equipos informáticos	[host]	Grandes equipos	[E_servidor]	Servidor de bases de datos, servidores de dominio e internet	[PR] preventivas	Políticas de seguridad
					[AW] de concienciación	Capacitación al personal en el manejo de la información.
					[RC] recuperativas	Copias de Seguridad
	[pc]	informática personal	[E_computadores]	Computadores de la entidad	[PR] preventivas	Políticas de seguridad
					[AW] de concienciación	Capacitación al personal en el manejo de la

Tipo de Activo	Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des Salvaguarda
						información.
					[RC] recuperativas	Copias de Seguridad
	[switch]	conmutadores	[E_switch]	Conmutadores de la entidad	[PR] preventivas	Políticas de seguridad
					[AW] de concienciación	Capacitación al personal en el manejo de la información.
					[RC] recuperativas	Copias de Seguridad
	[pabx]	centralita telefónica	[E_planta]	Planta telefónica	[PR] preventivas	Políticas de seguridad
					[AW] de concienciación	Capacitación al personal en el manejo de la información.
					[RC] recuperativas	Copias de Seguridad

Tipo de Activo	Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des Salvaguarda
	[print]	medios de impresión	[E_impresoras]	impresoras	[PR] preventivas	Políticas de seguridad
					[AW] de concienciación	Capacitación al personal en el manejo de la información.
					[RC] recuperativas	Copias de Seguridad
Soportes de Información	[disk]	discos	[S_copias]	Discos duro de respaldo de la información	[PR] preventivas	Políticas de seguridad
					[AW] de concienciación	Capacitación al personal en el manejo de la información.
					[AD] administrativas	Puesta en marcha del Plan Director
Redes de Comunicaciones	[LAN]	Red local	[R_lan]	Lan de la entidad	[PR] preventivas	Políticas de seguridad

Tipo de Activo	Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des Salvaguarda
					[AW] de concienciación	Capacitación al personal en el manejo de la información.
					[AD] administrativas	Puesta en marcha del Plan Director
Equipamiento Auxiliar	[Furniture]	Mobiliario	[M_mobiliario]	Muebles, estantes de la entidad.	[PR] preventivas	Políticas de seguridad
					[AW] de concienciación	Capacitación al personal en el manejo de la información.
					[AD] administrativas	Puesta en marcha del Plan Director
Instalación y	[local]	cuarto	B_rack	Rack de Comunicaci	[DC] de detección	Detección de

Tipo de Activo	Código grupo de Activo Magerit	Nombre grupo de activo Magerit	Código Activo de acuerdo a la empresa	Nombre activo de acuerdo a la empresa	Tipo de Protección	Des Salvaguarda
Personas				ones		Incendios
	[adm]	administradores de sistemas	B_sistemas	Profesional Universitario de Sistemas	[AW] de concienciación	Capacitación al personal en el manejo de la información.
					[AD] administrativas	Puesta en marcha del Plan Director
	[prov]	proveedores	B_proveedores	Proveedores	[AW] de concienciación	Capacitación al personal en el manejo de la información.

Anexo B RESUMEN ANALÍTICO ESPECIALIZADO (RAE)

Título	DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL ÁREA DE RECURSOS INFORMÁTICOS DE LA CONTRALORÍA DEPARTAMENTAL DEL META, SEGÚN LA NORMA ISO 27001.
Autor	Cazaran Buitrago Olger Yonatan
Director	Romero Torres Mariano Esteban
Publicación	Villavicencio. Universidad Nacional Abierta y a Distancia, 2018.
Palabras Claves	Seguridad informática, gestión de riesgos, administración de riesgos, política de seguridad, sistema de gestión de seguridad de la información, valoración de amenazas, confidencialidad, integridad, disponibilidad, ISO 27001:2015 y auditorías.
Descripción	Monografía para optar el título de especialista en seguridad informática. La actual investigación se realiza con el objetivo de Analizar el Comportamiento del Cibercrimen en el municipio de Quibdó, departamento del Chocó.
Resumen	La oficina de Gestión de Recursos Informáticos, es la dependencia que se encarga de prestar el servicio de soporte TI, copias de seguridad, gestión de la navegación de internet, administración de los sistemas de información entre otros en la Contraloría Departamental del Meta, los cuales ayudan al normal funcionamiento de los procesos misionales, así mismo es el área que se encarga de velar por los activos informáticos y la seguridad de la información de la

	entidad. De esta manera al diseñar el SGSI, se pretende dejar fija bases para una futura implementación del SGSI en la dependencia, mediante el uso de las mejores prácticas de seguridad como la norma ISO/IEC 27001:2013 apoyado en la metodología de gestión de riesgos MAGERIT y de esta manera establecer un plan para la continuidad de los servicios.
Fuentes	UNAD, Repositorio Institucional Unad, Recuperado de: http://repository.unad.edu.co/simple-search?query=seguridad+informatica Portal ISO, (2005), Recuperado de: http://www.iso27000.es/sgsi.html SUÁREZ SIERRA, Lorena. Guía Integradora de la asignatura Sistema de Gestión de Seguridad Informática. UNAD - Especialización en Seguridad Informática. 2015. 10 p. PORTAL DE ADMINISTRACIÓN ELECTRÓNICA - MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS DE ESPAÑA - SECRETARÍA DE ESTADO DE ADMINISTRACIONES PÚBLICAS. Artículo: MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.VSxjRvBx6U1.
Objetivos	Objetivo General Diseñar un SGSI, que permita restar la probabilidad de ocurrencia y mitigar el impacto de los riesgos asociados con las vulnerabilidades y amenazas existentes en la oficina de gestión de recursos informáticos de la contraloría departamental del Meta.

	Objetivos Específicos Identificar los activos de información y las amenazas que puedan afectar la seguridad de los activos de la oficina de gestión de recursos informáticos. Realizar la evaluación de los riesgos informáticos existentes en la oficina de gestión de recursos informáticos de la contraloría departamental del Meta. Establecer controles que permita mitigar las causas que originan los riesgos. Definir políticas de seguridad que permitan minimizar los riesgos a los que están expuestos los activos de información de la oficina de recursos informáticos.
Metodología	El desarrollo del siguiente proyecto, se realiza con base en el tipo de investigación descriptiva, en razón a que ya se tiene conocimiento del problema, y se espera plantear un SGSI a través de las variables y requerimientos de la ISO/IEC 27001.
Recomendaciones	Total compromiso de parte directiva de la Contraloría Departamental del Meta, que se involucre a los diferentes procesos como planeación y comunicaciones, despacho del contralor, secretaría general y funcionaros de toda la entidad, así mismo realizar jornadas de sensiblización a todos los funcionarios de la entidad sobre temas de seguridad informática, con mirar a ampliar el alcance del SGSI. Implementar el SGSI el cual no debe quedar en la fase de planeación por el bien de la entidad.

Conclusiones	El desarrollo de esta investigación permitió conocer los beneficios que incorpora un sistema de gestión de seguridad de la información para el área de sistemas de la Contraloría Departamental del Meta, de igual manera se lograron evidenciar vulnerabilidades, efectos a la falta de controles de acceso físico para el rack principal y la entidad. Se realizó la clasificación los activos de la dependencia, y clasificación de acuerdo al impacto que generaría para la entidad frente a materialización de amenazas. El diseño de un SGSI en el área de sistemas de la Contraloría Departamental del Meta, genera beneficios a largo plazo, lo que garantiza el cumplimiento de la gestión de la entidad y aquellos procesos que trabajan por la protección de la información y los activos relacionados. Contribuyendo para fortalecer la continuidad del negocio.

Elaborado por	Cazaran Buitrago Olger Yonatan
Revisado por	Romero Torres Mariano Esteban

Fecha de Elaboración	27 de febrero de 2017