1. NOMBRE :

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN -SGSI- EN LA CONTRALORÍA GENERAL DEL MAGDALENA -CGM- BASADO EN LA NORMA ISO 27001 Y LA FASE DE PLANIFICACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION -MSPI- DE MINTIC

2. DURACIÓN ESTIMADA DEL PROYECTO:

El presente proyecto se realiza bajo el contexto de un período de prácticas profesionales como opción de grado en la CONTRALORIA GENERAL DEL DEPARTAMENTO DEL MAGDALENA, desarrollándose a lo largo de 5 de los 5 meses de la duración de las mismas, las cuales se encuentran estipuladas en el contrato realizado entre las partes a través del programa Estado Joven del Ministerio del Trabajo mediante la Caja de Compensación Familiar del Magdalena – CAJAMAG.

3. PRESENTACIÓN:

La Contraloría General del Magdalena nace mediante la Ordenanza No. 70 del 29 de Abril de 1926 expedida por la Asamblea Departamental, a través ésta ordenanza se expone la organización fiscal del departamento, dando origen a dos entidades complementarias y con funciones afines: “La Contraloría y La Contaduría”. Durante su existencia ha sufrido transformaciones importantes, destacándose la sufrida con la expedición de la Constitución Política de 1.991,

donde se le confiere a las contralorías territoriales el ejercicio del control fiscal sobre los entes territoriales y personas jurídicas o natural que manejen bienes y recursos del Estado. (CGM, 2018)

4. OBJETIVOS:

Objetivo General:

Diseñar la propuesta del Sistema de Gestión de Seguridad de la Información - SGSI – que permita salvaguardar la disponibilidad, confidencialidad e integridad de los activos de Información en la Contraloría General del Departamento del Magdalena

Objetivos Específicos:

I. Identificar los activos de información de la Contraloría General del Departamento del Magdalena
II. Identificar las vulnerabilidades y las amenazas que puedan afectar la seguridad de los activos existentes de la Contraloría General del Departamento del Magdalena.
III. Definir los roles y las responsabilidades para el sistema de gestión de seguridad de la información de la Contraloría General del Departamento del Magdalena.
IV. Definir políticas que permitan minimizar los riesgos a los que están expuestos los activos de información de la Contraloría General del Departamento del Magdalena
V. Establecer lineamientos o normas sobre el uso y las buenas prácticas de seguridad de la información para con los activos de la Contraloría General del Departamento del Magdalena

5. JUSTIFICACIÓN:

Teniendo en cuenta que la misión de la Contraloría General del Departamento del Magdalena es *"Ejercer control fiscal sobre las entidades y particulares administradores de los recursos públicos del departamento y sus municipios, garantizando la eficiencia y eficacia de la gestión pública, promoviendo la participación ciudadana en búsqueda de su propio bienestar"*, dicho control se lleva a cabo en su mayor parte en la revisión de gran cantidad de información de manera física y digital, recolectada o bien a través de sistemas de información o bien a través de las auditorías realizadas en cada uno de los municipios sujetos de control, esta información se convierte entonces en el activos más importante para la contraloría, de allí la necesidad de mantenerla protegida, salvaguardar su integridad y garantizar la disponibilidad, esta información digital y física, se convierte día a día en parte activa de la entidad en la toma de decisiones permitiendo alcanzar los objetivos enmarcados en el plan estratégico de la entidad, de allí la importancia de la implementación de un Sistema de Gestión de Seguridad de la Información, que propicie y facilite dicho respaldo en la Contraloría General del Departamento del Magdalena.

6. GENERALIDADES DE LA EMPRESA:

La Contraloría es una entidad de Carácter Técnico con autonomía administrativa y presupuestal. No Tendrá funciones distintas a las inherentes a su propia organización. El Control Fiscal es una función pública, la cual vigila la gestión fiscal de la administración y los particulares o entidades que manejen fondos o bienes de la Nación. La vigilancia del control fiscal del estado incluye el control financiero de gestión y resultados, fundando en la eficiencia, la economía, la equidad y la valoración de los costos ambientales. En los casos excepcionales, previstos por la ley, la contraloría podrá ejercer control posterior sobre las cuentas de cualquier entidad Territorial (Artículo 269 CP). La vigilancia de la gestión fiscal de los departamentos, distritos y municipios donde haya Contralorías corresponderá a éstas y se ejercerá en forma posterior y selectiva (Artículo 272 CP). (CGM, 2018)

MISION

Ejercer control fiscal sobre las entidades y los particulares administradores de los recursos públicos del departamento y sus municipios, garantizando la eficiencia y eficacia de la gestión pública, promoviendo la participación ciudadana en búsqueda de su propio bienestar. (CGM, 2018)

VISION

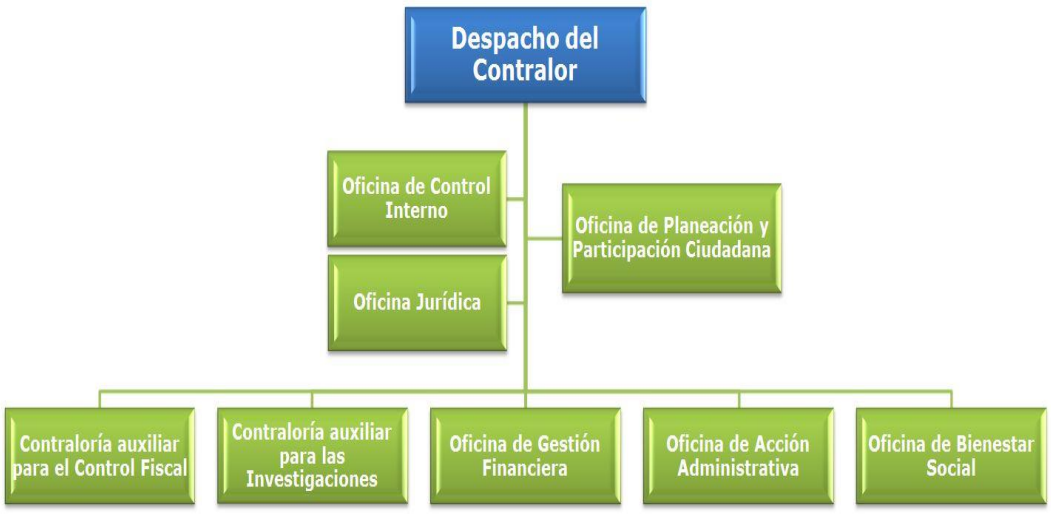
En el año 2019 la Contraloría General del Departamento del Magdalena será reconocida por ejercer control fiscal serio y transparente, por su modelo de gestión basado en la participación activa de sus ciudadanos, coadyuvando al mejoramiento integral de la administración pública territorial. (CGM, 2018)

CÓDIGO DE ÉTICA Y BUEN GOBIERNO

La Contraloría General del Departamento del Magdalena ejerce sus actividades con sujeción a los principios de Eficiencia, Eficacia, Economía, Equidad y Valoración de Costos Ambientales Establecidos en el Artículo 8 de la Ley 42 de 1993. (CGM, 2018)

ESTRUCTURA ORGANIZACIONAL Y PLANTA DE PERSONAL

En concordancia con lo dispuesto en la Ley 909 de 2.004 y la reglamentación complementaria establecida en los decretos leyes 770 y 785 de 2.005, la Contraloría General del Magdalena estableció su estructura organizacional y la planta de personal. La Entidad para sus actividades misionales, administrativas y operativas cuenta con las siguientes dependencias: Despacho del Contralor, Oficina Administrativa, Oficina Asesora de Control Interno, Oficina Jurídica y Jurisdicción Coactiva, Oficina de Control Fiscal y Oficina de Responsabilidad Fiscal. (CGM2, 2018)



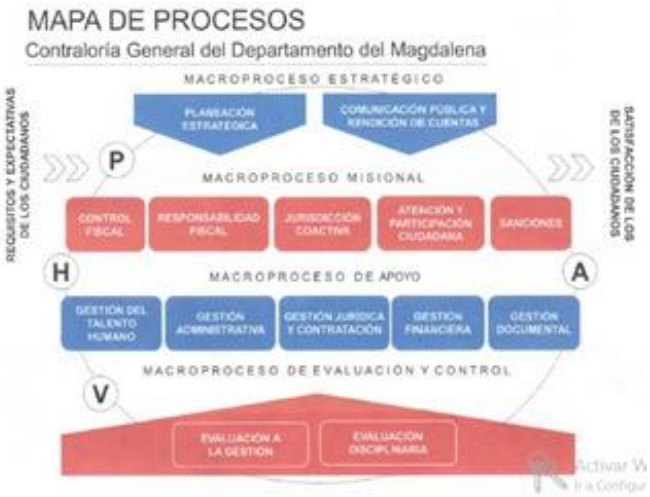
Estructura Organizacional

7. FUNCIONES DEL PRACTICANTE EN LA ORGANIZACIÓN:

1. Definir el alcance
2. Planeación de mecanismos de recolección de los activos de información.
3. Realizar la recolección de los activos de información.
4. Identificar las amenazas.
5. Identificar las vulnerabilidades
6. Definición de los roles y responsabilidades
7. Creación de políticas
8. Establecer lineamientos
9. Establecer controles

8. PROCESOS DE LA EMPRESA:

La Contraloría General del Departamento del Magdalena tiene su mapa de procesos que se presenta a continuación (CGM3, 2018) :



9. DIAGNÓSTICO:

La Contraloría General del Departamento del Magdalena es la entidad pública encargada de vigilar el presupuesto y la contratación de las entidades públicas sujetas de control del departamento del magdalena; esa vigilancia se hace mediante la recolección de información de manera física o digital en las auditorías realizadas en campo (salidas de comisión) y a través de las plataformas SIA observa y SIA contraloría, toda esta documentación se convierte en parte activa en el día a día de la entidad para cumplir con su misión en el control fiscal.

Teniendo en cuenta las amenazas y vulnerabilidades que pueden causar riesgo de pérdida o daño de los activos de información, lo cual implicaría desde perdida de dinero hasta sanciones judiciales y fiscales; de allí la importancia de que los funcionarios estén concientizados sobre el control de los equipos, medios y sistemas para el manejo de la información.

Teniendo en cuenta que entre sus objetivos estratégicos generales está el de innovar en la gestión fiscal, a través de la implementación de mecanismos, metodologías y sistemas de información soportados en tecnologías de la información haciendo uso de las Tics y las herramientas que ayuden a mantener la seguridad de los activos de información de la entidad se evidencia la necesidad de un Sistema de Gestión de Seguridad de la Información

10. PROPUESTA:

La propuesta consiste en diseñar un Sistema de Gestión de seguridad de la Información en su fase de planificación basado el norma ISO 27001 y las guías del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, donde la implementación y puesta en marcha quedara a disposición de la Contraloría General del Departamento del Magdalena todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información y contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital y así cumplir con las exigencia del Gobierno Nacional a través de sus programas de Gobierno en Línea del MinTIC.

11. CRONOGRAMA:

FASES	ACTIVIDAD	SEMANAS																		
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
FASE I	Definición del alcance y el compromiso de la directiva de la CGM																				
	Definición los roles y las responsabilidades																				
FASE II	Planeación y diseño de un mecanismo de recolección para los activos de información.																				
	Recolección de los activos de información en distintas oficinas de la CGM																				
FASE III	Identificar las amenazas existentes sobre los activos de																				

	información																		
	Identificar las vulnerabilidades de los activos de información																		
FASE IV	Diseño y creación de política general																		
	Diseño y creación de políticas especificas																		
	Establecimientos de los lineamientos de uso para las políticas																		
FASE V	Controles de seguridad para el sistema																		

12. IMPACTOS ESPERADOS

N°	Impactos
1	Se espera que el SGSI pueda ser implementado en su totalidad y pueda ayudar a la gestión de calidad y seguridad de la CGM
2	Se espera la eliminación completa de los errores humanos en el uso de los activos de información con la socialización de las políticas que generen buenas prácticas de seguridad
3	Generar confianzas entre funcionarios, entidades sujetas de control, entes de control y la sociedad de acuerdo al manejo de la información.

13. DESARROLLO DE LA PROPUESTA

DISEÑO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION BASADO EN LA ISO 270001 Y LA FASE DE PLANIFICACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION – MSPI – DE MINTIC PARA LA CONTRALORIA GENERAL DEL MAGDALENA

ESTABLECER EL SGSI

COMPROMISO DE LA DIRECCIÓN

La alta dirección de la **Contraloría General del Magdalena** (**CGM**) se compromete con la implementación, establecimiento, operación, monitorización, mantenimiento, revisión y mejora del **Sistema de Gestión de Seguridad de la Información** (**SGSI**). Para ello, se pueden llevar a cabo las siguientes iniciativas:

- Desarrollar una política de seguridad de la información.
- Garantizar el cumplimiento de planes y objetivos de Sistema de Gestión de Seguridad de la Información.
- Constituir roles y responsabilidades de seguridad de la información.
- Informar a la entidad la importancia de alcanzar los objetivos de seguridad de la información y de cumplir con la política de seguridad.
- Designar todos los recursos necesarios para llevar a cabo el SGSI.

- Determinar todos los criterios de aceptación de riesgos y sus amenazas.
- Asignar los recursos suficientes para todas las fases del SGSI.
- Garantizar que se realizan todas las auditorías internas.
- Llevar a cabo revisiones periódicas del SGSI.

Alcance

El contenido de este SGSI, comprende como principal objetivo la seguridad de la información de los procesos y subprocesos que ha establecido la Contraloría Departamental del Madalena y de todos sus activos y plataformas tecnológicas.

- **Procesos**

  Hacen parte del alcance del SGSI todos los procesos descritos en el mapa de procesos de la CGM y sus subprocesos, que están clasificados en macroprocesos estratégicos, misionales, de apoyo y de evaluación y control.

- **Activos**

  Dentro del alcance del SGSI están los activos de información identificados y clasificados en la CGM y los equipos, cajas y archivadores donde se alojan dichos activos de información en cada una de las oficinas de la CGM y que están a cargo de cada uno de sus funcionarios y contratistas.

- **Plataformas tecnológicas**

  Las plataformas tecnológicas que hacen parte del alcance del SGSI son (i) la página web de la CGM, SIA OBSERVA y SIA CONTRALORIA. También hacen parte del alcance del SGSI el software de gestión documental MOLECULA y SIIGO de gestión financiera. (Aprende, 2016)

OBJETIVOS

Objetivo General

- Implementar un SGSI, que permita preservar la confidencialidad, integridad y disponibilidad de los activos de información en la CGM.

Objetivos Específicos

- Identificar los activos de información de la CGM.
- Identificar las amenazas y vulnerabilidades que puedan afectar la seguridad de los activos de información de la CGM
- Identificar los riesgos existentes sobre los activos de información de la CGM que puedan causar daño o pérdida sobre los mismos.
- Establecer controles que permita mitigar las causas que originan los riesgos.

- Definir la política general y las políticas específicas de seguridad y sus lineamientos que permitan minimizar los riesgos a los que están expuestos los activos de información.
- Realizar acciones preventivas y correctivas para la monitorización, mantenimiento, revisión y mejora del SGSI.

ROLES Y RESPONSABILIDADES

La entidad debe definir mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad.

La dirección debe gestionar 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 cada oficina; también debe organizar el grupo de trabajo responsable para implementar el Sistema de Gestión de seguridad de la información en la entidad, definiendo el perfil y rol de conformidad con lo establecido en las políticas de la entidad.

Teniendo en cuenta lo anterior, al final del ejercicio el grupo de trabajo que lidera la implementación del SGSI, debe dar a conocer el perfil y responsabilidades de los responsables.

El grupo de trabajo encargado de la implementación en la entidad se encargará de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades necesarias para adoptar el Sistema de Gestión de Seguridad de la Información al interior de la CGM, así como planear las actividades necesarias para una adecuada administración y sostenibilidad del mismo.

Con el fin de poder realizar la labor de la manera más eficiente, se sugiere que los integrantes para el grupo de trabajo al interior de la entidad, se denominen de la siguiente forma:

Responsable de Seguridad de la Información para la entidad

Se recomienda la definición de un responsable de seguridad que responda a las necesidades del SGSI que cuente con experiencia y conocimientos en el área de planeación estratégica de tic y seguridad de la información. El Responsable de Seguridad de la información será el líder del proyecto, escogido dentro del grupo de trabajo mencionado anteriormente y tendrá las siguientes responsabilidades:

Responsabilidades del Responsable de Seguridad de la información:

- Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo

- Identificar la brecha entre el Sistema de Gestión de seguridad de la información y la situación de la entidad.
- Generar el cronograma de la implementación del Sistema de Gestión de seguridad de la información.
- Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.
- Gestionar el grupo de trabajo de la entidad, definiendo roles, responsabilidades, entregables y tiempos.
- Coordinar las actividades diarias del grupo de trabajo y gestionar apoyo administrativo.
- Encarrilar el proyecto hacia el cumplimiento de la implementación del Sistema de Gestión de Seguridad de la Información para la entidad.
- Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y comunicarlo al Comité de seguridad o la directiva en caso de ser necesario.
- Trabajar de manera integrada con el grupo de trabajo.
- Asegurar la calidad de los entregables y del proyecto en su totalidad.
- Velar por el mantenimiento de la documentación del proyecto, su custodia y protección.
- Contribuir al enriquecimiento del conocimiento sobre el proyecto en cuanto a la documentación de las lecciones aprendidas.
- Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto.

Grupo de trabajo del Proyecto

El grupo de trabajo de la entidad, debe conformarse por personal del área o la persona encargada de tecnologías y sistemas de información, miembros directivos y representantes de las oficinas misionales, con el propósito de asegurar que toda la información más relevante de la entidad esté disponible oportunamente. Para de esta forma garantizar que sea un proyecto de carácter transversal a la entidad, y que no dependa exclusivamente del área o persona encargada de tecnologías y sistemas de información.

El líder del proyecto tiene como tarea principal entregar y dar a conocer los perfiles y responsabilidades de cada personaje al grupo de trabajo e identificar las personas idóneas para tomar cada rol. Se pone a consideración el siguiente listado para que la entidad analice de acuerdo a su composición orgánica cuales deben ser los miembros del grupo de trabajo de seguridad de la información, de acuerdo a los siguientes perfiles:

- Personal de seguridad de la información.

- Un representante del área de Tecnología.
- Un representante del área de Control Interno.
- Un representante del área de Planeación.
- Un representante de sistemas de Gestión de Calidad.
- Un representante del área Jurídica.
- Funcionarios, proveedores, y ciudadanos

Es importante resaltar nuevamente la necesidad del compromiso de la Alta dirección de la entidad.

Responsabilidades del grupo de trabajo del proyecto:

- Apoyar al líder de proyecto al interior de la entidad.
- Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto.
- Ayudar al líder de proyecto designado, en la gestión de proveedores de tecnología e infraestructura.
- Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder de proyecto.
- Las que considere el líder del proyecto o el comité de seguridad de la entidad.

Comité de seguridad

Las funciones de este comité pueden ser incluidas por el comité Institucional de desarrollo administrativo, como instancia orientadora de la implementación de la estrategia de Gobierno en línea de acuerdo al señalado en el Art. 2.2.9.1.2.4. Responsable de orientar la implementación de la Estrategia de Gobierno en Línea. O si la Entidad así lo estima conveniente, se debe crear un comité de Seguridad de la Información para la Entidad conformado por los siguientes perfiles:

1. El Jefe del área o persona encargada de tecnologías y sistemas de información.
2. El Jefe de la oficina de Planeación o su representante.
3. El feje de la oficina Jurídica o su delegado.
4. El Directivo encargado de los sistemas de Gestión de Calidad o su delegado
5. El Directivo encargado de la Gestión Documental o su delegado.
6. El jefe de la oficina de Control Interno o su delegado.
7. El responsable de Seguridad de la información de la entidad.

Formación y concientización sobre la seguridad de la información

Los funcionarios y de ser necesario el personal contratista del área o persona encargada de tecnologías y sistemas de información, 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 desarrollarán de acuerdo al plan integral de capacitación de la entidad en las funciones, responsabilidades y habilidades de los funcionarios.

Proceso ante un incidente de seguridad

En el momento de presentarse un incidente de seguridad, el profesional universitario encargado de tecnología y sistemas de información, 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 oficina.

Devolución de activos

Al momento del retiro de funcionario de la entidad, este mismo debe devolver todos sus activos de información, para así ser descargados del archivo de inventarios de activos, retirando los accesos físicos y lógicos, como requisito para la firma de paz y salvos, lo anterior se gestiona desde la oficina de acción administrativa con la supervisión y operación de la persona encargada de backup y borrado seguro. (MinTic, 2016)

AMENAZAS

Amenazas: Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización. Las amenazas son eventos que pueden afectar a los activos de información y causar perdida. Las amenazas fueron identificadas y clasificadas en las siguientes categorías:

Amenazas informáticas: esta categoría de amenazas puede presentarse por falta de un antivirus o mal uso del internet y supervisión por parte de los funcionarios.

Amenazas de origen informático para la CGM:

- Spywre (Programas espías)
- Troyanos, virus y gusanos
- Phishing
- Spam
- Botnets (Redes de robots)
- Trashing

Amenazas de Origen Físico: Están se pueden presentar por desastres ambientales, degradación o fallas físicas en las instalaciones de la CGM.

Amenazas de origen físico para la CGM:

- Incendio

- Inundación o humedad
- Sismo o temblor
- Polvo
- Falta de ventilación
- Electromagnetismo
- Sobrecarga eléctrica
- Falla de corriente (apagones)
- Falla de sistema (Daño disco duro)

Amenazas de Usuario: Estas pueden presentarse por los errores que pueda causar un usuario sobre los activos en la CGM.
Amenazas para la CGM originadas por funcionarios:

- Falta de inducción, capacitación y sensibilización sobre riesgos.
- Mal manejo de equipos, sistemas y herramientas.
- Perdida de datos por error de usuario.

Amenazas de Hardware: Se pueden presentar por diferentes fallas que puedan presentarse en los componentes de hardware de la CGM.
Amenazas de Hardware para la CGM:

- Infección de sistemas a través de unidades portables sin escaneo
- Exposición o extravío de equipo
- Perdida de datos por error hardware
- Falta de mantenimiento físico (proceso, repuestos e insumos)

Amenazas de Datos: Estas se enfocan en la información y datos de los sistemas y equipos que pueden estar expuestos a un acceso no autorizado, una alteración, entre otros.
Amenazas de datos para la CGM:

- Manejo inadecuado de datos críticos (codificar, borrar, etc.)
- Transmisión no cifrada de datos críticos

Amenazas de Software: Dentro de esta categoría se encuentran los errores de diseño, pruebas e implementación de software en la CGM.
Amenazas de Software para la CGM:

- Falta de actualización de software (proceso y recursos)

Amenazas de Infraestructura: Dentro de esta categoría se encuentran los problemas de organización en la parte de infraestructura que puede ocasionar perjuicios al sistema GIS.
Amenazas de infraestructura para la CGM:

- Dependencia a servicio técnico externo

- Red cableada expuesta para el acceso no autorizado

Amenazas sobre las Políticas: Estas se enfocan en la falta de normas y reglas de la organización de las cuales pueden llegar a tener un gran riesgo los activos de la CGM.
Amenazas por políticas para la CGM

- Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)
- Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de control Ausencia de documentación
- Falta de definición de perfil, privilegios y restricciones de los funcionarios
- Falta de definición de política de seguridad corporativa

Amenazas de Redes: En esta categoría se encuentran las fallas de seguridad en el acceso y transmisión a través de la red de la CGM.
Amenazas en redes para la CGM:

- Red inalámbrica expuesta al acceso no autorizado
- Acceso electrónico no autorizado a sistemas externos
- Acceso electrónico no autorizado a sistemas internos

Amenazas de Acceso: Dentro de esta categoría se encuentran los accesos de personal no autorizado a los sistemas e instalaciones de la CGM
Amenazas de acceso para la CGM:

- Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas)
- Compartir contraseñas o permisos a terceros no autorizados
- Acceso de personas no autorizadas a las instalaciones de la CGM. (robo, sabotaje, vandalismo, etc.) (Colombia, 2013)

VULNERABILIDADES

VULNERABILIDAD: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza. Las vulnerabilidades fueron identificadas y clasificadas en las siguientes categorías:
Vulnerabilidades de los Recursos Humanos: Las vulnerabilidades identificadas en esta categoría son aquellas ligadas a los funcionarios que trabajan o prestan un servicio en la CGM.
Vulnerabilidad de los funcionarios para la CGM:

- Ausentismo o personal insuficiente
- Definición de rol inadecuada

- Falta de conciencia de la seguridad de la información
- Falta de capacitación de funcionarios
- Falta de mecanismos de monitoreo
- Falta de políticas/normas/procedimientos
- Circunstancias personales
- Falta de delegación/participación/sucesión
- Medioambiente adverso - calefacción, humedad, ruido, iluminación, olor, etc.
- Empleado molesto
- Recursos insuficientes, inadecuados, incompatibles

Vulnerabilidades de Software en la CGM: Las vulnerabilidades detectadas en esta categoría están relacionadas van con el uso, mantenimiento y administración de software de la CGM.
Vulnerabilidades Software de la CGM:

- Diseño de aplicación inadecuado
- Interface de usuario inadecuada/complicada
- Control de acceso inadecuado
- Uso impropio/no controlado
- Contraseñas o claves no protegidas
- Administración deficiente de contraseña
- Incompatibilidad Software
- Falta de documentación
- Uso de parches de software
- Administración de encriptación inadecuada
- Falta de protección contra virus y código malicioso
- Administración de configuración inadecuada

Vulnerabilidades de Hardware: Las vulnerabilidades identificadas en esta categoría están relacionadas con el uso, mantenimiento y configuración de los equipos de cómputo, de red, de impresión u otros tipos de hardware desde una planta eléctrica hasta cámaras fotográficas pertenecientes a la CGM.
Vulnerabilidades Hardware de la CGM:

- Falla Hardware
- Exceso de Uso en la vida útil del Hardware
- Almacenamiento inadecuado/impropio
- Localización - exposición a daño
- Localización - exposición - temperatura
- Localización - exposición - humedad/agua

- Localización - exposición – contaminación/polvo
- Localización - exposición a intercepción visual, auditiva o electromagnética
- Falta de manutención planificada
- Incompatibilidad Hardware
- Control de acceso inadecuado
- Remoción de equipo para mantención
- Capacitación inadecuada
- Falta en tiempo de sincronización
- Suministro eléctrico (estabilizadores, reguladores y UPS´s)
- Control de configuración inadecuado
- Conexión de equipo no autorizado

Vulnerabilidades por Medio Ambiente e Infraestructura: Las vulnerabilidades pertenecientes a esta categoría son aquellas ligadas a la infraestructura de la CGM y el medio ambiente que rodea a la entidad.
Vulnerabilidades medio ambiente e infraestructura en la CGM:

- Protección física inadecuada – oficina
- Protección física inadecuada – edificio
- Control de acceso inadecuado – oficina
- Control de acceso inadecuado - edificio
- Abastecimiento de energía eléctrica inestable
- Desastre natural (tormentas eléctricas, inundación, temblor, tsunami, etc.)
- Desastre provocado por el hombre
- Monitoreo insuficiente de medidas de seguridad para el medio ambiente e infraestructura
- Falta de mantención a la infraestructura
- Inadecuada prevención contra incendio (detección)

Vulnerabilidades de Comunicaciones: Las vulnerabilidades identificadas para esta categoría tienen que ver con el sistema de comunicaciones en la transmisión de datos por medio redes de intranet o redes WAN o LAN, o hasta la red telefónica.
Vulnerabilidades comunicaciones de la CGM:

- Líneas de comunicación no protegidas
- Uniones de cables deficientes/conexiones
- Falta de identificación del remitente/receptor
- Transferencia de contraseñas/claves viables en texto visible

- Acceso por discado no controlado (red telefónica conmutada fija, o digital como GSM, pero que su objeto principal es la telefonía de voz.)
- Protección inadecuada de trafico sensible
- Administración de redes inadecuada
- Protección inadecuada para acceso publico
- Comunicaciones móviles
- Capacidad inadecuada de la red (Colombia, 2013)

RIESGOS Y MEDIDAS DE SEGURIDAD

Un riesgo es la probabilidad de que ocurra un evento en contra de la seguridad de los activos de información causando daños o pérdidas. Un análisis de riesgos permitirá a la entidad especificar cuáles riesgos son más probables de ocurrencias, cuáles serán más destructivos y cuáles serán los más urgentes de minimizar.

Las medidas de seguridad son las acciones que tomara la entidad para disminuir los riesgos de seguridad. Las medidas de seguridad se dividen en:

- **Preventivas:** son las medidas que tienden a disminuir el riesgo de que una amenaza ocurra antes de producirse.
- **Perceptivas:** estas medidas consisten en realizar acciones que revelen riesgos no detectados.
- **Correctivas:** son las medidas que se toman cuando ha ocurrido una amenaza.

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La dirección de la CGM, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

La CGM, determina que la información es un activo de alta importancia para la entidad, por tal motivo la protección de la información es un objetivo principal, lo cual genera la necesidad de implementar reglas y medidas que permitan proteger la integridad, la confidencialidad y la disponibilidad de la información sobre los riesgos y amenazas, por ende, la CGM está comprometida a proteger sus activos de información

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance para, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas.

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas, terceros y la ciudadanía en general.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de CGM.
- Garantizar la continuidad de los procesos y actividades frente a incidentes.

PRINCIPIOS DE SEGURIDAD QUE SOPORTAN EL SGSI DE LA CGM

- La CGM ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de los procesos de la entidad.

- Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de **los funcionarios, proveedores, practicantes, sujetos de control, terceros y la ciudadanía en general**.

- La CGM **protegerá la información** generada, procesada o resguardada por sus procesos y subprocesos, su plataformas tecnológica y sus activos del riesgo que se genera de los accesos **otorgados a terceros** (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

- La CGM **protegerá la información** creada, procesada, transmitida o resguardada por sus procesos y subprocesos, con el fin de minimizar impactos financieros, operativos o legales debido a un **uso incorrecto** de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- La CGM **protegerá su información** de las amenazas originadas por parte **de los funcionarios**.

- La CGM **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.

- La CGM **controlará la operación** de sus procesos y subprocesos garantizando la seguridad de los recursos tecnológicos.

- La CGM **implementará control de acceso** a la información, sistemas y recursos de red.

- La CGM garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- La CGM garantizará a través de una adecuada gestión de los eventos de seguridad y las vulnerabilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- La CGM **garantizará la disponibilidad** de sus procesos y subprocesos y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- La CGM garantizará el cumplimiento de las **obligaciones legales, regulatorias y contractuales establecidas.**

El incumplimiento a la política de Seguridad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere. (MinTic2, 2016)

POLÍTICAS ESÉCIFICAS DE SEGURIDAD DE LA INFORMACIÓN

Política de estructura organizacional de seguridad de la información

La CGM en cumplimiento al compromiso del Sistema de Gestión de Seguridad de la Información crea un esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información, así como la creación del Comité y el Administrador de Seguridad de la Información.

El área o las personas encargada de las Tecnologías y Sistemas de Información deben establecer los roles, funciones y responsabilidades de operación y administración de los sistemas de información de la CGM a los funcionarios disponibles en la entidad. Estos roles, funciones y responsabilidades, deberán estar debidamente documentadas y distribuidas.

Política de seguridad para los recursos humanos

La CGM implementa acciones para asegurar que los funcionarios y demás colaboradores de la Entidad, entiendan sus responsabilidades como usuarios en relación con las políticas de seguridad de la información y la responsabilidad de los roles asignados, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones, o los equipos empleados para el tratamiento de la información

La CGM y los funcionarios diligenciaran y firmaran el debido formato de entrega de equipos cuando se provea de estos al funcionario para el desarrollo de las actividades que tengan lugar para cumplir con las funciones a su cargo, en dicho formato el funcionario se hace responsable del equipo. (Crear formatos para la entrega de equipos, donde se hace firmar a los funcionarios como responsables de dichos equipos)

Se debe capacitar y sensibilizar a los funcionarios durante la inducción sobre las políticas de seguridad de la información.

Políticas específicas para usuarios de la CGM.

Definir las pautas generales para asegurar una adecuada protección de la información de la CGM por parte de los usuarios de la entidad.

Políticas específicas para funcionarios y contratistas del Área de Tecnologías y Sistemas de Información o la persona encargada.

Definir las pautas generales para asegurar una adecuada protección de la información de la CGM por parte de los funcionarios y contratistas de TI de la entidad.

Política de tratamiento de datos personales

Objetivo: Establecer los lineamientos para administración y tratamiento de datos personales en la CGM.

Los funcionarios, contratistas y proveedores deben dar aprobación a la CGM para el tratamiento de sus datos personales de acuerdo a la Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales lo que se deberá reflejado en las cláusulas de los contratos y en el aplicativo aspirante.

Datos de menores de edad: El suministro de los datos personales de menores de edad es facultativo y debe realizarse con autorización de los padres de familia o representantes legales del menor, en concordancia con lo establecido por la Ley 1098 de 2006 "Código de Infancia y Adolescencia".

Política de Tercerización u Outsourcing.

La CGM implementara las directrices para mantener la seguridad de la información y los servicios de procesamiento de información a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.

Política de gestión de activos de Información

La CGM es la dueña de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios de la CGM y los contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

La CGM es propietaria de los activos de información y los administradores de estos activos son los funcionarios o demás colaboradores de la CGM que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información (TIC).

La CGM mantendrá un inventario actualizado de sus activos de información de acuerdo al formato de registro y actualización de los inventario de activos de información (hay que colocarle un código o un nombre al formato para identificarlo), quedando bajo la responsabilidad de cada propietario de información y centralizado por el Área o persona a cargo de Tecnologías y Sistemas de Información. (El cual puede o debe publicarse en la página web de la CGM).

La Entidad debe realizar el tratamiento de información documental de acuerdo a como lo tenga establecido. (Manual de gestión documental).

Política de uso de los activos

La Entidad implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

Los usuarios no deben mantener almacenados en los discos duros de los equipos de cómputo o discos duros portátiles, archivos de vídeo, música y fotos y cualquier tipo de archivo que no sean de carácter institucional.

Política de clasificación de la información.

La CGM consiente de la necesidad de asegurar que la información reciba el nivel de protección apropiado de acuerdo al tipo de clasificación establecido por la entidad, define reglas de como clasificar la información, liderado por el proceso de inventario de activos de información.

- Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere la CGM como, por ejemplo:
  - ✓ Formularios/ comprobantes propios o de terceros.
  - ✓ Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
  - ✓ Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
  - ✓ Información o conocimiento transmitido de manera verbal o por cualquier otro medio de comunicación.
  - ✓ Procesos, demandas o hallazgos.
- Los funcionarios responsables de la información de la CGM, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.
- Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como "Valiosa" para la CGM; Independiente del tipo de activo, se deben considerar las siguientes características:
  - ✓ El activo de información es reconocido como valioso para la CGM.
  - ✓ No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.
  - ✓ Forma parte de la identidad de la organización y sin el cual la CGM puede estar en algún nivel de riesgo.
  - ✓ Los niveles de clasificación de la información valiosa que se ha establecido son: INFORMACIÓN PÚBLICA RESERVADA, INFORMACIÓN PÚBLICA CLASIFICADA e INFORMACIÓN PÚBLICA.

- Se debe monitorear periódicamente Las reglas se encuentran definidas en el formato de registro y actualización de los Inventarios de la Información

Política de control de acceso.
La Entidad define las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataforma informática de la CGM, considerándolas como importantes para el SGSI.
La conexión remota a la red de área local de la CGM debe realizarse a través de una conexión VPN (red privada virtual) segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada, por el Área o persona encargada de Tecnologías y Sistemas de información.
Todo aplicativo informático o software debe ser comprado o aprobado por el Área o persona encargada de Tecnologías y Sistemas de información en concordancia con la política de adquisición de bienes de la entidad. De acuerdo con lo definido en el proceso Adquisición de Bienes y Servicios que tenga la entidad.
Política de establecimiento, uso y protección de claves de acceso
Ningún usuario deberá acceder a la red o a los servicios TIC de la CGM, utilizando una cuenta de usuario o clave de otro usuario.
La CGM suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.
El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, comunicándose con el Área o persona encargada de Tecnologías y Sistemas de información, en donde se llevará a cabo la validación de los datos personales: en caso de ser solicitado el cambio de contraseña para otra persona, debe ser realizada por su jefe inmediato.
Las claves o contraseñas deben:

- Tener mínimo ocho (8) caracteres alfanuméricos.
- Cada vez que se cambien estas deben ser distintas por lo menos de las últimas doce anteriores.
- La contraseña debe cumplir con tres de los siguientes cuatro requisitos:
  - ✓ Caracteres en mayúsculas
  - ✓ Caracteres en minúsculas
  - ✓ Base de 10 dígitos (0 a 9)
  - ✓ Caracteres no alfabéticos (Ejemplo: ¡, $, %, &)

Manejo de contraseñas para administradores de tecnología
Los usuarios súper-administradores y sus correspondientes contraseñas a las consolas administrables se dejan en custodia en sobre sellado en el área

segura donde designe la entidad, las credenciales allí contenidas deben ser modificadas de manera mensual o cuando amerite.
Las contraseñas referentes a las cuentas "predefinidas incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.
El personal del Área o la persona encargada de Tecnologías y Sistemas de la Información no debe dar a conocer su clave de usuario de los sistemas de información a terceros, sin previa autorización del Jefe del Área o persona encargada de Tecnologías y Sistemas de la Información o de un jefe superior.
Los usuarios y claves de los administradores de sistemas y del personal del Área o persona encargada de Tecnologías y Sistemas de la Información son de uso personal e intransferible.
El personal del Área o persona encargada de Tecnologías y Sistemas de la Información debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo al rol asignado.
Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el Jefe del Área o persona encargada de Tecnologías y Sistemas de Información o el Asesor para la de Seguridad de la Información o jefes superiores.

Política de uso de equipos de cómputo

La CGM establece reglas que permitan orientar que la seguridad es parte integral de los activos de información y mediante la correcta utilización de los equipos de cómputo por funcionarios o los usuarios finales

Política de uso de Internet.

La Entidad permite el acceso a servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

Política de uso de correo electrónico.

Definir las pautas generales para asegurar una adecuada protección de la información de la CGM, en el uso del servicio de correo electrónico por parte de los usuarios autorizados.

Política para uso de dispositivos móviles

La Entidad establece las directrices de uso y manejo de dispositivos móviles (teléfonos móviles. teléfonos inteligentes "Smartphone. Tabletas), Entre otros suministrados por la CGM y personales que hagan uso de los servicios de información de la Entidad.

Política de uso de mensajería instantánea y redes sociales.
La CGM define las pautas generales para asegurar una adecuada protección de la información de la entidad, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.
Política de uso de discos de red o carpetas virtuales.
Asegurar la operación correcta y segura de los discos de red o carpetas virtuales.
Política de uso de impresoras y del servicio de Impresión.
Asegurar la operación correcta y segura de las impresoras y del servicio de impresión.
Política de uso de puntos de red de datos (red de área local — LAN).
Asegurar la operación correcta y segura de los puntos de red.
Política de escritorio y pantalla limpia.
Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los funcionarios.
Política de respaldo y restauración de información.
La CGM Proporcionara los medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.
Política para la Transferencia de Información.
Proteger la información transferida al interior y exterior de la CGM.
Política de manejo y disposición de información, medios y equipos
La entidad establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados por la CGM, velando por la integridad, disponibilidad y confidencialidad de la información.
Política de retención y archivo de datos.
Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.
La política de retención de archivos debe establecer cuánto tiempo se deben mantener almacenados los archivos en la CGM de acuerdo a las tablas de retención documental.
Las reglas y los principios generales que regulan la función archivística de la entidad se encuentran definidos por la Ley, la cual es aplicable a la administración pública en sus diferentes niveles producidos en función de su misión y naturaleza.
La ley prevé el uso de las tecnologías de la información y las comunicaciones en la administración, conservación de archivos y en la elaboración e implantación de programas de gestión de documentos.

Política de adquisición, desarrollo y mantenimiento de sistemas de información.

Garantizar que la seguridad es parte integral de los sistemas de información.

Política de registro y seguimiento de eventos de sistemas de información y comunicaciones.

Preservar la integridad, confidencialidad y disponibilidad de los registros de eventos generados por los sistemas de información y comunicaciones de la CGM.

Política de gestión de vulnerabilidades

Evitar la utilización de vulnerabilidades técnicas de los sistemas de información y comunicaciones de la CGM, e implementar los lineamientos para gestión de vulnerabilidades.

Políticas específicas para Web master.

Proteger la integridad de las páginas Web institucionales, el software y la información contenida.

Política de Seguridad Física

Implementar un programa de seguridad física para el acceso a las instalaciones que permita fortalecer la confidencialidad, disponibilidad e integridad de la información

Políticas de seguridad del centro de datos y/o centros de cableado.

Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte, en las instalaciones del centro de datos o de los centros de cableado existentes.

Políticas de seguridad de los Equipos.

Asegurar la protección de la información en los equipos.

Política de seguridad de las comunicaciones.

Implementar mecanismos de control que permitan mantener la disponibilidad de las redes de datos, sistemas de comunicaciones e instalaciones de procesamiento de la CGM.

Política de Gestión de los Incidentes de la Seguridad de la Información

Asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de tomar oportunamente las acciones correctivas.

Política de Revisiones de Seguridad de la Información

Garantizar el funcionamiento del sistema de gestión de seguridad de la información de acuerdo a las políticas y procedimientos implementados en la CGM. (MinTic2, 2016)

LINEAMIENTOS

Lineamientos específicos para usuarios de la CGM

La CGM no se hace responsable por las copias no autorizadas de programas instalados o ejecutados en los equipos asignados a sus funcionarios, contratistas o practicantes.

Los recursos tecnológicos y de software asignados de propiedad de la CGM son responsabilidad de cada funcionario o usuario.

Los funcionarios, son los responsables de la información que administran y generan en sus equipos personales, deben abstenerse de almacenar en ellos información institucional, de acuerdo con la guía de clasificación de la información.

Los funcionarios solo tendrán acceso a los datos y recursos autorizados por la CGM, y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.

Es responsabilidad de cada funcionario proteger la información que está contenida en documentos, formatos, listados, etc., los cuales son el resultado de los procesos informáticos; adicionalmente se deben proteger los datos de entrada de estos procesos.

Los dispositivos electrónicos (computadores, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por la entidad.

Cualquier evento o posible incidente que afecte la seguridad de la información, debe ser reportado inmediatamente al Área de Tecnología y Sistemas de la Información o persona encargada de la CGM.

Los jefes de las oficinas de la CGM, en conjunto con el comité de seguridad de la Información(si se crea el comité) o la persona encargada propiciarán actividades para concienciar al personal sobre las precauciones necesarias que deben realizar los funcionarios finales, para evitar revelar información clasificada, como por ejemplo: cuando se hace una llamada telefónica, que pueda ser interceptada mediante acceso físico a la línea o al auricular o ser escuchada por personas que se encuentren cerca, este lineamiento aplica en situaciones en que el funcionario, contratista o colaborador se encuentre en sitios públicos como restaurantes, transporte público, ascensores, etc.

Lineamientos específicos para funcionarios y contratistas del Área de Tecnología y Sistemas de la Información

Los documentos y la información de procedimientos, seriales, software etc. deben mantenerse custodiados para evitar el acceso a personas no autorizadas.

Para el cambio o retiro de equipos de los funcionarios, se deben llevar a cabo mejores prácticas para la eliminación de la información de acuerdo al software disponible en la entidad. Se debe hacer un Formateo seguro, una destrucción total de documentos o borrado seguro de equipos electrónicos.

Los funcionarios encargados de realizar la instalación o distribución de software, sólo instalarán productos con licencia y software autorizado y acorde con los derechos de autor.
Los funcionarios del Área de Tecnologías y Sistemas de Información o la persona encargada no deben otorgar privilegios especiales a los funcionarios sobre las estaciones de trabajo, sin la autorización correspondiente del Jefe del Área de Tecnologías y Sistemas de Información o la persona encargada.
Los funcionarios del Área de Tecnologías y Sistemas de Información o persona encargada se obligan a no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones de acuerdo con la guía de clasificación de la información según sus niveles de seguridad. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.
Los funcionarios del Área de Tecnologías y Sistemas de Información o persona encargada no utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.
Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.
Las copias licenciadas y registradas del software adquirido, deben ser únicamente instaladas en los equipos y servidores de la entidad. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de la entidad.
La copia de programas o documentación, requiere tener la aprobación escrita de la CGM y del proveedor si éste lo exige.
El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.

Lineamientos para Tercerización u Outsourcing.

Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.
Se debe establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información de la CGM, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.
En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información

Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por la CGM.
El Área o persona encargada de Tecnologías y Sistemas de Información deberá mitigar los riesgos de seguridad con referencia al acceso de los proveedores y/o contratistas a los sistemas de información de la CGM.
Se debe identificar y monitorear los riesgos relacionados con los contratistas o proveedores en relación a los objetos contractuales, incluyendo la cadena de suministro de los servicios de tecnología y comunicación.
Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas a la CGM. El resultado del análisis de riesgos será la base para el establecimiento de los controles y debe ser presentado al Comité de seguridad de la Información antes iniciar el estudio de mercado y publicación del proyecto de pliegos del contrato de outsourcing en el portal de contratación.
Los funcionarios de la CGM que tengan la función como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.
Se deben establecer mecanismos o condiciones con los contratistas o proveedores que permitan realizar la gestión de cambios en los servicios suministrados.

Lineamientos para el uso de los activos

Los activos de información pertenecen a la CGM y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.
Los usuarios deberán utilizar únicamente los programas y equipos autorizados por el Área o la persona encargada de Tecnologías y Sistemas de Información.
La CGM proporcionará al usuario, los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de la CGM, los funcionarios no podrán realizar backup de sus archivos personales o de información pública, para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato, de acuerdo a las normas sobre clasificación de la información de acuerdo a los niveles de seguridad establecidos por la CGM; Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución, serán sancionadas de acuerdo con las normas y legislación vigentes.
Periódicamente, el Área de Tecnologías y Sistemas de la Información efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos NO autorizados será considerado como una violación a las Políticas de Seguridad de la Información de la CGM.

Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados por el jefe de la oficina a través de un oficio con su respectivo soporte al Área o persona encargada de Tecnologías y Sistemas de Información.
Estarán bajo custodia del Área o persona encargada de Tecnologías y Sistemas de la Información los medios magnéticos/electrónicos (disquetes, CDs u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y los passwords de administración de los equipos informáticos, sistemas de información o aplicativos.
En caso de ser necesario y previa autorización del Comité de Seguridad de la Información (que debe crearse) de la CGM, los funcionarios de la CGM podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban, a través de Internet o de cualquier otra red o medio, en los equipos informáticos a su uso.
Los recursos informáticos de la CGM no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.
Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos o que vayan en contravía de las políticas de seguridad de la información entre ellos envíos o reenvíos masivos de correos electrónicos o spam, practica de juegos en línea, uso permanente de redes sociales personales, conexión de periféricos o equipos que causen molestia a compañeros de trabajo, etc.
Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización del Área o persona encargada de Tecnologías y Sistemas de la Información:

- Instalar software en cualquier equipo de la CGM;
- Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de la CGM;
- Modificar, revisar, transformar o adaptar cualquier software propiedad de la CGM;
- Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la CGM.
- Copiar o distribuir cualquier software de propiedad de la CGM.
- Cambiar la configuración de hardware de propiedad de la CGM.

El usuario deberá informar al Área o persona encargada de la Tecnologías y Sistemas de Información de la CGM a través de la Ext. xxxx o correo electrónico

"soportes"@contraloriadelmagdalena.gov.co y al Jefe Inmediato, sobre cualquier violación de las políticas de seguridad, uso indebido y debilidades de seguridad de la información de la CGM que tenga conocimiento.
El usuario será responsable de todas las transacciones o acciones efectuadas con su cuenta de usuario.
Ningún usuario deberá acceder a la red o a los servicios TIC de la CGM, utilizando una cuenta de usuario o clave de otro usuario.
Los usuarios no están autorizados para hacer uso de redes externas a través de dispositivos personales en las instalaciones de la entidad (modem USB, router, wifi público, etc.), esto compromete la seguridad de los recursos informáticos de la CGM.
El Área o persona encargada de Tecnologías y Sistemas de Información de la CGM, es el área responsable de realizar el aseguramiento de los accesos a internet, acceso a redes de terceros y a las redes de la entidad; esta responsabilidad incluye, pero no se limita a prevenir que intrusos tengan acceso a los recursos informáticos y a prevenir la introducción y propagación de virus.
Todo archivo o material descargado o recibido a través de medio magnético/electrónico o descarga de Internet o de cualquier red externa, deberá ser revisado para detección de virus y otros programas maliciosos antes de ser instalados en la infraestructura TIC de la CGM.
Todos los archivos provenientes de equipos externos a la CGM, deben ser revisados para detección de virus antes de su utilización dentro de la red de la CGM.
Todo cambio a la infraestructura informática deberá estar controlado y será realizado, supervisado, o autorizado por el Área o persona encargada de Tecnologías y Sistemas de Información de la CGM.
La información del CGM debe ser respaldada de forma frecuente, debe ser almacenada en lugares apropiados en los cuales se pueda garantizar que la información está segura y podrá ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento.
Los funcionarios deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados por el CGM en el proceso de desvinculación, de igual manera deberán documentar y entregar al CGM los conocimientos importantes que posee de la labor que ejecutan.

Lineamientos para control de acceso

La Entidad define la de forma de Autorización de acceso físico a Visitantes y Proveedores a las instalaciones de la CGM, que será ejecutado por la empresa contratista de seguridad privada, la Oficina de Acción Administrativa y el Área o persona encargada de Tecnologías y Sistemas de Información.
El Área o persona encargada de Tecnologías y Sistemas de Información configura los niveles de acceso para usuarios de los servicios y sistemas de información de la CGM, acorde con Solicitud para la creación o Ajuste de

Cuenta de usuario y servicios de Tecnología de Información mediante solicitud escrita de creación de cuenta de usuario por parte Jefe de oficina del funcionario y la autorización de la oficina de Acción administrativa
La CGM debe contar con un firewall, sistemas de prevención y detección de intrusos para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en outsourcing o de terceros.
La CGM proporcionará a los funcionarios, personal en comisión y contratistas (personas naturales) todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales fueron contratados, por tal motivo no se permite conectar a la red o instalar dispositivos fijos o móviles, tales como: computadores portátiles, tablets, enrutadores, agendas electrónicas, celulares inteligentes, access point; el Área o la persona encargada de Tecnologías y Sistemas de Información podrá realizar la mencionada conexión previa solicitud del interesado y autorización de la oficina de Acción administrativa si lo amerita.
Todo funcionario que requiera ingresar a los servicios de red de la CGM deberá diligenciar la solicitud por escrito, excepto la configuración de acceso a internet de visitantes, en equipos no institucionales o personales, estas deben ser supervisadas por el funcionario a cargo del visitante.
Todo usuario final con privilegios de publicación o administración de servicios Web, administrador de servicios o aplicativos de la CGM, deberá diligenciar y firmar el formato entrega de Rol, en caso de asignación o entrega del rol.
Solo los funcionarios pertenecientes al Área de Tecnologías y Sistemas de Información o la persona encargada, están autorizados para instalar software y/o hardware en los equipos, servidores e infraestructura de telecomunicaciones de la CGM, así como el uso de herramientas que permitan realizar tareas de mantenimiento, revisión de software, recuperar datos perdidos, eliminación de software malicioso.
El Área o persona encargada de Tecnologías y Sistemas de Información debe restringir el acceso a los códigos fuentes de los programas y elementos asociados como diseños, especificaciones, librerías de fuentes de programas, planes de verificación y planes de validación, así mismo debe auditar este acceso de manera periódica.
El retiro e ingreso de todo activo de información de los visitantes que presten servicios a la CGM (consultores, pasantes, practicantes, visitantes, etc.) será registrado e inspeccionado en los controles de accesos de las instalaciones de la Entidad. El personal de seguridad y vigilancia en los controles de acceso verificarán y registrarán las características de identificación del activo de información.

Lineamientos para el establecimiento, uso y protección de claves de acceso

Se debe concienciar y controlar a los funcionarios para que apliquen buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un funcionario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.

Los funcionarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la Entidad.

Ningún funcionario deberá acceder a la red o a los servicios TIC de la CGM, utilizando una cuenta de usuario o clave de otro funcionario.

Los funcionarios deben tener en cuenta los siguientes aspectos:

- El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, comunicándose a el área o persona encargada de Tecnologías y Sistemas de Información de donde se llevará a cabo la validación de los datos personales; en caso de ser solicitado el cambio de contraseña para otro funcionario que se encuentre de licencia, comisión, vacaciones, o que no se encuentre presente por motivo sustentable y se requiera información bajo su poder, debe ser solicitada por su jefe inmediato.
- Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.
- Se bloqueará el acceso a todo usuario que haya intentado el ingreso, sin éxito, a un equipo o sistema informático, en forma consecutiva por “x” veces.
- La clave de acceso será desbloqueada sólo por el personal del área o la persona encargada Tecnologías y Sistemas de Información luego de la solicitud formal por parte del responsable de la cuenta.
- La CGM suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados.
- Es responsabilidad del funcionario el manejo apropiado de las claves asignadas de los servicios de red y de acceso a la red, estas claves de acceso y usuarios son personales e intransferibles.

Manejo de contraseñas para administradores de tecnología

El personal del Área o persona encargada de Tecnologías y Sistemas de la Información no debe dar a conocer su clave de usuario de los sistemas de información a terceros, sin previa autorización del Jefe del Área de

Tecnologías y Sistemas de la Información o su jefe inmediato o de superiores de la directiva.
Los usuarios y claves de los administradores de sistemas y del personal del Área o de la persona encargada de Tecnologías y Sistemas de la Información son de uso personal e intransferible.
El personal del Área o la persona encargada de Tecnologías y Sistemas de la Información debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo al rol asignado.
Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el jefe del Área o la persona encargada de Tecnologías y Sistemas de Información.
Las claves o contraseñas deben:
Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, ni productos a resaltar de su entidad, evite asociarla con fechas especiales, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
Nunca utilice sus contraseñas personales en el entorno laboral
La contraseña debe tener mínimo ocho caracteres alfanuméricos.
Cambiarse obligatoriamente la contraseña, la primera vez que el usuario ingrese al sistema.
La contraseña debe cambiarse obligatoriamente cada 30 días, o cuando lo establezca o lo recomiende el Área o persona encargada de Tecnologías y Sistemas de Información.
Cada vez que se cambien las claves, estas deben ser distintas por lo menos de las últimas doce anteriores.

Lineamientos para uso de equipos de cómputo

La instalación de software en los computadores suministrados por la CGM, es una función exclusiva del Área o la persona encargada de Tecnologías y Sistemas de Información el cual mantendrá una lista actualizada del software autorizado en una unidad de almacenamiento para instalar en los computadores.
Se define los perfiles de Administrador local para ingreso a equipos:
1. Sistema
2. Cuentas de usuario (nombre y apellido del funcionario)

Los funcionarios que hagan uso de equipos institucionales en préstamo, NO deberán almacenar información en estos dispositivos y deberán borrar aquellos que copien en estos al terminar su uso.

Los funcionarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos de red, archivos de vídeo, música, fotos y cualquier tipo de archivo que no sean de carácter institucional.
En el Disco C:\ de las estaciones cliente se tiene configurado el sistema operativo, aplicaciones y perfil de usuario, la persona que haga uso de los equipos deberá abstenerse de realizar modificaciones a éstos archivos.
Los funcionarios podrán trabajar sus documentos institucionales en la estación cliente asignada por el CGM y deberán ubicar copias y documentos finales en las carpetas virtuales que se establezca para cumplir con las tablas de retención documental (TRD) de la Entidad.
El préstamo de equipos de cómputo, computadores portátiles y vídeo beam, se debe tramitar a través de solicitud escrita o por medio de correo electrónico remitido a la dirección de correo del Área o la persona encargada de Tecnologías y Sistemas de Información, con anticipación y se proveerá de acuerdo a la disponibilidad.
Los equipos que ingresan temporalmente a la CGM que son de propiedad de terceros: deben ser registrados en los controles de acceso de la entidad y su retiro; posteriormente la CGM no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a sus instalaciones.
El Área o la persona encargada de Tecnologías y Sistemas de Información no prestarán servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de la CGM.

Lineamientos para uso de Internet

La infraestructura, servicios y tecnologías usados para acceder a internet son propiedad de la CGM, por lo tanto, se reserva el derecho de monitorear el tráfico de internet y el acceso a la información, respetando en todo momento el derecho a la privacidad y a la seguridad de los datos personales consagrados en la Ley 1581 de 2012
No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de la CGM o que representen peligro para la entidad como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por la CGM. El acceso a este tipo de contenidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del comité de seguridad de la Información de la CGM
El Jefe del Área o la persona encargada de Tecnologías y Sistemas de Información autoriza los cambios solicitados de permisos de navegación a los funcionarios, previa solicitud del Jefe de cada una de las oficinas, de acuerdo a Lineamientos de Control de Acceso.
El Área o la persona encargada de Tecnologías y Sistemas de Información implementa herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales así mismo controla el acceso a

la información contenida en portales de almacenamiento en internet para prevenir la fuga de información.
La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio.

Lineamientos de uso de correo electrónico

- **Creación de correo electrónico:**

El correo electrónico de la entidad para un funcionario, debe ser creado mediante Autorización previa de creación de cuenta de usuario por parte del Jefe de Oficina de Acción Administrativa de la CGM.
El funcionario encargado del área de Tecnología y Sistemas de información, responsable de crear la cuenta red y de correo electrónico, la define de la siguiente forma:

- ✓ Para funcionarios: primernombre_primerapellido@contraloriadelmagdalena.gov.co, si ya existe un usuario con este nombre asignado en la cuenta de red de la Entidad, se agrega posterior a primerapellido la inicial del segundo apellido.

- **Servicio de correo electrónico:**

Permite a los funcionarios de la CGM, el intercambio de mensajes, a través de una cuenta de correo electrónico institucional, que facilita el desarrollo de sus funciones.

Principios guía

- Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.
- Los servicios de correo electrónico corporativo se emplean para servir a una finalidad operativa y administrativa en relación con la Entidad. Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura TIC de la CGM se consideran bajo el control de la entidad.
- Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la CGM y no debe utilizarse para ningún otro fin.
- No está autorizado el envío de cadenas de correo, envío de correos masivos con archivos adjuntos de gran tamaño que no sea información laboral de la entidad y que puedan congestionar la red.
- No está autorizado el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la entidad.

- Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire de la CGM, su cuenta de correo será desactivada.
- Los correos electrónicos deben contener el estándar establecido por la CGM para la firma y aviso legal respecto al manejo del contenido:

  La firma de los correos electrónicos está dividida en dos partes, al lado izquierdo se encuentra el logo de la entidad y al costado derecho se encuentran los siguientes datos:
  - Nombre completo del funcionario
  - Cargo del funcionario dentro de la entidad
  - El nombre de la entidad
  - Dirección de correo electrónico institucional del funcionario
  - Número de Teléfono fijo de la Entidad y la extensión (si aplica)
  - Número de teléfono celular
  - Dirección de la entidad ciudad y país
  - Dirección web de la entidad

  Y el aviso legal es el siguiente:
  "En virtud de lo establecido en la Ley 527 del 18 de agosto de 1999 y la Ley 962 del 8 de julio de 2005 (Ley antitrámites), la información diligenciada por este medio tiene total validez y es objeto de plena prueba.
  AVISO LEGAL: La información contenida en este mensaje y en los archivos electrónicos adjuntos es confidencial y reservada, conforme a lo previsto en la Constitución, y está dirigida exclusivamente a su destinatario, sin la intención de que sea revelada o divulgada a otras personas. El acceso al contenido de esta comunicación por cualquier otra persona diferente al destinatario no está autorizado por la CONTRALORÍA GENERAL DEL MAGDALENA y está sancionado de acuerdo con las normas legales aplicables".
- La Oficina de Acción Administrativa debe solicitar la creación o ajuste de las cuentas electrónicas para sus funcionarios o contratistas nuevos o antiguos
- La Oficina de Acción Administrativa es la responsable de solicitar la cancelación de las cuentas electrónicas al Área o la persona encargada de Tecnologías y Sistemas de Información de la CGM, por retiro de funcionario o término del contrato.

- Las cuentas de correo electrónico son propiedad de la CGM, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con la entidad, ya sea como funcionario o contratistas, consultores o personal temporal, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en la Entidad y no debe utilizarse para ningún otro fin.
- Cada funcionario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo, de acuerdo a la clasificación de la información establecida por la CGM.
- Todos los mensajes son sujetos a análisis frente a amenazas y ataques informáticos dirigidos, y pueden ser conservados, puestos en cuarentena y/o eliminados permanentemente por parte de la Entidad.
- Todo funcionario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asume la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo

Lineamientos de usos de dispositivos móviles

Los dispositivos móviles (teléfonos móviles, teléfonos inteligentes (Smartphone) tabletas, entre otros) ya sean personales o suministrados por la entidad, son una herramienta de trabajo que se deben utilizar únicamente para facilitar las comunicaciones de los usuarios de la entidad.

En los casos del uso de WhatsApp o Messenger de Facebook en la CGM, no se permite por estas aplicaciones el envío de fotografías, audios y videos y cualquier otro tipo de archivo clasificados como información pública reservada o información pública clasificada.

Los usuarios no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo, únicamente se deben aceptar y aplicar las actualizaciones.

Lineamientos para uso de mensajería instantánea y redes sociales

El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para un grupo reducido de funcionarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía.

No se permite el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de la CGM, que sea creado a **nombre personal** en redes sociales como: twitter®, facebook®, youtube®

likedink®, blogs, instagram, etc, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.
Toda información distribuida en las redes sociales que sean originadas por la entidad debe ser autorizada por los jefes de oficina para ser socializadas y con un vocabulario institucional.
No se debe utilizar el nombre de la entidad en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la institución.

Lineamiento para uso de discos o carpetas virtuales

La aprobación de funcionarios para obtener acceso a la información ubicada en los discos de red, debe ser mediante solicitud del Jefe inmediato del funcionario a el Área o persona encargada de Tecnologías y Sistemas de Información de la CGM, y en el caso de carpeta virtual el jefe inmediato del usuario deberá enviar un mensaje de correo electrónico institucional autorizando el acceso y permisos, en ambos casos correspondientes al rol y funciones a desempeñar.
Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red y las carpetas virtuales, dependiendo de la solicitud a las funciones y el rol asignado.
La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.
Está prohibido almacenar archivos Que incumplan leyes de derechos de autor, información no relacionada con las funciones asignadas al funcionario, información personal calificada como sensible de acuerdo con la ley 1581 de 2012, información de naturaleza intima del funcionario. Archivos que puedan ocasionar o constituir riesgos informáticos, como Software o código malicioso.
Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red o estaciones de trabajo, sin expresa autorización de su jefe inmediato.
Se prohíbe el uso de la información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial.

Lineamientos de uso de impresoras y del servicio de Impresión

Los documentos que se impriman en las impresoras de la CGM deben ser de carácter institucional.
Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner, impresora, fotocopiadora y multifuncionales) para que no se afecte su correcto funcionamiento.
Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar al Área o persona encargada de Tecnologías y Sistemas de Información.
Los funcionarios en el momento de realizar impresiones de documentos con clasificación pública reservada o información pública clasificada, debe

mantener control de la impresora, por lo cual no la deberán dejar desatendida, preservando la confidencialidad de la información.
No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.

Lineamientos de uso de puntos de red de datos (red de área local – LAN).

Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos Institucionales.
La instalación, activación y gestión de los puntos de red es responsabilidad del Área o la persona encargada de Tecnologías y Sistemas de Información

Lineamientos de escritorio y pantalla limpia.

Los funcionarios, contratistas, practicantes y terceros que tienen algún vínculo con la CGM debe conservar su escritorio libre de información propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
Los funcionarios de los sistemas de información de la CGM deben bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
Los usuarios de los sistemas de información de la CGM deben cerrar las aplicaciones y servicios de red cuando ya no los necesite.
Al imprimir documentos con información pública reservada y/o pública clasificada deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

Lineamiento de respaldo y restauración de información.

La restauración de copias de respaldo en cada oficina debe estar debidamente aprobada por el propietario de la información y solicitadas al área o la persona encargada de Tecnologías y Sistemas de Información de entidad encargada de administrar los backup.
Periódicamente la persona encarga de administrar los backup de la CGM, verificarán la correcta ejecución de los procesos de backup, suministrarán los medios (discos duros externos, memorias USB) requeridas para cada trabajo y controlarán la vida útil de cada medio empleado.
Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.
El administrador de backup de la entidad, debe generar tareas de restauración aleatorias de la información y deben ser documentadas.

Lineamiento para la Transferencia de Información.

La trasferencia de información física y digital entre oficinas se realiza mediante un oficio entre jefes de oficinas de acuerdo como ya está establecidos en la CGM, basados en la necesidad de la Entidad que permita automatizar servicios, fortaleciendo la gestión de la entidad.

La Entidad generará acuerdos de transferencia de información con organizaciones gubernamentales y privadas basados en la necesidad de la Entidad que permita automatizar servicios, fortaleciendo la gestión de la entidad.
El Área o persona encargada de Tecnologías y Sistemas de Información, realiza el control del uso de sistemas de transferencia de archivos vía FTP a terceros.

Lineamientos de manejo y disposición de información, medios y equipos

Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.
El servicio de acceso a Internet, Intranet, Sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo son propiedad de la Entidad y deben ser usados únicamente para el cumplimiento de la misión de la Entidad.
Se debe realizar la aplicación de backup, de borrado seguro y baja en los equipos de cómputo y demás dispositivos, una vez el funcionario haya sido retirado de la entidad o el equipo haya terminado su vida útil, de acuerdo a lo definido por la CGM.

Lineamientos de adquisición, desarrollo y mantenimiento de sistemas de información

En caso de desarrollos propios el Área o la persona encargada de Tecnologías y Sistemas de Información debe separar los ambientes de desarrollo, prueba y producción, en diferentes procesadores y dominios.
El Área o la persona encargada de Tecnologías y Sistemas de Información deberá realizar pruebas de funcionamiento y de seguridad a los nuevos sistemas, actualizaciones y/o aplicaciones en ambiente de pruebas, para validar la necesidad y operatividad de estos, previo a la aprobación e implementación.
El Área o persona encargada de Tecnologías y Sistemas de Información desarrollará y/o adquirirá el software requerido por la CGM; de manera coordinada con el Oficina que manifieste la necesidad del software, el Área o la persona encargada de Tecnologías y Sistemas de Información establecerá claramente los requerimientos funcionales, operacionales y especificaciones técnicas para la adquisición o desarrollo de sistemas de información y/o comunicaciones, contemplando requerimientos de seguridad de la información.
Todo hardware y software nuevo que se vaya a adquirir y conectar a la plataforma tecnológica de la CGM, por cualquier dependencia o proyecto de la entidad, deberá ser gestionado por el Área o la persona encargada de Tecnologías y Sistemas de Información para su correcto funcionamiento.

Todo aplicativo informático o software debe ser comprado con previa aprobación generada por el Área o la persona encargada de Tecnología y Sistemas de la Información en concordancia con la política de adquisición de bienes de la entidad.
Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.
El Área o persona encargada de Tecnologías y Sistemas de Información será la única dependencia autorizada para realizar copia de seguridad del software original.
La instalación del software en los activos informáticos de la CGM, se realizará únicamente a través del Área o persona encargada de Tecnologías y Sistemas de Información o bajo su supervisión.
El Área o persona encargada de Tecnologías y Sistemas de Información implementará reglas y herramientas que restrinjan la instalación de software no autorizado en los activos de información de la CGM.
El software proporcionado por el CGM no puede ser copiado o suministrado a terceros.
En los equipos de la CGM se podrá utilizar el software licenciado por el Área o persona encargada de Tecnologías y Sistemas de Información de la entidad y el adquirido o licenciado por los proyectos o programas que se encuentran en la CGM.
Para la adquisición y actualización de software, es necesario efectuar la solicitud al Área o la persona encargada de Tecnologías y Sistemas de Información con su justificación, quien analizará las propuestas presentadas para su evaluación y aprobación.
El software que se adquiera a través de proyectos o programas, debe quedar licenciado a nombre de la Contraloría General del Magdalena.
Se debe establecer los lineamientos para la supervisión y seguimiento a las actividades de desarrollo contratado, los cuales deben quedar inmersos en las clausulas y/o especificaciones técnicas de los contratos a ejecutar por la CGM.
Se encuentra prohibido el uso e instalación de juegos en los computadores de la CGM.
Para dar de baja el software Se presentarán solicitud de acuerdo con el procedimiento de Baja de Bienes de la entidad.
El Área o persona encargada de Tecnologías y Sistemas de Información debe implementar actividades para la protección contra códigos maliciosos y de reparación.
El Área o persona encargada de Tecnologías y Sistemas de Información debe implementar métodos y/o técnicas para el desarrollo de software seguro, estas deben incluir definiciones y requerimientos de seguridad, buenas prácticas para

desarrollo, que le permita a los desarrolladores aplicarlas de manera clara y eficiente.
El Área o persona encargada de Tecnologías y Sistemas de Información debe implementar y aplicar metodologías que permitan proteger las transacciones de los servicios de aplicaciones de la CGM.

Lineamiento para registro y seguimiento de eventos de sistemas de información y comunicaciones
El Área o persona encargada de Tecnologías y Sistemas de Información debe implementar los lineamientos para elaborar, preservar y revisar los registros de actividades de los usuarios de los sistemas de la CGM.
Los profesionales del Área o la persona encargada de Tecnologías y Sistemas de Información, no están facultados para modificar, borrar o desactivar registros de sus actividades propias, ni de los usuarios de los sistemas de información y/o telecomunicaciones, de igual forma se deben realizar las configuraciones de seguridad necesarias para evitar la eliminación o cambios no autorizados a los registros de información.
Lineamiento para la gestión de vulnerabilidades
El Área o persona encargada de Tecnologías y Sistemas de Información realizará pruebas técnicas de vulnerabilidad a intervalos planificados en los sistemas de información y comunicaciones de la CGM.
El Área o persona encargada de Tecnologías y Sistemas de Información implementará un programa de gestión de vulnerabilidades técnicas que incluya el **plan de tratamiento de vulnerabilidades**, el cual deberá ser aprobado por el Comité de Seguridad de la Información.
Lineamientos específicos para Web Master
Los responsables de los contenidos de las páginas Web (Web masters), deben preparar y verificar la información antes de que esta se cargue y se actualice la página de acuerdo a los lineamientos del sitio, y deben registrar en el formato de autorización de publicaciones, luego de verificada la publicación.
Los responsables de los contenidos de la Pagina Web deben reportar a la directiva los requerimientos de actualización de la versión del software que se requieran.
Se deberá seguir la Política Editorial y Actualización de Contenidos Web, que permita auditar la publicación o modificación de información oficial en las páginas web.
Las claves de acceso de los responsables de los contenidos de las páginas Web (Web masters), son estrictamente confidenciales, personales e intransferibles.
Lineamientos de Seguridad Física
La Oficina de Acción Administrativa debe implementar un sistema de seguridad física para las instalaciones de la CGM.

El Área o persona encargada de Tecnologías y Sistemas de Información debe tener implementadas alarmas de detección de intrusos a los centros de datos y centros de cableado de la CGM.
La oficina de Acción Administrativa de la CGM debe mantener actualizado el sistema de seguridad física de las instalaciones, así como el mantenimiento de las barreras de seguridad (Perimetrales e internas) de las instalaciones pertenecientes a la Entidad.
Se debe informar sobre las debilidades que encuentren a nivel de barreras físicas a la oficina de Acción Administrativa de la CGM para aprobación y corrección.

Políticas de seguridad y control de acceso al centro de datos y/o centros de cableado.

No se permite el ingreso al centro o lugar de cableado, al personal que no esté expresamente autorizado por el Jefe de Área o la persona encargada de Tecnologías y Sistemas de Información.
Se debe llevar un control de ingreso y salida del personal que visita o manipula el centro o lugar de cableado, en un Formato de Registro de ingreso, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.
Solo el Jefe del Área o persona encargada de Tecnologías y Sistemas de Información pueden autorizar el ingreso de computadores, dispositivos de comunicación y herramientas destinadas a las labores específicas de trabajo en el centro o lugar de cableado.
La grabación de vídeo en las instalaciones del centro o lugar de cableado debe estar expresamente autorizada por el comité de seguridad de la Información y exclusivamente con fines institucionales.
El Área o persona encargada de Tecnologías y Sistemas de la Información deberá garantizar que todos los equipos de los centros o lugar de cableado cuenten con un sistema alterno de respaldo de energía.
La limpieza y aseo del centro o lugar de cableado estará a cargo del Oficina de Acción Administrativa y debe efectuarse en presencia de un funcionario del Área o la persona encargada de Tecnología y Sistemas de la Información dela CGM. El personal de limpieza debe ser ilustrado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza. Debe prohibirse el ingreso de personal de limpieza con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.
En las instalaciones del centro de datos o de los centros de cableado, No está permitido:

- ✓ Fumar dentro del centro de datos o de los centros de cableado.
- ✓ Introducir alimentos o bebidas al centro de datos o de los centros de cableado.
- ✓ El porte de armas de fuego, corto punzantes o similares.

- ✓ Mover, desconectar y/o conectar equipo de cómputo sin autorización.
- ✓ Modificar la configuración del equipo o intentarlo sin autorización.
- ✓ Alterar software instalado en los equipos sin autorización.
- ✓ Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.
- ✓ Extraer información de los equipos en dispositivos externos.
- ✓ Abuso y/o mal uso de los sistemas de información.
- ✓ Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.
- ✓ Para el ingreso al centro o lugar de cableado se debe seguir los lineamientos de control de acceso
- ✓ Se debe seguir los lineamientos de seguridad física.

El centro o lugar de cableado debe estar provisto de:

- Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.
- Pisos elaborados con materiales no combustibles.
- Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración.
- Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
- Alarmas de detección de humo y sistemas automáticos de extinción de fuego. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.
- Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.
- El cableado de la red debe ser protegido de interferencias, por ejemplo usando canaletas que lo protejan.
- Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
- Las actividades de soporte y mantenimiento dentro del centro o lugar de cableado siempre deben ser supervisadas por un funcionario del Área o la persona encargada de Tecnologías y Sistemas de Información.

- Las puertas del centro o lugar de cableado deben permanecer cerradas; Si por alguna circunstancia se requiere ingresar y salir del centro o lugar de cableado, el funcionario responsable de la actividad se ubicará dentro del centro o lugar de cableado.
- Cuando se requiera realizar alguna actividad sobre algún armario, este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.
- Mientras no se encuentre personal dentro de las instalaciones del centro o lugar de cableado, las luces deben permanecer apagadas.
- Los equipos del centro o lugar de cableado que lo requieran, deben estar monitoreados para poder detectar las fallas que se puedan presentar.

Lineamientos de seguridad para los Equipos

- **Instalación de equipos de procesamiento y almacenamiento**
  - Los equipos de procesamiento y almacenamiento deben ser instalados en las áreas de trabajo seguras definidas por el Área o la persona encargada de Tecnologías y Sistemas de Información.
- **Protecciones en el suministro de energía**
  - A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como computadores, pantallas; los otros elementos deberán conectarse a la red no regulada. Esta labor debe ser revisada por la oficina de Acción Administrativa.
  - La Oficina de Acción Administrativa de la CGM debe implementar sistemas redundantes de alimentación eléctrica, como, por ejemplo: plantas generadoras de energía que permita soportar la operación de los sistemas de información durante una falta de suministro del proveedor de energía.
- **Seguridad del cableado**
  - Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
  - Deben existir planos que describan las conexiones del cableado.
  - El acceso al centro o lugar de cableado debe estar protegido.
  - El Área o persona encargada de Tecnologías y Sistemas de Información establece un programa de revisiones y/o inspecciones físicas al cableado, con el fin de detectar dispositivos no autorizados.

- **Mantenimiento de los Equipos**
  - La CGM debe mantener contratos de soporte y mantenimiento de los equipos.
  - Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada equipo.
  - Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser programadas y realizadas por personal autorizado por el Área o la persona encargada de Tecnologías y Sistemas de Información.
  - Los equipos que requieran salir de las instalaciones de la CGM para reparación o mantenimiento, deben estar debidamente autorizados por la oficina de Acción Administrativa y el Área o persona encargada de Tecnologías y Sistemas de Información y se debe garantizar que en dichos elementos no se encuentra información clasificada de acuerdo a los niveles de clasificación de la información pública reservada o información pública clasificada.
  - Para que los equipos puedan salir de las instalaciones, se debe suministrar un nivel mínimo de seguridad, que al menos cumpla con los requerimientos internos de la entidad, teniendo en cuenta los diferentes riesgos que se pueden presentar al trabajar en un ambiente que no cuenta con las protecciones ofrecidas en el interior de la CGM.
  - Los equipos retirados de la entidad deben ser protegidos, no se deben dejar sin vigilancia en lugares públicos, de igual forma se debe continuar con las recomendaciones de uso de los fabricantes de estos y la conexión con los sistemas de información de la CGM debe cumplir con la política de control acceso y de sistemas de información.
  - Cuando un dispositivo vaya a ser reasignado o retirado de servicio debe contar con aprobación del Área o persona encargada de Tecnologías y Sistemas de Información, así mismo debe garantizarse la eliminación de toda información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información, utilizando herramientas para realizar sobre-escrituras sobre la información existente o la presencia de campos magnéticos de alta intensidad realizando el Procedimiento de borrado seguro para equipos. Este proceso

puede además incluir, una vez realizado el proceso anterior, la destrucción física del medio, utilizando impacto, fuerzas o condiciones extremas.
    - El traslado entre dependencias de la CGM de todo activo de información, está a cargo de la Oficina de Acción Administrativa para el control de inventarios y bajo supervisión del Área o persona encargada de Tecnologías y Sistemas de Información.
- **Ingreso y retiro de activos de información de terceros.**
    - El retiro e ingreso de todo activo de información de propiedad de los funcionarios de la CGM, utilizados para fines personales, se realizará mediante los procedimientos establecidos en el control de acceso a las instalaciones de la entidad. La CGM no se hace responsable de los bienes o los problemas que se presenten al conectarse a la red eléctrica de la entidad.
    - El retiro e ingreso de todo activo de información de los visitantes que presten servicios a la CGM (consultores, practicantes, visitantes, proveedores etc.) será registrado e inspeccionado en los controles de accesos de las instalaciones de la Entidad. El personal de seguridad y vigilancia en los controles de acceso verificarán y registrarán las características de identificación del activo de información.
    - El traslado entre oficinas de la CGM de todo activo de información, está a cargo de la oficina de Acción Administrativa, para el control de inventarios.
- **Normas de protección**
    - Los funcionarios que hagan uso de los equipos de la CGM, no deben dejar desatendidos los equipos de cómputo en sitios públicos y deben transportarlos en lugares visibles bajo medidas que le provean seguridad física.
    - Los computadores portátiles siempre deben ser transportados como equipaje de mano, evitando golpes, exponerlo a líquidos, y prevenir la perdida y/o hurto.
    -

Lineamientos seguridad de las comunicaciones.
El Área o persona encargada de Tecnologías y Sistemas de Información debe implementar medidas para asegurar la disponibilidad de los recursos y servicios de red de la CGM.

El Área o persona encargada de Tecnologías y Sistemas de Información debe crear los estándares técnicos de configuración de la Red de la CGM y configuración de seguridad y de dispositivos de seguridad.
El Área o persona encargada de Tecnologías y Sistemas de Información debe implementar sistemas de protección entre las redes de la CGM y las redes externas no administradas por la entidad.
El Área o persona encargada de Tecnologías y Sistemas de Información debe identificar y documentar los servicios, protocolos y puertos autorizados en las redes de datos e inhabilitar o eliminar los servicios, protocolos y puertos no utilizados.
El Área o persona encargada de Tecnologías y Sistemas de Información debe segmentar la red, de modo que permita separar los grupos de servicios de información.

Lineamientos para la gestión de incidentes de seguridad de la información

La CGM establecerá responsables y procedimientos de gestión para el tratamiento de incidentes de seguridad de la información asegurando una respuesta rápida, eficaz y eficiente, quienes investigarán y solucionarán los incidentes presentados, implementando las acciones necesarias para evitar su repetición.
El Área o persona encargada de Tecnologías y Sistemas de Información responderá en primera instancia a los eventos o incidentes de seguridad informática, y se encargará junto con la oficina de Acción Administrativa de coordinar y adelantar las gestiones pertinentes para dar aviso a las autoridades.
Se debe establecer la implementación de lecciones aprendidas al término del análisis y solución de incidentes de seguridad de la información, estos deben ser socializados a los interesados conservando la confidencialidad de estas, así mismo, estas deben ser utilizadas como herramienta para la toma de decisiones y revisiones de la política de seguridad.

Lineamientos de Revisiones de Seguridad de la Información

La CGM realiza auditorias con personal externo a la entidad al sistema de gestión de seguridad de la información, para la verificación y cumplimiento del alcance, los controles, las políticas y lineamientos de seguridad de la Información.
Los Altos Directivos y/o Jefes de Oficina, deben verificar y supervisar el cumplimiento de las políticas de seguridad de la información en su área de responsabilidad.
La CGM asigna un funcionario para realizar revisiones esporádicas no programadas con el fin verificar el cumplimiento de las políticas de seguridad de la información en las instalaciones de la entidad y fuera de ella.
El Área o persona encargada de Tecnologías y Sistemas de Información debe establecer el procedimiento para revisar periódicamente los sistemas de

información con las herramientas automáticas y especialistas técnicos. (Colombia P. d., 2018)

14. CONCLUSIONES Y LINEAS FUTURAS

En la actualidad vemos como las TIC son parte primordial en cualquier organización en todos sus procesos desde los más minuciosos hasta los que representan un alto grado de importancia para entidades gubernamentales tales como la transparencia, la igualdad, la equidad y la participación ciudadana. Pero el uso de las TIC para las organizaciones trae consigo riesgos que exponen la seguridad de la información las cuales se desconocen por parte de las directivos, por los cuales no se proporcionan presupuestos y que pueden ocasionar daño o pérdida de información y económicos.

El desarrollo del diseño del Sistema de Gestión de Seguridad de la Información -SGSI- en la Contraloría General del Magdalena -CGM- basado en la norma ISO 27001 y la fase de planificación del modelo de seguridad y privacidad de la información -MSPI- de MINTIC ayudo a conocer los ya sabidos beneficios que incorpora un SGSI para la seguridad de la información de la entidad para lograr resguardar la confidencialidad, integridad y disponibilidad de los activos al diseñar las políticas de seguridad y establecer los lineamientos para el uso y las buenas prácticas de seguridad, además se logró identificar activos mediante la clasificación determinada en el formato de registro para el inventario.

En términos generales para mí fue una experiencia muy enriquecedora el poder hacer mis prácticas en una entidad pública como es la Contraloría General del Magdalena donde además de tener como jefe inmediata a la Ingeniera **Lizette de Armas** egresada del alma mater de la Universidad del Magdalena de quien pude aprender mucho de su experiencia y conocimiento y a quien le agradezco por su apoyo, también pude poner en practica aspectos aprendido en

asignaturas de ingeniería aplicada para administración de tecnologías de la información como son: Diseño Organizacional TI, planeación estratégica informática, gobierno de TIC y hasta legislación de informática, donde además pude investigar sobre la norma ISO 270001 y darme cuenta como se viene desarrollando el tema de seguridad de la información en el país en los últimos años y como el gobierno nacional a través del ministerio de las tecnologías de información y las comunicaciones con estrategias como gobierno en línea promueve la construcción de un Estado más eficiente, transparente y participativo haciendo una de las tecnologías en la gestión públicas y específicamente pude conocer y estudiar la guía del Modelo de Seguridad y Privacidad de la Información que el MinTIC tiene para las entidades del Estado. En conclusión se puede determinar que el diseño de la fase de planificación del SGSI para la CGM es un punto de partida muy importante para una futura implementación del sistema, que a largo plazo generara grandes beneficios y ayudara a garantizar la gestión de los procesos de la entidad contribuyendo a la gestión de calidad y a la implementación de buenas prácticas establecidas por el Gobierno Nacional a través del Ministerio de las Tics mediante su programa de gobierno en línea.

15. BIBLIOGRAFÍA

Bibliografía

Aprende, C. (Junio de 2016). *https://www.colombiacompra.gov.co*. Obtenido de https://www.colombiacompra.gov.co/sites/cce_public/files/cce_documentos/20160623alcancedelsgsi.pdf

CGM. (Julio de 2018). *http://www.contraloriadelmagdalena.gov.co*. Obtenido de http://www.contraloriadelmagdalena.gov.co/nuestra-entidad/

CGM2. (Julio de 2018). *http://www.contraloriadelmagdalena.gov.co*. Obtenido de http://www.contraloriadelmagdalena.gov.co/estructura-organica/

CGM3. (Julio de 2018). *http://www.contraloriadelmagdalena.gov.co*. Obtenido de http://www.contraloriadelmagdalena.gov.co/wp-content/uploads/2017/08/PLAN-ESTRATEGICO-16-19-CGM10082017_0001.pdf

Colombia, P. d. (2018). *http://es.presidencia.gov.co*. Obtenido de http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/Forms/AllItems.aspx

Colombia, U. C. (Noviembre de 2013). *https://repository.ucatolica.edu.co*. Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/1305/1/RIESGOS%20AMENAZAS%20Y%20VULNERABILIDADES%20DE%20LOS%20SISTEMAS%20DE%20INFORMACION%20GEOGRAFICA%20GPS.pdf

MinTic. (Abril de 2016). *http://www.mintic.gov.co*. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

MinTic2. (Mayo de 2016). *http://www.mintic.gov.co*. Obtenido de http://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

16. ANEXOS

FORMATO PARA EL REGISTRO DE INVENTARIO DE ACTIVOS DE INFORMACION DE LA CONTRALORIA GENERAL DEL MAGDALENA

	REGISTRO DE ACTIVOS DE INFORMACIÓN **CONTRALORIA DEPARTAMENTAL DEL MAGDALENA**

Nombre del proceso			**Área responsable**		
Nombre del responsable			**Cargo del responsable**		
Nombre del enlace de la dirección u oficina			**Clasificación del documento**		
Idioma	ESPAÑOL				

INFORMACIÓN ACTIVOS																					
IDENTIFICACIÓN DEL ACTIVO					**UBICACIÓN** ***(información publicada o disponible)***			**CLASIFICACIÓN**				**PROPIEDAD**		**TIPO DE ORIGEN**		**ACCESO**	**GESTIÓN**		**INFORMACIÓN PÚBLICA O DISPONIBLE**	**OBSERVACIONES**
Código del activo	**Nombre del Procedimiento**	**Nombre del activo**	**Descripción *(descripción del contenido de la***	**Tipo INF - Información SOF - Software HDW -**	**Física**	Tecnológica	**Formato**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Criticidad**	**Propietario**	**Custodio**	**Interno/Externo**	**Oficina/Entidad**	**Usuarios**	**Fecha de Ingreso**	**Fecha de Salida**		

		categoría de la información)	**Hardware SER - Servicios RH - Recursos Humano INT - Intangible OTR - Otros**																	

DESCRIPCION DEL FORMATO PARA EL REGISTRO DE INVENTARIO DE ACTIVOS DE INFORMACION DE LA CONTRALORIA GENERAL DEL MAGDALENA

CODIGO DEL ACTIVO: Número consecutivo único que identifica al activo en el inventario. Conformado a partir del código del procedimiento, la sigla del tipo de activo y un consecutivo (de dos dígitos). Ejemplo: M-PD-086-INF-01.

NOMBRE DEL PROCEDIMIENTO: Nombre del proceso al que pertenece el activo.

NOMBRE DEL ACTIVO: Nombre de identificación del activo dentro del proceso al que pertenece.

DESCRIPCIÓN/OBSERVACIONES: Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.

TIPO: Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores:

- **INFORMACIÓN:** Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
- **SOFTWARE:** Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
- **HARDWARE:** Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.
- **SERVICIO:** Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.
- **RECURSO HUMANO:** Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.

- **INTANGIBLE:** Son aquellos que tienen que ver con la imagen y la reputación de la entidad; son inmateriales.
- **OTROS:** activos de información que no corresponden a ninguno de los tipos descritos anteriormente pero deben ser valorados para conocer su criticidad al interior del proceso.

UBICACIÓN: Describe la ubicación tanto física como electrónica del activo de información, y el formato en el que se encuentra almacenado. Esta característica consta de tres campos que son los siguientes:

- **FISICA:** Especifica detalladamente el lugar exacto (Edificio, piso, costado, área, archivador y sector) donde se encuentra el activo de información, bajo custodia del Custodio de la información, por ejemplo: archivadores, planotecas, archivos de gestión, centro de cómputo, bodegas de almacenamiento con terceros y oficinas.
- **TECNOLOGICA:** Especifica la ubicación de los activos de información digitales (electrónico), bajo custodia del Custodio de la información, tales como: computadores, dispositivos de almacenamiento internos y externos, carpeta pública o privada, sistema de información, equipo de escritorio (dirección IP), nombre del servidor (base de datos, aplicaciones) o url. Si la información no es almacenada digitalmente, indicar N/A.
- **FORMATO:** Este campo aplica cuando la ubicación es digital, en ese caso puede ser doc, xls, pdf, etc. si la ubicación es física se coloca N/A.

CLASIFICACIÓN: Hace referencia a la protección de información de acuerdo a Confidencialidad, Integridad y Disponibilidad.

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
IPR: INFORMACIÓN PUBLICA RESERVADA	**ALTA (A)**	**ALTA (1)**
IPC: INFORMACIÓN PUBLICA CLASIFICADA	**MEDIA (M)**	**MEDIA (2)**
IPB: INFORMACIÓN PÚBLICA (BASICA)	**BAJA (B)**	**BAJA (3)**
NO CLASIFICADA	**NO CLASIFICADA**	**NO CLASIFICADA**

- **CLASIFICACIÓN DE ACUERDO CON LA CONFIDENCIALIDAD:** La confidencialidad se refiere a que la información no esté disponible ni sea

revelada a individuos, entidades o procesos no autorizados, Esta se debe definir de acuerdo con las características de los activos que se manejan en cada entidad, a manera de ejemplo en la guía se definieron tres (3) niveles alineados con los tipos de información declarados en la ley 1712 del 2014:

INFORMACION PUBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACION PUBCLCA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACION PÚBLICA (BASICA)	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

- **CLASIFICACIÓN DE ACUERDO CON LA INTEGRIDAD:** La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. En esta guía se recomienda el siguiente esquema de clasificación de tres (3) niveles:

A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar

	sus funciones, o generar pérdidas de imagen severas de la entidad.
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

- **CLASIFICACIÓN DE ACUERDO CON LA DISPONIBILIDAD:** La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso. En esta guía se recomienda el siguiente esquema de clasificación de tres (3) niveles:

1 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
3 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o

	entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA

CRITICIDAD: Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información:

- **ALTA:** Activos de información en los cuales la clasificación de la información en dos o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
- **MEDIA:** Activos de información en los cuales la clasificación de la información es alta en una de sus propiedades (confidencialidad, integridad, y disponibilidad) o al menos una de ellas es de nivel medio.
- **BAJA:** Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

PROPIEDAD

- **PROPIETARIO:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. Deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.
- **CUSTODIO:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los funcionarios o el proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original).

TIPO DE ORIGEN

- **EXTERNO/INTERNO:** De donde proviene el activo. Interno cuando el activo proviene de dentro de la misma entidad y externo cuando proviene de fuera de la entidad.
- **ENTIDAD/OFICINA:** cuando es externo se describe el nombre de la entidad de donde proviene el activo y si es interno se describe el nombre de la oficina de donde proviene.

ACCESO

- **USUARIOS:** Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.

GESTIÓN

- **FECHA INGRESO DEL ACTIVO:** Fecha de ingreso del activo de información en el inventario
- **FECHA SALIDA DEL ACTIVO:** Fecha de exclusión del activo de información del inventario.

TABLA DE CONTROLES

CONTROLES DEL ANEXO A DEL ESTÁNDAR ISO/IEC 27001:2013

El Sistema de Gestión de Seguridad de la Información en su fase de Planificación se realiza la selección de controles, y durante la fase Implementación se ejecuta la implementación de controles de seguridad de la información, por lo cual se cuenta con el anexo de controles del estándar ISO 27002.

Núm.	Nombre	Descripción / Justificación
1	Objeto y campo de aplicación	Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información - SGSI
2	Referencias normativas	La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación.
3	Términos y definiciones	Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.
	Políticas de seguridad de la información	
A.5.1	Directrices establecidas por la dirección para la seguridad de la información	Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
A.5.1.1	Políticas para la seguridad de la información	Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.

A.5.1.2	Revisión de las políticas para seguridad de la información	Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
A.6	Organización de la seguridad de la información	
A.6.1	Organización interna	Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
A.6.1.1	Roles y responsabilidades para la seguridad de información	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades	Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2	Dispositivos móviles y teletrabajo	Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.
A.6.2.1	Política para dispositivos móviles	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo	Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o

		almacenada en los lugares en los que se realiza teletrabajo.
A.7	Seguridad de los recursos humanos	
A.7.1	Antes de asumir el empleo	Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
A.7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2	Durante la ejecución del empleo	Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
A.7.2.1	Responsabilidades de la dirección	Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.7.2.3	Proceso disciplinario	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

A.7.3	Terminación o cambio de empleo	Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.
A.8	Gestión de activos	
A.8.1	Responsabilidad por los activos	Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
A.8.1.1	Inventario de activos	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deberían tener un propietario.
A.8.1.3	Uso aceptable de los activos	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2	Clasificación de la información	Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
A.8.2.1	Clasificación de la información	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.8.2.2	Etiquetado de la información	Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de

		clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos	Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.8.3.1	Gestión de medios removibles	Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
A.8.3.2	Disposición de los medios	Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9	Control de acceso	
A.9.1	Requisitos del negocio para control de acceso	Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.
A.9.1.1	Política de control de acceso	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Política sobre el uso de los servicios de red	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
A.9.2	Gestión de acceso de usuarios	Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
A.9.2.1	Registro y cancelación del registro de usuarios	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios	Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de

		acceso a todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.
A.9.3	Responsabilidades de los usuarios	Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
A.9.3.1	Uso de la información de autenticación secreta	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.9.4	Control de acceso a sistemas y aplicaciones	Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.
A.9.4.1	Restricción de acceso Información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
A.9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
A.9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios

		que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A.9.4.5	Control de acceso a códigos fuente de programas	Control: Se debería restringir el acceso a los códigos fuente de los programas.
A.10	Criptografía	
A.10.1	Controles criptográficos	Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
A.10.1.1	Política sobre el uso de controles criptográficos	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
A.11	Seguridad física y del entorno	
A.11.1	Áreas seguras	Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
A.11.1.1	Perímetro de seguridad física	Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
A.11.1.2	Controles físicos de entrada	Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras	Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.

A.11.1.6	Áreas de despacho y carga	Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2	Equipos	Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
A.11.2.1	Ubicación y protección de los equipos	Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
A.11.2.2	Servicios de suministro	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.
A.11.2.4	Mantenimiento de equipos	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de activos	Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.

A.11.2.8	Equipos de usuario desatendidos	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12	Seguridad de las operaciones	
A.12.1	Procedimientos operacionales y responsabilidades	Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
A.12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios	Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.12.1.3	Gestión de capacidad	Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2	Protección contra códigos maliciosos	Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.12.2.1	Controles contra códigos maliciosos	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
A.12.3	Copias de respaldo	Objetivo: Proteger contra la perdida de datos.

A.12.3.1	Respaldo de información	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
A.12.4	Registro y seguimiento	Objetivo: Registrar eventos y generar evidencia.
A.12.4.1	Registro de eventos	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.
A.12.4.4	sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.
A.12.5	Control de software operacional	Objetivo: Asegurar la integridad de los sistemas operacionales.
A.12.5.1	Instalación de software en sistemas operativos	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
A.12.6	Gestión de la vulnerabilidad técnica	Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.

A.12.7	Consideraciones sobre auditorias de sistemas de información	Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.
A.12.7.1	Información controles de auditoría de sistemas	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
A.13	Seguridad de las comunicaciones	
A.13.1	Gestión de la seguridad de las redes	Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
A.13.1.1	Controles de redes	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.
A.13.2	Transferencia de información	Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
A.13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación
A.13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.

A.13.2.3	Mensajería electrónica	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14	Adquisición, desarrollo y mantenimientos de sistemas	
A.14.1.1	Requisitos de seguridad de los sistemas de información	Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
A.14.2	Seguridad en los procesos de desarrollo y soporte	Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
A.14.2.1	Política de desarrollo seguro	Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de

		sistemas, a los desarrollos que se dan dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.
A.14.2.5	Principios de construcción de sistemas seguros	Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente	Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.
A.14.3	Datos de prueba	Objetivo: Asegurar la protección de los datos usados para pruebas.

A.14.3.1	Protección de datos de prueba	Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.
A.15	Relación con los proveedores	
A.15.1	Seguridad de la información en las relaciones con los proveedores	Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
A.15.2	Gestión de la prestación de servicios con los proveedores	Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
A.15.2.2	Gestión de cambios en los servicios de proveedores	Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del

		negocio involucrados, y la revaloración de los riesgos.
A.16	Gestión de incidentes de seguridad de la información	
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
A.16.1.1	Responsabilidad y procedimientos	Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

A.17	Aspectos de seguridad de la información de la gestión de continuidad de negocio	
A.17.1	Continuidad de seguridad de la información	Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2	Redundancias	Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.18	Cumplimiento	
A.18.1	Cumplimiento de requisitos legales y contractuales	Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos

		actualizados para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual	Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3	Protección de registros	Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de datos personales	Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
A.18.1.5	Reglamentación de controles criptográficos	Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2	Revisiones de seguridad de la información	Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
A.18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas

		de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.