GOBERNACION DEL MAGDALENA

OFICINA DE TECNOLOGIAS DE LA INFORMACION – ÁREA FUNCIONAL DE SISTEMAS

PRELIMINAR PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

SANTA MARTA., ENERO DE 2020

OBJETIVOS

Definir y describir el Modelo de Seguridad y Privacidad de la Información permitiendo la integridad, disponibilidad y confidencialidad de los activos de información y comunicación, comprometiendo a todo el talento humano de la Gobernación del Magdalena en los procesos de seguridad, convirtiéndose en una guía que permitirá informar sobre las normas y procedimientos orientados a la seguridad de la información.

ALCANCE

El Plan de Seguridad y Privacidad de la Información se aplica a todos los procesos y procedimientos de las diferentes dependencias de la Gobernación del Magdalena, que para su realización, los servidores públicos se apoyen en tecnologías de la Información o recursos tecnológicos, de igual manera a todos los funcionarios y contratistas de la entidad.

Este plan incluye controles preventivos y correctivos para incidencias de seguridad de la información en: Ataques maliciosos externos, Ataques maliciosos internos, Acceso a la red por personas no autorizadas, acceso físico no autorizado, roles del sistema.

Administración de red inadecuada, cambio de datos no intencionado en un sistema de información, copias de seguridad defectuosas, destrucción de archivos, extracción de información, falsificación de archivos, instalación de software no autorizado, Ilegalidad en Licenciamientos, mal uso de sistemas de información, mal uso de recursos de red, pérdidas de conectividad, pérdida de Contraseñas, pérdida de Código fuente de desarrolladas internamente.

MARCO NORMATIVO

Ley 527 de 1999: Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.

Ley 594 de 2000: Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.

CONPES 3701 de 2011: Lineamientos de política para ciberseguridad y Ciberdefensa

Ley 1581 de 2012: Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.

Ley 1221 de 2008: Promover y regular el teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones.

Ley 1712 de 2014: Ley de transparencia y del derecho de acceso a la Información pública nacional.

La Ley 1581 de 2012 y decreto 1377 de 2013. Ley de protección de datos personales.
Ley 1273 de 2009. Ley de delitos informáticos y la protección de la información y de los datos.

Decreto 1078 de 2015. Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Alcance: Ámbito de la organización que queda sometido al SGSI.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

Control detectivo: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Control disuasorio: Control que reduce la posibilidad de materialización de una amenaza.

Estimación de riesgos: Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Gestión de activos: Busca proteger los activos de información, controlando el acceso solo a las personas que tienen permiso de acceder a los mismos, tratando que cuenten con un nivel adecuado de seguridad.

Gestión de comunicaciones y operaciones: Esta sección busca asegurar la operación correcta de los equipos, así como la seguridad cuando la información se transfiere a través de las redes, previniendo la pérdida, modificación o el uso erróneo de la información.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje, la información, ya sea impresa, almacenada digitalmente o hablada actualmente es considerada como un activo dentro de las compañías y que se debe proteger, ya que es de gran importancia.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual: El riesgo que permanece tras el tratamiento del riesgo.

Sistema de Gestión de la Seguridad de la Información: establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

Seguridad de los recursos humanos: Orientado a reducir el error humano, ya que en temas de seguridad, el usuario es considerado como el eslabón más vulnerable y por el cual se dan los principales casos relacionados con seguridad de la información, busca capacitar al personal para que puedan seguir la política de seguridad definida, y reducir al mínimo el daño por incidentes y mal funcionamiento de la seguridad.

ROLES Y RESPONSABLES

Para efectos de garantizar la funcionalidad de las acciones necesarias para proteger, preservar y administrar la información y las herramientas tecnológicas, es necesario definir roles y responsabilidades de cada una de las oficinas que intervienen en su desarrollo.

El Gobernador aprobará la política y sus modificaciones, una vez revisada por la oficina de **TECNOLOGÍAS DE LA INFORMACIÓN** Y EL **ÁREA FUNCIONAL DE SISTEMAS**.

La oficina de TI y el área funcional de Sistemas, velarán por la creación del Comité de Seguridad y Privacidad de la Información, y propondrán y revisarán el texto de la política, estructuración y seguimiento.

El Jefe de la Oficina de Tecnología de la Información y el Responsable del Área de Sistemas se encargarán de coordinar las acciones e impulsar la implementación y cumplimiento de la política y definir estrategias de publicidad al interior de la entidad.

Los secretarios de despacho, directores y jefes de oficina velarán por el cumplimiento de las normas establecidas e informarán a la Oficina TI y el área de Sistemas, de los cambios o rotación de personal para desactivar los servicios informáticos que tengan asignados.

El Jefe de Control Interno evaluará que los funcionarios públicos estén aplicando la Política de Seguridad y Privacidad de la Información.

El Jefe de Talento Humano velará que todo el personal vinculado a la administración (carrera administrativa, libre nombramiento, provisional o contratista) haga lo necesario para cumplir con la Política de Seguridad y

Privacidad de la Información, y junto con la Oficina TI y el Área de Sistemas, socializará y capacitará al personal en lo referente a la política que se desarrolle.

La Oficina Asesora Jurídica asesorará en materia legal a la entidad en los temas relacionados con la política.

Responsables de activos de información Los secretarios de despacho o jefes de oficina que tengan a cargo sistemas de información, conservarán la integridad y confidencialidad de la información, así como definirán que usuarios deben tener permisos de acceso a la información. Todos los usuarios que hayan sido autorizados para acceder a los recursos tecnológicos y procesamiento de la información, son responsables del cumplimiento de los procedimientos definidos en la misma.

PRINCIPIOS ENSEGURIDAD DE LA INFORMACION

- La responsabilidad ante la seguridad de la información será definida, compartida y publicada, y debe ser acatada por todos los funcionarios públicos.
- Proteger la información generada, procesada y almacenada, al igual que los activos de información que hacen parte de la entidad, a fin de minimizar los impactos financieros, operativos o legales por su uso incorrecto. Por ello es fundamental la aplicación de controles de acuerdo a la clasificación de la información.
- Se protegerá la información de las amenazas originadas por parte de los servidores públicos, de terceros y personal externo.
- Se resguardará y protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta los procesos críticos.
- La entidad implementará control de acceso a la información, sistemas y recursos de red.
- Se controlará la operación de los procesos garantizando la seguridad de los recursos tecnológicos y de redes de datos.

MATRIZ DE RIESGOS

CALIFICACIÓN DE LA PROBABILIDAD				
No	Activo	Riesgo	Descripción de Riesgo	Probabilidad
1	Página Web Institucional	Pérdida de la confidencialidad		
		Pérdida de la integridad	Pérdida de la integridad de la información o modificaciones no autorizadas por accesos o ataques maliciosos	IMPROBABLE
		Pérdida de disponibilidad	Interrupción de la operación de la página web y restricciones en el acceso de manera temporal	IMPROBABLE
2	Correos Electrónicos Institucionales	Pérdida de la confidencialidad	Filtración de información institucional hacia terceros no autorizados	IMPROBABLE
		Pérdida de la integridad	0	
		Pérdida de disponibilidad	Jaqueo de las cuentas de correos electrónicos que implican restricciones en el acceso y/o bloqueo temporal	IMPROBABLE

3	Copias de Seguridad de los equipos y/o Programas	Pérdida de la confidencialidad	Exposición de información que reposa en las copias de seguridad	IMPROBABLE
		Pérdida de la integridad	Alteración de la información que reposa en las copias de seguridad	IMPROBABLE
		Pérdida de disponibilidad	Daños en los medios de almacenamiento de las copias de seguridad	PROBABLE
4	Formulario Electrónico de PQR	Pérdida de la confidencialidad	Exposición indebida de información clasificada y datos personales de los usuarios	IMPROBABLE
		Pérdida de la integridad	0	
		Pérdida de disponibilidad	Inoperancia temporal de la formulario electrónico de peticiones, quejas, reclamos y sugerencias	IMPROBABLE
5	Portal Bancario	Pérdida de la confidencialidad	Filtración de información de claves de acceso o sobre transacciones	IMPROBABLE
		Pérdida de la integridad	0	

		Pérdida de disponibilidad	Bloqueo de cuenta de acceso al portal bancario	PROBABLE
6	Software Humano (Talento Humano)	Pérdida de la confidencialidad	Filtración de información sensible de los funcionarios	IMPROBABLE
		Pérdida de la integridad	Alteración de información de nómima, liquidaciones, historias labores y/o de trazabilidad de la gestión laboral	POSIBLE
		Pérdida de disponibilidad	Inutilidad parcial o temporal del software	IMPROBABLE
7	Software financiero (SIIAF)	Pérdida de la confidencialidad	Filtración de información sensible de las operaciones financieras	IMPROBABLE
		Pérdida de la integridad	Alteración de información de financiera: contable,de tesorería y presupuestal.	IMPROBABLE
		Pérdida de disponibilidad	Inutilidad parcial o temporal del software financiero	PROBABLE
8	Grupo de Funcionarios Sistemas de la	Pérdida de la confidencialidad	0	

	Gobernación	Pérdida de la integridad	0	
		Pérdida de disponibilidad	Inoperancia e incumplimiento en las actividades operativas: preventivas y reactivas del equipo humano de sistemas	CASI SEGURO
9	Red de ordenadores	Pérdida de la confidencialidad	0	
		Pérdida de la integridad	0	
		Pérdida de disponibilidad	Inutilidad parcial o total de la red de ordenadores	PROBABLE
10	Equipos de cómputos (De escritorio y portátiles)	Pérdida de la confidencialidad	Exposición de la información contenida en los equipos de cómputo	CASI SEGURO
		Pérdida de la integridad	Adulteración en la información contenida en los equipos de cómputo	PROBABLE
		Pérdida de disponibilidad	Inutilidad de los equipos de cómputo	CASI SEGURO

11	Equipos tecnológicos (scanner, impresoras, video bean, Reuters, accesorios)	Pérdida de la confidencialidad	0	
		Pérdida de la integridad	0	
		Pérdida de disponibilidad	Inutilidad de los equipos tecnológicos	PROBABLE
12	Software INFODOC de Gestión Documental	Pérdida de la confidencialidad	Filtración de información sensible	IMPROBABLE
		Pérdida de la integridad	Alteración de información institucional	IMPROBABLE
		Pérdida de disponibilidad	Inutilidad parcial o temporal del software de gestión documental	PROBABLE
13	Aplicativos Web nacionales administrado por las diversas secretarias o áreas (SISPRO, ADRES,	Pérdida de la confidencialidad	0	
		Pérdida de la integridad	0	

	SUPERSALUD , SEPPI, SIMIT, ETC)	Pérdida de disponibilidad	Bloqueo de cuenta de acceso a los portales o aplicativos web	IMPROBABLE
14	Internet Corporativo	Pérdida de la confidencialidad	0	
		Pérdida de la integridad	0	
		Pérdida de disponibilidad	Interrupción de la conexión a internet	IMPROBABLE
15	Firmas Digitales	Pérdida de la confidencialidad	0	
		Pérdida de la integridad	Legalización de documentos sin autorización del propietario de la firma digital	RARA VEZ
		Pérdida de disponibilidad	Daño o pérdida de toquen o claves de acceso para la firma digital de documentos	RARA VEZ
16	Software de Tránsito	Pérdida de la confidencialidad	Filtración de información sensible de los datos de los usuarios del Sistema Nacional de Tránsito	IMPROBABLE

		Pérdida de la integridad	Alteración de información del Sistema Nacional de Tránsito en el orden Departamental	IMPROBABLE
		Pérdida de disponibilidad	Inutilidad parcial o temporal del software de Tránsito	POSIBLE
17	Sistema operativos y herramientas ofimáticas	Pérdida de la confidencialidad	0	
		Pérdida de la integridad	Afectación con virus del sistema operativo, pogramas o herramientas ofimáticas licenciadas	PROBABLE
		Pérdida de disponibilidad	Inutilidad parcial o total de los equipos de cómputo por daño en el sistema operativo o herramientas ofimáticas	PROBABLE
18	Bases de Datos de las dependencias	Pérdida de la confidencialidad	Exposición de información que reposa en las Bases de Datos corporativas	POSIBLE
		Pérdida de la integridad	Alteración de la información que reposa en las bases de datos	POSIBLE
		Pérdida de disponibilidad	Daños en los medios de almacenamiento de las bases de datos	PROBABLE

19	Sistema de Cortafuegos	Pérdida de la confidencialidad	Filtración hacia información sensible de la entidad	CASI SEGURO
		Pérdida de la integridad	0	
		Pérdida de disponibilidad	0	
20	Sistema de antivirus	Pérdida de la confidencialidad	0	
		Pérdida de la integridad	0	
		Pérdida de disponibilidad	Afectación con virus del sistema operativo, pogramas o utilidades.	CASI SEGURO

POLITICA DE SEGURIDAD DE LA INFORMACION

Esta política plantea la necesidad de la implementación de un sistema de gestión de seguridad de la información en la entidad. Esta política es la posición de la Gobernación hacia el tema de la protección de los activos de información que soportan los procesos de la entidad.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno Digital, permite alinearse al componente de TIC para el Estado al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.
Y se alinea al componente de TIC para la Sociedad apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Gobernación del Magdalena, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

SEGURIDAD PARA EL RECURSO HUMANO

La Oficina de Talento Humano deberá investigar los antecedentes y estudios realizados por las personas que aspiran un cargo y que su perfil esté acorde a las responsabilidades y funciones del cargo.

El jefe de cada dependencia promoverá entre los funcionarios a su cargo el conocimiento de las políticas de seguridad de la información, con el fin de poder mitigar riesgos o pérdida de información.

GESTION DE ARCHIVOS

La Gobernación del Magdalena es el dueño de toda información que se genere, procese o almacene dentro y en los servicios de cloud propios o tercerizados por la entidad a través de los funcionarios públicos o contratistas.

La entidad mantendrá un inventario de sus activos de información actualizado, que será administrado por la Oficina de Almacén y la Oficina de TI, y cada secretaría u oficina brindará el apoyo necesario para recopilar la información que permita mantener actualizado el inventario de activos de información.

El área de sistemas revisará los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considerada como una violación a la Política de Seguridad y Privacidad de la Información de la entidad.

Los responsables de los procesos de las secretarías y oficinas deben generar un análisis de riesgos en temas de seguridad de la información.

Cuando se requiera un aplicativo, sistema de información o equipo de cómputo, debe ser solicitado al área de sistemas, con su correspondiente justificación para validar su viabilidad.

La Oficina de Tecnología de la Información será quien custodie el software, manuales y licencias de uso de los equipos de cómputo, sistemas de información o aplicativos.

No está permitido a los servidores públicos instalar o copiar software, al igual que extraer o instalar hardware en los equipos de la entidad sin previa autorización o supervisión de la Oficina TI.

Los jefes de cada oficina deben informar a la Oficina TI sobre cualquier anomalía, violación o incidente en contra de los activos de información.

Las acciones que se generen dentro de las cuentas de los usuarios, será responsabilidad únicamente del funcionario al cual esté vinculada dicha cuenta.

Todo funcionario desvinculado o trasladado debe hacer entrega de los activos de información en medio físico como magnético al jefe de cada dependencia.

SEGURIDAD FISICA Y DEL ENTORNO

Áreas Seguras:

La Secretaría General identificará las áreas o dependencias que procesan o almacenan información sensible o crítica para fortalecer los controles y evitar el ingreso de personal no autorizado, Con apoyo del Área de Sistemas y la Oficina TI y se instalarán sistemas de control de acceso.

Todo personal, sin importar su vinculación deberá portar el carnet en lugar visible mientras permanezca dentro de las instalaciones de la entidad.

Las instalaciones de la entidad, cuando se requiera, deben estar dotadas con cámaras de tv para monitorear y registrar las actividades de los funcionarios, contratistas y terceros.

Seguridad de los equipos

La ubicación de los equipos de computación deben estar en áreas de trabajo que permitan la seguridad de los mismos, evitando el ingreso de personal no autorizado y riesgos como humedad, goteras o acceso de polvo y deben estar conectados a una red regulada de energía para protegerlos de los picos de luz o fallas en el suministro.

Las áreas de Recursos Físicos y Sistemas, realizarán revisiones periódicas al cableado eléctrico y de datos, para mantener el normal funcionamiento de los servicios y evitar interferencias o fallas. Además, se debe asegurar un respaldo de energía automático en caso de falla del suministro, para permitan tomar acciones para salvaguardar los servicios informáticos.

Se realizará mantenimiento preventivo a los equipos de compúto de las dependencias para mantener la integralidad de los datos.

El registro de ingreso y salida de equipos electrónicos se realizará en un libro de control a la entrada de cada una de las sedes de la Gobernación.

SEGURIDAD DE LAS OPERACIONES TI

Controles contra códigos maliciosos

El área de sistemas, diseñará e implementará soluciones que propendan por salvaguardar los equipos de cómputo asignados a los funcionarios y contratistas de la entidad, propendiendo porque éstos, estén protegidos por software contra código malicioso.

Procesos Documentados

El Área de Sistemas de la Gobernación del magdalena, en coordinación con la oficina de TI, deben velar por la elaboración de documentos soportes acerca del desarrollo de los procesos misionales del área de sistemas.

Copias de Seguridad (Backup)

El área de sistemas desarrollará los procesos de copias de seguridad de las bases de datos de los sistemas de información principales de la entidad, los cuales sean gestionados y administrados por dicha área.

Seguridad en las redes

La transferencia de información está expuesta a múltiples riesgos, por ello la entidad debe implementar medidas preventivas para evitar su divulgación o modificación. Para lograr esto la Gobernación debe: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte y mantener la seguridad de la información transferida dentro de la entidad y con cualquier entidad externa.

Gestión de Incidentes de Seguridad

Construir un proceso consistente para gestionar los incidentes de seguridad de la información, el cual debe contener como mínimo:

- Reporte de incidente de seguridad de la información
- Investigación de incidente de seguridad de la información
- Adecuado control de cadena de custodia para gestión de evidencias.

La adecuada gestión de los incidentes de seguridad de la información permite proteger los tres pilares de la seguridad: la confidencialidad, la integridad y la disponibilidad de la información. La implementación de estos controles permite 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.

FABIÁN BOLAÑO
Ingeniero de Sistemas
Jefe Oficina TI

ERICK JAVIER ARIZA
Ingeniero de Sistemas
Responsable Área de Sistemas