

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

DIRECCIÓN TIC

SANTA MARTA, D.T.C.H.

2020

Contenido

1.	OBJETIVO	3
2.	ALCANCE.....	3
3.	DEFINICIONES.....	3
4.	RESPONSABLES.....	4
5.	REFERENCIAS NORMATIVAS	5
6.	DESCRIPCIÓN DE ACTIVIDADES.....	5
6.1	POLÍTICAS DE SEGURIDAD FÍSICA.....	5
6.2	NORMAS DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES.....	6
6.3	POLÍTICAS DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO	7
6.3.1	Normas de protección frente a software malicioso	7
6.4	POLÍTICA DE CONTROL AL SOFTWARE OPERATIVO	8
6.4.1	Normas de control al software operativo	8
6.5	POLÍTICA DE USO DEL CORREO ELECTRONICO	9
6.5.1	Normas de uso del correo electrónico.....	9
6.5.2	Normas de uso adecuado de internet.....	10
6.6	DIRECTRICES SUPERVISORES DE CONTRATOS CON TERCEROS	11

1. OBJETIVO

El objetivo de este documento es establecer criterios y clasificación para la gestión de riesgos en las políticas de seguridad y privacidad de la información para la Alcaldía Distrital de Santa Marta, con el fin de regular la gestión de la seguridad de la información al interior de la entidad.

2. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad Y Privacidad de la Información para la Alcaldía de Santa Marta cubren todos los aspectos administrativos y de control que deben ser considerados por los directivos, funcionarios y terceros que laboren o tengan relación con la Alcaldía Distrital de Santa Marta, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

3. DEFINICIONES

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de la Alcaldía Distrital de Santa Marta, y en consecuencia, debe ser protegido.

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Centros de cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Alcaldía Distrital de Santa Marta.

SGSI: Sistema de Gestión de Seguridad de la Información.

Sistema de información: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la Alcaldía Distrital de Santa Marta, o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

4. RESPONSABLES

Los responsables del cumplimiento del El Plan de Tratamiento de Riesgos de Seguridad Y Privacidad de la Información son de todos los directivos, funcionarios y terceros que laboren o tengan relación con la Alcaldía Distrital de Santa Marta, con el acompañamiento de los funcionarios de las Oficinas de Dirección TIC y Calidad.

5. REFERENCIAS NORMATIVAS

- La norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013.
- Guía del Riesgo del Departamento Administrativo de Función Pública
- Norma Técnica Colombiana NTC-ISO 9001:2015. Sistemas de Gestión de la Calidad. Requisitos.
- Norma Técnica Colombiana NTC-ISO 9000:2005. Sistemas de Gestión de la Calidad. Fundamentos y Vocabulario.

6. DESCRIPCIÓN DE ACTIVIDADES

6.1 POLÍTICAS DE SEGURIDAD FÍSICA

La Alcaldía Distrital de Santa Marta, proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

Normas dirigidas a: **TODOS LOS USUARIOS,**

Los ingresos y egresos de personal a las instalaciones de la Alcaldía distrital de Santa Marta, deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos y biométricos implantados.

Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la Alcaldía Distrital; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.

Los funcionarios de la Alcaldía Distrital y el personal provisto por terceras partes **NO** deben intentar ingresar a áreas a las cuales no tengan autorización.

6.2 NORMAS DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

La Oficina de Recursos Técnicos, en conjunto con la oficina de Recursos Físicos debe propender porque las áreas de carga, descarga y almacenamiento de equipos de cómputo se encuentren aisladas del centro de cómputo y otras áreas de procesamiento de información.

El área de mantenimiento de equipos de cómputo, debe estar independizada del centro de cómputo y otras áreas de procesamiento de información.

La Oficina de Recursos Técnicos debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios del distrito y configurar dichos equipos acogiendo los estándares generados.

Normas o Estándares oficiales:

- Protocolo De Seguridad Informático - Resolución 776 del 30 de Octubre 2015.
- Y Procedimiento para el mantenimiento de equipos de cómputo de la Alcaldía Distrital de Santa Marta. GRI-PRO-06.
- Procedimiento para el mantenimiento correctivo y preventivo de las impresoras de la Alcaldía Distrital de Santa Marta. GRI-PRO-07.
- Procedimiento para el mantenimiento correctivo y preventivo del cableado estructurado de voz y datos de la Alcaldía Distrital de Santa Marta. GRI-PRO-08

La Secretaria General debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios del distrito, ya sea cuando son dados de baja o cambian de usuario.

El Grupo de Recursos Físicos debe revisar los accesos físicos en horas no hábiles a las áreas donde se procesa información.

El Grupo de Recursos Físicos debe restringir el acceso físico a los equipos de cómputo de áreas donde se procesa información sensible.

El Grupo de Recursos Físicos debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la institución, posean pólizas de seguro.

Normas dirigidas a: TODOS LOS USUARIOS,

La Oficina de Recursos Técnicos es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos del distrito.

Las estaciones de trabajo y demás recursos tecnológicos asignados a los funcionarios y personal provisto por terceras partes (Contratistas) deben acoger las instrucciones técnicas que proporcione la Oficina de Recursos Técnicos.

Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad de la Alcaldía Distrital de Santa Marta, el usuario responsable debe informar a la Oficina de Recursos Técnicos en donde se atenderán o escalará al interior de la oficina, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo y demás recursos tecnológicos del distrito, solo puede ser realizado por los funcionarios de la Oficina de Recursos Técnicos, o personal de terceras partes (Contratista) autorizado por dicha área.

Los funcionarios y el personal provisto por terceras partes (Contratistas) NO deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.

Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

En caso de pérdida o robo de un equipo de cómputo de la Alcaldía Distrital de Santa Marta, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

6.3 POLÍTICAS DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

6.3.1 Normas de protección frente a software malicioso

La Oficina de Recursos Técnicos debe proveer herramientas tales como antivirus, antimalware, anti spam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la Alcaldía Distrital de Santa Marta y los servicios que se ejecutan en la misma.

Normas dirigidas a: **TODOS LOS USUARIOS**

Los usuarios no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, anti spam, definidas por la Oficina de Recursos Técnicos; por consiguiente, únicamente se podrán realizar tareas de escaneo de virus en diferentes medios.

Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, anti spam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.

Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la Oficina de Recursos Técnicos, para que a través de ella, la Dirección de Tecnología tome las medidas de control correspondientes.

Los funcionarios y el personal provisto por terceras partes (Contratistas) NO deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.

Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

En caso de pérdida o robo de un equipo de cómputo de la Alcaldía Distrital de Santa Marta, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

6.4 POLÍTICA DE CONTROL AL SOFTWARE OPERATIVO

6.4.1 Normas de control al software operativo

La Oficina de Recursos Técnicos debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la entidad.

La Oficina de Recursos Técnicos debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.

La Oficina de Recursos Técnicos debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.

6.5 POLÍTICA DE USO DEL CORREO ELECTRONICO

La Alcaldía Distrital de Santa Marta, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

6.5.1 Normas de uso del correo electrónico

La Oficina Tecnología TIC debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.

Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de la Alcaldía Distrital de Santa Marta. El correo institucional no debe ser utilizado para actividades personales.

Los mensajes y la información contenida en los buzones de correo son propiedad de la Alcaldía Distrital de Santa Marta y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

Los usuarios de correo electrónico institucional tienen prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios de la institución y el personal provisto por terceras partes.

No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia; a excepción de los que por su importancia, envíen los Contratistas que dan soporte a los sistemas de información.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la Alcaldía Distrital de Santa Marta y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

6.5.2 Normas de uso adecuado de internet

La Oficina de Recursos Técnicos debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

La Oficina de Recursos Técnicos debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

Normas dirigidas a: TODOS LOS USUARIOS,

Los usuarios del servicio de Internet de la Alcaldía Distrital de Santa Marta deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.

Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.


No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos, redes sociales o mensajería instantánea. (Facebook, Kazaa, MSN, Yahoo, Youtube, Net2phome, Myspace, Twitter, LinkedIn) y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de la Alcaldía Distrital de Santa Marta.

No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

6.6 DIRECTRICES SUPERVISORES DE CONTRATOS CON TERCEROS

Los Supervisores de contratos con terceros deben divulgar las políticas, normas y procedimientos de seguridad de la información de la Alcaldía Distrital de Santa Marta a dichos terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, por parte de los terceros se realice de manera segura, de acuerdo con las políticas, normas y procedimientos de seguridad de la información.

Proyectó:	Álvaro Castillo Bolaño Director TIC	
Revisó:	Álvaro Castillo Bolaño Director TIC	