Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Municipio de San José de Cúcuta

1. Información General

1.1 Objetivo

Establecer y ejecutar las actividades necesarias para tratar preventiva e integralmente los riesgos de Seguridad y Privacidad de la Información, a los que el municipio de San José de Cúcuta puede estar expuesta, por medio de la protección de la integridad, confidencialidad y disponibilidad de la información.

1.2 Responsable

La Oficina de las Tecnologías de la Información y la Comunicación, adscrita a la Secretaría general de la Alcaldía Municipal de San José de Cúcuta.

1.3 Definición

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la entidad.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y el porqué de ellos, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos, así como un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal.

1.4 Glosario

Activo de información: Conocimiento o información que tiene valor para el individuo u organización.

Amenazas: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Confidencialidad: Propiedad de la información que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad autorizada.

Integridad: Propiedad de exactitud y completitud.

No repudio: Capacidad para corroborar que es cierta la reivindicación de que ocurrió un evento o una acción y las entidades que lo originaron

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital, puede debilitar el logro de los objetivos económicos y sociales, así como afectar la soberanía nacional la integridad territorial, el orden constitucional y los intereses nacionales, incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

1.5 Alcance

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos a los que puede estar expuesta el municipio de San José de Cúcuta. Las actividades que se relacionan en el presente documento se realizarán conforme a los manuales y procedimientos para el tratamiento de los riesgos adoptados por del sistema de gestión de la Entidad en el marco de los lineamientos del MIPG.

2. Actividades y Procedimientos para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información

2.1. Solicitud de Proceso

Cada vez, que algún usuario de cualquier dependencia de la entidad requiera la ejecución de una actividad por parte de la oficina TIC, éste podrá hacer la solicitud de forma verbal mediante llamada telefónica o directamente en la oficina. Pero si la actividad a solicitarse requiere de la utilización de recursos se tendrá que hacer mediante un correo electrónico o por la web de la organización.

2.2. Orden de Trabajo

Todo técnico de la Oficina TIC que deba realizar una actividad en alguna de las dependencias de la entidad, tendrá que llevar una orden de trabajo y en ella se plasmará como mínimo lo siguiente: Nombre de quien solicitó el servicio y su firma, fecha en la que se realizó el trabajo, nombre del técnico que desarrolló la actividad; lo anterior, con el fin de evidenciar el trabajo realizado y desarrollar buenas prácticas en la manipulación de los equipos que guardan información.

2.3. Orden de Movilización

En el momento de trasladar un equipo electrónico de un departamento a otro se deberá llenar una orden de movilización para tener la ubicación exacta del equipo o en algún caso que ingrese del exterior de la institución.

2.4. Adopción de Medidas de Seguridad en la Oficina TIC

Un punto muy importante dentro de un centro de cómputo y una Oficina TIC es sin duda la seguridad, los activos y la información que ahí se manejan son tan críticos que cualquier daño que pudieran sufrir se convertiría en un gran desastre para la entidad. Por

ello, es de vital importancia implementar un procedimiento que regule precisamente este punto.

- Control de acceso al área TIC.
- Utilización de antivirus actualizados para los equipos de cómputo de la oficina.
- Definir responsabilidades para la seguridad de datos, sistemas y programas.
- Involucrar a varias personas en funciones delicadas, esto con el fin de no depender de una sola para la realización de ellas.
- Enfatizar al personal de la dependencia la importancia de la seguridad y su responsabilidad personal.
- Establecer planes de contingencia y para casos de emergencia.
- Dar a conocer solo al personal autorizado donde se encuentran y como obtener los datos confidenciales.
- Mantener en buen estado los detectores de incendios, extintores y demás equipo para caso de incendio u otro desastre.
- Proteger el equipo de daños físicos. (Polvo, humo, etc.)
- Alejar todo material magnético dado que puede dañar las unidades de almacenamiento.
- Cambiar claves de acceso con regularidad.
- Tener y llevar a cabo un plan de respaldos.
- Mantener el área limpia y ordenada.

2.5. Respaldo de los Servicios Tecnológicos de la Entidad

La entidad ha elaborado un diagnóstico de cada uno de los Centros Integrales de Operación de Comunicaciones y Datos CIOCD, en el que se ha inventariado el estado de los componentes de protección y se ha elaborado un plan de mantenimiento preventivo de los aires acondicionados de los CIOCD.

2.6. Plan de Continuidad TIC

En cumplimiento a lo estipulado en el Decreto 1008 de 2018, compilado en el Decreto 1078 de 2015 Gobierno Digital, se ha elaborado la definición de los servicios y el seguimiento a los proveedores, con el fin de realizar el catálogo de servicios y el tablero de indicadores; el cual fue compartido al equipo de Arquitectura de Transformación Digital.

2.7. Programa de Gestión de Servicio al Cliente y Datos Abiertos del Sistema TIC

Con la creación de este programa se busca resolver los temas relacionados de servicio al cliente, caracterización de usuarios, datos abiertos, etc., cumpliendo de esta manera con lo establecido en la Ley 1712 de 2014 y el Decreto 1008 de 2018 compilado en el Decreto 1078 de 2015 Gobierno Digital.

3. Actividades

ITEM	ACTIVIDAD	DESCRIPCIÓN
1	Elaboración del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Establecer y ejecutar las actividades necesarias para tratar preventiva e integralmente los riesgos de Seguridad y Privacidad de la Información, a los que la Alcaldía de Cúcuta puede estar expuesta, por medio de la protección de la integridad, confidencialidad y disponibilidad de la información
2	Reunión con los coordinadores o jefes de departamentos	Establecer la información que manejan en su dependencia Definir las posibles vulneraciones legales por las malas prácticas en el tratamiento de la información Designación de los propietarios de los datos, funciones y responsabilidades.
3	Plan de continuidad TIC	Definición de los servicios y el seguimiento a los proveedores
4	Programa de Gestión de Servicio al Cliente y Datos Abiertos del Sistema CTIC de la Alcaldía de San José de Cúcuta	Resolver los temas relacionados de servicio al cliente, caracterización de usuarios, datos abiertos, etc., cumpliendo de esta manera con lo establecido en la Ley 1712 de 2014 y el Decreto 1008 de 2018 compilado en el Decreto 1078 de 2015 Gobierno Digital.
5	Centros Integrales de Operación de Comunicaciones y Datos CIOCD	Inventario del estado de los componentes de protección y se ha elaborado un plan de mantenimiento preventivo de los aires acondicionados de los CIOCD
6	Divulgar las políticas adoptadas en la entidad para el manejo de la seguridad de la información	Comunicar a todo el personal involucrado con el manejo de información
7	Identificar los funcionarios de cada dependencia con capacidad para tomar decisiones para la seguridad de la información	Detallar explicita y correctamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas. Explicar las ventajas de implementar una política de seguridad informática y los riesgos de no tenerla
8	Monitorear periódicamente los procedimientos y operaciones de la entidad	Actualizar oportunamente las políticas adoptadas por la entidad Establecer mecanismos que permitan auditar tanto los elementos físicos de la red como el desempeño de los funcionarios y contratistas
9	Respaldo de la información permanente	Definir los permisos de acceso, escritura, lectura de archivos y carpetas de acuerdo con el cargo asignado
10	Creación de grupos de usuarios en los equipos de cómputo	Creación de grupos de usuarios de acuerdo con el perfil y cargo

4. Normatividad Vigente

NORMA	AÑO	DESCRIPCIÓN
Ley 1341	2009	Definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnología e Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones
CONPES 3701	2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.
Ley 1581	2012	Disposiciones generales para la protección de datos personales
Decreto 1078	2015	Decreto único reglamentario del sector de Tecnología e Información y las comunicaciones (define el componente de seguridad y privacidad de la información)
Decreto 1081	2015	"Decreto Reglamentario Único del Sector Presidencia de la República" (En especial Libro 2)
Decreto 415	2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones.
Resolución CDS 004	2017	Fortalecimiento Institucional en Materia de TIC, para Plan Estratégico de Tecnología y Sistemas de Información (PETI) y para la Gestión de Proyectos TIC
CONPES 3854	2017	Política Nacional de Seguridad Digital
Decreto 1499	2017	Modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública.
CONPES 3920	2018	Política Nacional de Explotación de Datos (Big Data)