Control de cambios

Versión	Fecha	Descripción de la modificación
01	**20 de diciembre de 2022**	Se crea documento como parte de la implementación del Modelo de Seguridad y Privacidad de la información – MSPI en la entidad.

Método de Elaboración	Revisa	Aprueba
Se realizó la construcción del documento, por parte de la Dirección de Tecnologías e Información mediante mesas de trabajo, en las cuales participaron los profesionales de la DTI y el analista del proceso de la OAP.	Orlando Benavides Santacruz **Dirección de Tecnologías e Información** Angela Patricia Cabeza Morales **Profesional OAP – Analista del proceso**	Martha Liliana Soto Iguarán **Subsecretaría de Gestión Institucional** Documento revisado y aprobado mediante caso aplicativo Hola No. **283454**

1. INFORMACIÓN GENERAL

1.1. Propósito

Establecer actividades, criterios y condiciones de gestión de incidentes de seguridad de la información, en relación con la priorización y categorización de incidentes de seguridad de la información, que se puedan presentar en la Secretaría Distrital de Gobierno con el fin de garantizar una solución oportuna y eficaz de acuerdo con el Manual de Gestión de Seguridad de la información vigente en la Entidad.

1.2. Responsable

Director(a) de Tecnologías e Información

1.3. Glosario

Activo de información
Es cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

Código Malicioso
Es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos.1

Confidencialidad
Propiedad de la información, por la que se garantiza que la misma está accesible únicamente al personal autorizado.

Contener
Suspender o impedir el desarrollo de un proceso. Se realizará todas aquellas tareas necesarias con el fin de contener el incidente de seguridad y así minimizar su impacto.

[1] https://latam.kaspersky.com/resource-center/definitions/malicious-code

Datos personales
Los datos personales son cualquier información relativa a una persona física viva identificada o identificable. Las distintas informaciones, que recopiladas pueden llevar a la identificación de una determinada persona, también constituyen datos de carácter personal.

Disponibilidad
Propiedad de la información de estar accesible y utilizable cuando se requiera.

Ethical Hacking
Actividad cuyo objetivo es hackear un sistema, identificar y en algunos casos reparar posibles vulnerabilidades, lo que previene eficazmente la explotación por hackers maliciosos.2

Evento De Seguridad
Compromete los niveles de riesgo, pero no afecta la operación de la organización y sus objetivos de negocios.[3]

Exploit
Secuencia de comandos utilizados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto. Mediante la ejecución del *exploit* se suele perseguir: el acceso a un sistema de forma ilegítima, obtención de permisos de administración en un sistema ya accedido o un ataque de denegación de servicio a un sistema.

Incidente de seguridad
Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

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

Mitigación
Reducción o atenuación de los daños potenciales sobre los sistemas, aplicaciones y dispositivos causados por un evento, como una vulnerabilidad o ataque.

Riesgo
Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado. El riesgo puede ser mitigado mediante políticas de seguridad y continuidad del negocio que suelen prever posibles ataques y proponen soluciones de actuación ante situaciones cuyo riesgo pueda ser elevado.

[2] https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-el-hacking-etico/
[3] https://www.escuelaeuropeaexcelencia.com/2020/04/definiciones-de-evento-incidencia-o-no-conformidad-en-iso-27001/

VPN
Es una tecnología de red que sirve para conectar una o más computadoras a una red privada utilizando como medio una red pública como internet 4.

Vulnerabilidad
Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina *exploit*). Cuando se descubre la vulnerabilidad, el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto. Sinónimo: hueco de seguridad.

2. INSTRUCCIONES

2.1. Disposiciones Generales

- ✓ La gestión de incidentes de seguridad comprende la asignación de roles y responsabilidades para el desarrollo de actividades ante la ocurrencia de incidentes de seguridad; por lo que la DTI será la encargada de coordinar las acciones conjuntas con las partes interesadas para una atención oportuna y eficaz.
- ✓ El proceso de gestión de incidentes de seguridad de la información debe estar enmarcado en la mejora continua (planificar, hacer, verificar y actuar), por lo que los resultados de la gestión deben ser documentados, ya que permitirá analizar e implementar mejoras a controles existentes o implementar nuevos.
- ✓ Los diferentes especialistas de la Dirección de Tecnologías e Información deben conocer y aplicar los lineamientos del GDI-TIC-M004 Manual de gestión de seguridad de la información, el GDI-TIC-P009 procedimiento de gestión de incidentes de seguridad de la información y el presente instructivo para la correcta atención de incidentes de seguridad de la información.

2.2. Priorización de Incidentes de Seguridad

El nivel de prioridad de los incidentes de seguridad de la información se basa esencialmente en dos parámetros:

- ✓ Impacto: determina la importancia del incidente de acuerdo con el nivel de afectación de los procesos misionales de la Entidad, número de usuarios y/o activos de tecnologías de la información afectados, y la importancia de estos en la organización, como se describe en la tabla 1.

[4] https://www.hn.cl/blog/que-es-y-para-que-sirve-una-conexion-vpn/

IMPACTO	
VALOR	DESCRIPCIÓN
ALTO	-Se afectan activos de información clasificados como de criticidad ALTA. (Revisar el inventario de activos de información en conjunto con el grupo de seguridad de la información) -Requiere acciones de contención inmediatas. -Se compromete la prestación de los servicios. -Pérdidas considerables para el negocio.
MEDIO	-Se afectan activos de información importantes con clasificación de criticidad MEDIA. -No causan impacto en la prestación del servicio. -Pueden ser fácilmente subsanados.
BAJO	-Afecta activos de información irrelevantes -No afecta la prestación de los servicios -Son de fácil atención o no requieren acciones.

Tabla 1 Nivel de Impacto

✓ Prioridad: depende del tiempo máximo de recuperación que se acepte para la resolución del incidente de seguridad de la información, como se muestra en la tabla 2.

PRIORIDAD	
VALOR	DESCRIPCIÓN
ALTA	La tasa de masificación del incidente es alta y se requiere aplicar medidas de contención inmediatas para evitar que se afecte la prestación de los servicios o se afecte la seguridad de la información clasificada como crítica
MEDIA	El incidente se encuentra en propagación y representa una amenaza potencial para la disponibilidad de los servicios y para la seguridad de la información clasificada como crítica.
BAJA	El incidente se detectó en focos aislados y no representan una amenaza de alto impacto.

Tabla 2 Nivel de Prioridad

Igualmente, se establecen tiempos de respuesta para los incidentes que se puedan presentar de acuerdo con el nivel de prioridad:

- ✓ Alta: 5 – 12 horas
- ✓ Media: 13 – 36 horas
- ✓ Baja: 37 – 48 horas.

Nota: Los tiempos establecidos en el presente instructivo están sujetos a cambios de acuerdo con las definiciones de la Mesa de servicio y de la Dirección de Tecnologías e Información.

2.3. Categorización de Incidentes de Seguridad

En la Secretaría Distrital de Gobierno se establecen nueve (9) categorías de incidentes de seguridad de la información, que se encuentran en la herramienta de gestión TI vigente en la entidad, y corresponden a las siguientes:

CATEGORÍA 1 - VIOLACIÓN A LA POLÍTICA, NORMAS Y PROCEDIMIENTOS DE SEGURIDAD

Ocurre cuando un funcionario, colaborador o tercero, directa o indirectamente, incumple las directrices indicadas en el Manual de Gestión de Seguridad de la información - GDI-TIC-M004, Política para el tratamiento y protección de datos personales GDI-TIC-M007 de la Secretaria Distrital de Gobierno, el Acuerdo de Confidencialidad GDI-TIC-F020 y en las normas, procedimientos, manuales, formatos y demás documentos aprobados y divulgados en la Entidad, en los cuales se indique los derechos, deberes y adecuado proceder en la protección de la información.

El agente de la Mesa de servicios, para poder escalar el caso debe validar lo siguiente:

- ✓ La política, norma o procedimiento afectado debe corresponder a la última versión publicada en la Intranet.
- ✓ Fue incumplido algún lineamiento de las políticas, normas o procedimientos.
- ✓ Evidencia del incumplimiento o violación al manual de gestión de seguridad de la información GDI-TIC-M004 o Política para el tratamiento y protección de datos personales GDI – TIC M007.

CATEGORÍA 2 - FUGA DE INFORMACIÓN

La información clasificada como privada y/o confidencial no debe ser accedida, transmitida, impresa, digitalizada o copiada sin previa autorización de acuerdo con lo definido en el Manual de Gestión de Seguridad de la información GDI-TIC-M004.

El agente de la Mesa de servicios, para poder escalar el caso debe validar lo siguiente:

- ✓ Validar la clasificación de la información y control de acceso, de acuerdo con la matriz de activos de información (acudir al grupo de seguridad de la Información).
- ✓ Solicitar y validar la/las evidencias que soporten el caso de fuga de información reportado.
- ✓ Otra situación no contemplada pero reportada por el usuario final.

CATEGORÍA 3 - USO INADECUADO DE LOS ACTIVOS DE INFORMACIÓN

Este tipo de incidente ocurre cuando los activos de información (bases de datos, software, hardware, información, PCs, teléfonos, impresoras, servicios, instalaciones etc.) se emplean para actividades consideradas no éticas o ilegales (Ley 1273 de delitos informáticos) y de acuerdo con lo manifestado en el GDI-TIC-M004.

El agente de la Mesa de servicios debe categorizar y escalar el caso si valida alguna de las siguientes situaciones:

- ✓ Se realizan actividades no autorizadas con los recursos tecnológicos asignados (aquellas que no están directamente relacionadas con las funciones del cargo u objetivo del contrato).
- ✓ Cuando se utiliza el acceso a internet para visualizar, descargar o transmitir material discriminatorio, difamatorio, ofensivo, pornográfico, obsceno o páginas restringidas por la entidad.
- ✓ Cuando el correo electrónico corporativo se emplea para emisión de correo no deseado, cadenas de correo, publicidad, mensajes ofensivos o que atenten contra la integridad y el buen nombre de las personas.
- ✓ Cuando se instala software no autorizado en las estaciones de trabajo (consulta en software línea base).
- ✓ Si los mecanismos de seguridad y control implementados en los equipos o dispositivos son deshabilitados sin previa justificación y autorización.
- ✓ Uso de los recursos informáticos para labores no relacionadas con las actividades asignadas.
- ✓ Cuando se comparten nombres de usuario, contraseñas o privilegios, pues estos se consideran personales e intransferibles.

CATEGORÍA 4 - VULNERABILIDADES Y DETECCIÓN DE EXPLOITS

Se deben clasificar como incidentes de seguridad en esta categoría cualquiera de los siguientes casos:

- ✓ Información suministrada en los boletines de seguridad de las casas fabricantes de las aplicaciones críticas de la organización, clasificadas como "Muy Críticas" y de atención inmediata.
- ✓ Vulnerabilidades que no hayan sido atendidas dentro de los planes de remediación.
- ✓ Vulnerabilidades detectadas en actividades de *Ethical Hacking*.
- ✓ Desviaciones de la arquitectura de aseguramiento de la plataforma tecnológica.

- ✓ Eventos de monitoreo en los cuales se detecte el intento de aprovechamiento de una vulnerabilidad conocida por un *Exploit*.

CATEGORÍA 5 - MONITOREO, ANÁLISIS DE TRÁFICO Y PRUEBAS SOBRE LA RED

Se presenta cuando de forma no autorizada se realiza algún tipo de acción sobre el flujo de tráfico de la red de datos de la Secretaría Distrital de Gobierno o sobre cualquiera de los canales de comunicación entre la organización y las redes de sus Clientes / Proveedores.

Esto debe ser reportado por el especialista de seguridad informática o seguridad perimetral de la Mesa de servicios o el responsable de Infraestructura de la DTI, mediante caso generado en la Herramienta de Gestión vigente en la Entidad.

CATEGORÍA 6 - INFECCIÓN CON CÓDIGO MALICIOSO

Ocurre cuando se detecta la presencia de un programa de este tipo en un sistema de cómputo o se detecta la alteración (infección) de un archivo por esta misma causa.

Esto debe ser reportado por los servidores públicos, contratistas, terceros, el responsable del antivirus o el responsable de Infraestructura, mediante caso generado en la Herramienta de Gestión vigente en la Entidad.

CATEGORÍA 7 - ACCESO NO AUTORIZADO

Ocurre cuando un atacante logra ganar acceso lógico o físico a la red de datos, a los elementos de la infraestructura tecnológica, a los servicios o sistema de información o a la información misma a la cual no debe tener acceso. Este tipo de incidentes de seguridad de la información genera un alto impacto en la confidencialidad e integridad de la información. Dentro de la categoría de accesos no autorizados se encuentran:

- ✓ Acceso no autorizado a sistemas de información
- ✓ Acceso no autorizado a equipo de cómputo
- ✓ Acceso no autorizado a equipo de telecomunicaciones
- ✓ Hurto de partes, componentes y equipos de cómputo y/o telecomunicaciones.
- ✓ Intento fallido de conexión VPN de clientes
- ✓ Consultas no autorizadas

Esto debe ser reportado por los servidores públicos, contratistas, terceros, el especialista de seguridad informática o seguridad perimetral por intentos a VPN, especialista Windows por Directorio Activo o el responsable de Infraestructura.

CATEGORÍA 8 - DENEGACIÓN DE SERVICIO

Los ataques de denegación de servicios se refieren al uso específico de ciertas herramientas por parte de intrusos con el fin de causar que las redes y/o sistemas dejen de operar apropiadamente. Esto incluye:

- ✓ Consumo excesivo de recursos de cómputo limitados de forma tal que se impide la asignación de recursos para la prestación del servicio a usuarios válidos.
- ✓ Uso indebido y excesivo de recursos, como el almacenamiento y transferencia masiva de información no corporativa que puede saturar la capacidad de los elementos de almacenamiento y de los canales de comunicaciones.
- ✓ Alteración de la configuración de los elementos de tecnología que impida el acceso a los mismos por parte de los usuarios autorizados y que afecte la prestación de un servicio.
- ✓ Destrucción o alteración física de los elementos de tecnología.

Esto debe ser reportado por los servidores públicos, contratistas, terceros, el especialista de seguridad informática o seguridad perimetral, el responsable de Infraestructura o quien administre el servicio tecnológico de la Secretaría Distrital de Gobierno que sufra la denegación del servicio.

CATEGORÍA 9 - VIOLACIÓN DE DERECHOS A LA PROPIEDAD INTELECTUAL (DERECHOS DE AUTOR)

Son todas aquellas violaciones a la ley de derechos de autor (Ley 23 de 1982, la violación de derechos de propiedad intelectual relacionados con Derecho de Autor tiene sanciones civiles y penales):

- ✓ Uso de los recursos de la Secretaría Distrital de Gobierno para descargar material sin consentimiento de su propietario o titular, como música, películas, libros, etc.
- ✓ Uso de la información propietaria de la Secretaría Distrital de Gobierno para beneficio particular.
- ✓ Uso de información sin autorización de su autor o propietario para ser usada en provecho de la Secretaría Distrital de Gobierno, como fotografías, textos y contenidos digitales.
- ✓ La reproducción superior a 14% de un texto o libro sin autorización del autor a través de fotocopia.
- ✓ La descarga o compra de software sin licencia.
- ✓ La simple copia en cualquier medio de almacenamiento que contenga música en sistemas o equipos tecnológicos de la entidad.

Esto debe ser reportado por los servidores públicos, contratistas, tercero o el encargado de protección de datos, mediante caso generado en la Herramienta de Gestión vigente en la Entidad.

2.4. Clasificación del incidente de seguridad

Está sujeta a la infraestructura, riesgos y criticidad de los activos. Se tiene la siguiente clasificación:

- Acceso no autorizado: Es un incidente que involucra a una persona, sistema o código malicioso que obtiene acceso lógico o físico sin autorización adecuada del dueño a un sistema, aplicación, información o un activo de información.
- Modificación de recursos no autorizado: Un incidente que involucra a una persona, sistema o código malicioso que afecta la integridad de la información o de un sistema de procesamiento.
- Uso inapropiado de recursos: Un incidente que involucra a una persona que viola alguna política de uso de recursos.
- No disponibilidad de los recursos: Un incidente que involucra a una persona, sistema o código malicioso que impide el uso autorizado de un activo de información.
- Multicomponente: Un incidente que involucra más de una categoría anteriormente mencionada.
- Otros: Un incidente que no puede clasificarse en alguna de las categorías anteriores. Este tipo de incidentes debe monitorearse con el fin de identificar la necesidad de crear nuevas categorías.

3. DOCUMENTOS RELACIONADOS

3.1 Documentos internos

Código	Documento
GDI-TIC-P009	Gestión de incidentes de seguridad de la información
GDI-TIC M004	Manual de Gestión de Seguridad de la información
GDI-TIC-P008	Gestión de Incidentes
GDI-TIC-M007	Política para el tratamiento y protección de datos personales
GDI-TIC-F020	Acuerdo de Confidencialidad

3.2 Normatividad vigente

Norma	Año	Epígrafe	Artículo(s)
Ley 1273	2009	Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado “de la protección de la información y de los datos”	Toda
Resolución 500	2021	Por la cual se establecen los lineamientos y estándares para la estrategia de	Toda

Norma	Año	Epígrafe	Artículo(s)
		seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital	
Ley 23	1982	Sobre los Derechos de Autor	Toda

3.3. Documentos externos

Nombre	Fecha de publicación o versión	Entidad que lo emite	Medio de consulta
Norma ISO 27001:2013 "Sistema de gestión de seguridad de la información"	2013	ICONTEC	Virtual
Norma ISO 27002:2013 "Information technology -- Security techniques -- Code of practice for information security controls"	2013	ICONTEC	Virtual
COBIT "Objetivos de control para la información y tecnologías relacionadas"	12 de abril de 2012	ISACA	Virtual