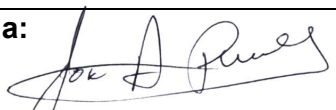
CONTROL DE CAMBIOS

NO. DE ACTA DE APROBACIÓN	FECHA	VERSIÓN	DESCRIPCIÓN
037	25/11/2021	1.0	Adopción del Procedimiento

AUTORIZACIONES

ELABORÓ:	REVISÓ	APROBÓ
ÁREA TÉCNICA	**OFICINA ASESORA DE PLANEACIÓN**	**LIDER DEL PROCESO**
Nombre: Jose Alfonso Pérez Contreras	**Nombre:** Diana María Mora Ramírez Yovanny Arias G.	**Nombre:** Gotardo Antonio Yáñez Alvarez
Firma: 	**Firma:** 	**Firma:** 
Cargo: Contratista área de Tecnología SGC	**Cargo:** Profesional Especializada Oficina Asesora Planeación	**Cargo:** Subdirector de Gestión Corporativa

1. OBJETIVO

Establecer acciones y lineamientos que permitan atender en forma adecuada ante la ocurrencia de cualquier incidente de seguridad relacionado con los activos de información, y nos permita evaluarlos junto con la gestión de las vulnerabilidades, asegurando que los sistemas, redes, y aplicaciones sean lo suficientemente seguros.

2. ALCANCE

El procedimiento inicia con el reporte de un incidente de seguridad y termina con el desarrollo de las actividades post incidente.

3. RESPONSABILIDADES GENERALES

Profesional Universitario Subdirección Gestión Corporativa o quien haga sus veces - Sistemas de Información y Seguridad.

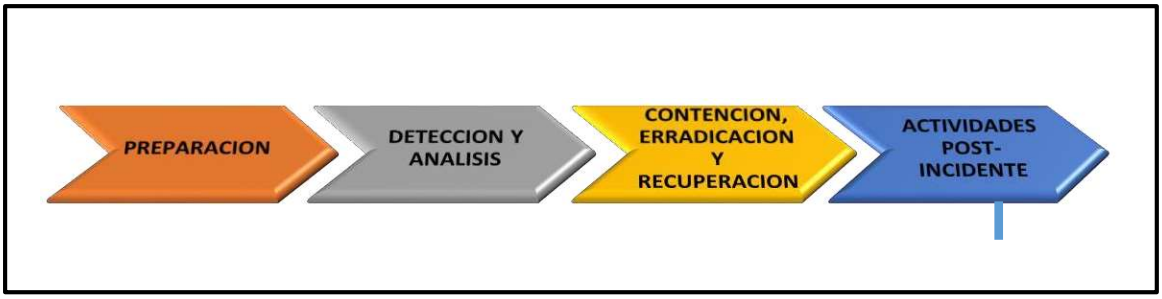
- Recibir, documentar y dar respuesta al incidente de seguridad de la información
- Articular y gestionar los incidentes de seguridad de la información
- Recibir y registrar los reportes de incidentes de seguridad de la información mediante el uso del formato.
- Establecer la criticidad y/o severidad de los incidentes de Seguridad de la información
- Evaluar y dar respuesta de manera eficiente y adecuada a los incidentes de Seguridad de la información
- Revisar la documentación del incidente para identificar las posibles causas
- Escalar el incidente a quienes puedan entregar la solución del mismo
- Identificar e implementar las acciones correctivas posteriores al incidente
- Identificar y aprender de las situaciones evidenciadas, desde su identificación, detección, reporte, contención, recolección y preservación de evidencia y su posterior eliminación.

Profesional Universitario Subdirección Gestión Corporativa o quien haga sus veces - Sistemas de Información y seguridad / Web Master / Sistemas de Información / Infraestructura tecnológica / Proveedores

- Recibir, documentar y dar respuesta al incidente de seguridad de la información relacionado con sus obligaciones y/o funciones

4. LINEAMIENTOS Y/O POLITICAS DE OPERACIÓN

a. Etapas de Incidentes de Seguridad de la información



b. **Preparación**:

Consiste en poner a disposición los recursos necesarios para la atención de incidentes y las herramientas para cubrir las demás etapas del ciclo de vida del mismo.

c. Detención y análisis:

Descripción del evento: En este primer paso se requiere que el equipo describa con el máximo nivel de detalle qué ocurrió.

Identificación de fallos y errores: En este paso se requiere que el equipo identifique cuáles fueron los errores cometidos en el proceso.

Para este paso se puede obtener la información de entrevistas en profundidad, entrevistas grupales con los involucrados o a través de otros medios.
Predisponentes y favorecedores: Una vez identificados los fallos y errores, se requiere que se proceda a identificar los factores predisponentes o favorecedores de estos.
La información requerida en este paso puede obtenerse a través de entrevistas con los involucrados en el evento, reuniones con los jefes directos de los mismos y con compañeros de trabajo.

Identificación de barreras: En este paso se requiere que se describan las barreras que se encontraban establecidas para evitar los errores del proceso y que no funcionaron.

En el caso de no existir barreras previamente establecidas, debe dejarse constancia de ello.

Análisis de barreras existentes: Se requiere que se explique por qué no funcionaron dichas barreras. Aquí podremos encontrar aspectos relacionados a la falta de entrenamiento, desatención de las normas, situaciones de emergencias o requerimiento de soluciones que requerían celeridad.

En este punto es muy importante realizar un análisis sistémico, buscando conocer qué, cómo, por qué ocurrió y qué puede hacerse para que no vuelta a ocurrir.

Diseño de mejoras: se requiere que se proponga un diseño de mejora sobre las barreras anteriores o que diseñen nuevas barreras para evitar que el error vuelva a ocurrir, Para optimizar los tiempos y aumentar la fidelidad de la información

d. Contención Erradicación y Recuperación

Para evitar la propagación del incidente, disminuir el impacto sobre los activos de información, y garantizar la confidencialidad, integridad y disponibilidad de la información se establecen las siguientes actividades:

e. Contención:

Busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI.

Contención de incidentes de seguridad

EVENTO Y/O INCIDENTE DE SEGURIDAD	ESTRATEGIA
Código Malicioso	Desconexión de la red del equipo afectado Bloqueo de Puertos Actualización de herramientas de detección y bloqueo de software malicioso
Accesos no Autorizados	Bloqueos de cuenta Apagado de la máquina Bloqueo de puertos
Reconocimiento	Nuevas reglas de filtrado Bloqueo de Puertos
Corrupción	Retiro de funcionario Bloqueo de Cuentas

Una vez se apliquen las estrategias de contención, se procede a la recolección de la evidencia, para lo cual se debe tener en cuenta:

- Autenticidad: Quien haya recolectado la evidencia debe poder probar que es auténtica.
- Cadena de Custodia: Registro detallado del tratamiento de la evidencia, incluyendo quienes, como y cuando la transportaron, almacenaron y analizaron, con tal fin de evitar alteraciones o modificaciones que comprometan la misma.
- Validación: Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.

Durante el proceso de recolección de evidencias es necesario realizar las siguientes acciones:

- Registrar información que rodea a la evidencia.
- Tomar fotografías del entorno de la evidencia.
- Tomar la evidencia.
- Registrar la evidencia.
- Rotular todos los medios que serán tomados como evidencia.

- Almacenar toda la evidencia de forma segura.
- Generar copias de seguridad de la evidencia original.
- Realizar revisiones periódicas para garantizar que la evidencia se encuentra correctamente conservada

f. Erradicación y Recuperación:

Luego de que el incidente de seguridad ha sido contenido se debe realizar una erradicación y eliminación de cualquier rastro dejado por el incidente en nuestros activos de información como código malicioso etc.
Posteriormente se procede a la recuperación a través de la restauración de los sistemas y/o servicios afectados ya sea mediante backups y levantamiento se servicios no funcionales, seguidamente se procederá en el fortalecimiento de la vulnerabilidad afectada para que no vuelva a ocurrir dicho incidente de seguridad en el futuro.

Recuperación de incidentes de seguridad

EVENTO Y/O INCIDENTE DE SEGURIDAD	ESTRATEGIA
Denegación de Servicios	Restitución del servicio caído Restauración de Backups si es necesario
Código Malicioso	Restauración de Backups Actualización de Antivirus Verificar actualizaciones del equipo
Intrusión	Reinstalación del S.O del equipo Recuperación de datos Restauración de Backups
Corrupción	Retiro de funcionario Bloqueo de Cuentas
Vandalismo	Reparación del sitio web Restauración de backups

g. Actividades Post-Incidente

Las actividades posteriores al incidente se componen de un reporte apropiado de las actividades realizadas y la solución al problema detectado, de la generación de lecciones aprendidas, así como el registro en la base de conocimiento para posibles soluciones a próximos incidentes.

Una de las partes más importantes de un plan de respuesta a incidentes es la de aprender y mejorar, por eso se propone seguir las siguientes recomendaciones:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Los procedimientos documentados.
- Si se tomaron las medidas o acciones que podrían haber impedido la recuperación.
- Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.
- Acciones correctivas pueden prevenir incidentes similares en el futuro.

- Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

5. CLASIFICACIÓN DE INCIDENTES DE SEGURIDAD

La clasificación de los incidentes de seguridad de la información se debe realizar según la siguiente tabla:

NIVEL	NOMBRE	TIEMPO DE ATENCIÓN
1	Bajo	7 días
2	Medio	3 días
3	Alto	12 horas
4	Critico	2 horas

NIVEL	DESCRIPCIÓN
CRITICO	El incidente de seguridad afecta a activos de información considerados de impacto catastrófico y mayor que influyen directamente a los objetivos misionales del Instituto Distrital de Protección y Bienestar Animal. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales.
ALTO	Este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o denunciados, porque es posible establecer una amenaza sobre los activos de información capaz de impactar de manera considerable las características de integridad, confidencialidad y disponibilidad de un activo no crítico o crítico para el Instituto Distrital de Protección y Bienestar Animal.
MEDIO	Se incluyen los eventos que comprometen de manera moderada la operación normal de los activos de información, que influyen directamente a los objetivos de un proceso determinado.
BAJO	Se incluyen aquellos eventos que NO comprometen de ninguna manera operación normal de los activos de información, los procesos o los servicios; sus consecuencias NO comprometen la integridad, confidencialidad y la disponibilidad de los activos de información del el Instituto Distrital de Protección y Bienestar Animal.

6. FORMATOS Y DOCUMENTOS ANEXOS

No. de Anexo	Código	Nombre
1.	PA04-PR05-F01	FORMATO REGISTRO DE INCIDENTES DE SEGURIDAD

7. NORMATIVIDAD ASOCIADA

TIPO DE NORMA	NÚMERO DE IDENTIFICACIÓN	TÍTULO DEL DOCUMENTO	CAPÍTULOS O ARTÍCULOS	FECHA EXPEDICIÓN (DD/MM/AAAA)
ISO/IEC	9001	Calidad – Acciones para abordar el riesgo	Dominio 6.1	10/09/2015
ISO/IEC	27001	Gestión de incidentes de la seguridad de la información	Anexo A16.1	15/09/2013
ISO/IEC	27035	Tecnología de la información – Técnicas de seguridad – gestión de incidentes de seguridad de la información		15/02/2011
LEY	1581	Protección de datos personales	artículo 17 -18	17/10/2012
RESOLUCIÓN	500	por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital	Articulo 3,6,9	10/03/2021

8. DEFINICIONES

ISO/IEC **TERMINO**	**DEFINICIÓN**
ACTIVO DE INFORMACIÓN	Es todo aquello que representa valor para la Entidad desde software, hardware, información, servicios y personas.
AMENAZA PARA LA SEGURIDAD DE LA INFORMACIÓN	Una amenaza se refiere a cualquier cosa que tenga el potencial de causar daños graves a un sistema o activo de información. Una amenaza es algo que puede suceder o no, pero tiene el potencial de causar un daño grave. "https://normaiso27001.es/a16-gestion-de-incidentes-de-la-seguridad-de-la-informacion/ "

VULNERABILIDAD EN LA SEGURIDAD DE LA INFORMACIÓN	Se refiere a una debilidad o defecto en un sistema o activo de información que puede dejarlo expuesto a una amenaza o ataque. Una vulnerabilidad también puede referirse a cualquier tipo de debilidad en un sistema de información en sí mismo, en un conjunto de procedimientos o en cualquier cosa que deje la seguridad de la información expuesta a una amenaza. "https://normaiso27001.es/a16-gestion-de-incidentes-de-la-seguridad-de-la-informacion/ "
EVENTO EN LA SEGURIDAD DE LA INFORMACIÓN	Un evento de seguridad de la información es un cambio en las operaciones diarias de una red o servicio de tecnología de la información que indica que una política de seguridad puede haber sido violada o una protección de seguridad puede haber fallado. "https://normaiso27001.es/a16-gestion-de-incidentes-de-la-seguridad-de-la-informacion/ "
INCIDENTE EN LA SEGURIDAD DE LA INFORMACIÓN	Una sola o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar seguridad de información. Por ejemplo un comportamiento anómalo en un sistema es un evento, sin embargo, si se encuentra evidencia del virus en el sistema, se puede considerar un incidente de seguridad "https://normaiso27001.es/a16-gestion-de-incidentes-de-la-seguridad-de-la-informacion/ "
ATAQUE	Intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo. "https://normaiso27001.es/referencias-normativas-iso-27000/#def32"
AUDITORIA	Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarla objetivamente para determinar hasta qué punto se cumplen los criterios de auditoría. Las auditorias pueden ser internas o externas "https://normaiso27001.es/referencias-normativas-iso-27000/#def32"
CONFIDENCIALIDAD	Propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados. "https://normaiso27001.es/referencias-normativas-iso-27000/#def32"
MEJORA CONTINUA	Se define como acciones que se traducen en una mejora de los resultados, entonces la mejora continua es simplemente identificar y realizar cambios enfocados a

	conseguir la mejora del rendimiento y resultados de una organización. "https://normaiso27001.es/referencias-normativas-iso-27000/#def32"
INFORMACIÓN DOCUMENTADA	Se refiere a la información necesaria que una organización debe controlar y mantener actualizada tomando en cuenta y el soporte en que se encuentra. "https://normaiso27001.es/referencias-normativas-iso-27000/#def32"
SEGURIDAD DE INFORMACIÓN	Preservación de la confidencialidad, integridad y disponibilidad de la información. "https://normaiso27001.es/referencias-normativas-iso-27000/#def32"

9. DESCRIPCIÓN DE ACTIVIDADES CON FLUJOGRAMA INTEGRADO

10 días 3 horas 15 minutos

	TIEMPO	FLUJOGRAMA	REPONSABLE	COMENTARIOS
1	0,25	INICIO → Reportar el incidente de seguridad	Profesional universitario o quien gaga sus veces – Subdirección de Gestión Corporativa TIC	Enviar requerimiento o reporte de incidente a la Mesa de Servicios por medio de correo electrónico.
2	0,5	Evaluar incidente reportado	Profesional universitario o quien gaga sus veces – Subdirección de Gestión Corporativa TIC	Se analiza e identifica el incidente reportado por el usuario.
3		¿Es un incidente de seguridad? NO / SI		Se escala el incidente de seguridad al grupo de seguridad de la información
4	56	Detener incidente de seguridad	Profesional universitario o quien gaga sus veces – Subdirección de Gestión Corporativa TIC	Se realizarán todas aquellas tareas necesarias con el fin de contener el incidente de seguridad y así minimizar su impacto
5	12	Solucionar incidente de seguridad	Profesional Subdirección de Gestión Corporativa TIC o quien haga sus veces	Se realizan todas las actividades necesarias para solucionar el incidente
6		¿El incidente continua? NO → A / SI → 1		

	TIEMPO	FLUJOGRAMA	REPONSABLE	COMENTARIOS
7	8	1 Identificar las evidencias ← A	Profesional Subdirección de Gestión Corporativa TIC o quien haga sus veces	Se documentan las lecciones aprendidas del incidente de seguridad
8	2	Realizar las actividades post - incidente	Profesional Subdirección de Gestión Corporativa TIC o quien haga sus veces	Se realiza el informe final del incidente de seguridad presentado
9	0,1	Cierre de caso FIN	Profesional Subdirección de Gestión Corporativa TIC o quien haga sus veces	Se cierra el caso y el ticket