 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 1 de 18

Firma de Autorizaciones		
Elaboró	Revisó	Aprobó
Omar Orlando Coronado Cacia Contratista Planeación y TI - OAP	César Alonso Linares Peña Técnico Operativo – OAP	Adriana Villamizar Navarro Jefe Oficina Asesora de Planeación
Control de Cambios		
Fecha	Descripción	
Agosto de 2019	Creación del documento atendiendo las recomendaciones de la auditoría interna realizada al proceso Gestión tecnológica y dando cumplimiento a lo establecido en la Guía No. 21 para la gestión y clasificación de incidentes de seguridad de la información del MINTIC.	
Diciembre 2019	Se incluyen de forma específica el capítulo 11. Herramientas, plataformas y controles de protección contra códigos maliciosos.	
Diciembre 2021	Se estructura ciclo de vida de metodología de manejo de los incidentes de seguridad, ajuste de roles y actividades, actualización de normas asociadas.	



 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p>GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION</p>	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 2 de 18

TABLA DE CONTENIDO

1. OBJETIVO.....	3
2. ALCANCE.....	3
3. REFERENCIAS NORMATIVAS.....	3
4. DOCUMENTOS ASOCIADOS.....	3
5. DEFINICIONES.....	4
6. CICLO DE VIDA DE LA GESTIÓN Y RESPUESTA A UN INCIDENTE DE SEGURIDAD.....	5
7. ROLES PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.....	7
8. TIPOS DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN.....	9
9. POLÍTICAS DE OPERACIÓN PARA LA GESTIÓN DE INCIDENTES.....	9
11. RELACIÓN DE ACTIVIDADES PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:.....	11
12. HERRAMIENTAS, PLATAFORMAS Y CONTROLES DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS.....	16
13. BIBLIOGRAFÍA.....	18

LISTA DE TABLAS

Tabla 1. Roles para la Gestión de Incidentes.....	7
Tabla 2. Impacto del Incidente de Seguridad.....	10
Tabla 3. Valoración del Incidente y Tratamiento.....	10
Tabla 4. Actividades para la gestión de incidentes.....	11

	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 3 de 18

1. OBJETIVO.

Gestionar adecuadamente los incidentes y eventos de seguridad y privacidad de la información, seguridad informática o seguridad digital (en adelante **incidentes de seguridad**), mediante el reporte oportuno de los usuarios y la respectiva identificación, atención y respuesta, para reducir la afectación negativa de la seguridad de la información y/o la continuidad de las operaciones en el IDEP.

2. ALCANCE.

Inicia con la detección del posible incidente de seguridad de la información, continúa con la estrategia de contención y solución y termina con el análisis y documentación post-incidente.


3. REFERENCIAS NORMATIVAS.

- a) Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información (MSPI-MinTIC).
- b) Guía Evidencia Digital (MSPI-MinTIC).
- c) GTC-ISO/IEC 27035:2013
- d) Gestión de incidentes de seguridad de la información Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0
- e) Manual de procedimientos para Cadena De Custodia — FISCALIA General de la nación. NTC-ISO-IEC27001:2013: Sistemas de Gestión de la Seguridad de la información. NTC-ISO-IEC27037:2012:
- f) Guía para la identificación, recolección, adquisición y preservación de evidencias digitales. Ley 527 de 1999: por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- g) Ley 1273 de 2009: de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones
- h) Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

4. DOCUMENTOS ASOCIADOS.

Los documentos asociados a la presente guía, aportan información para su elaboración y están directamente relacionados con la gestión de la seguridad y privacidad de la información del IDEP. A continuación, se relacionan:


- Resolución No. 040 de 2017 del IDEP – Política de Privacidad y Tratamiento de datos personales.
- PO-GT-12-01 Política Seguridad y privacidad de la información.
- PL-GT-12-02 Plan de Contingencia Tecnológica.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 4 de 18

- PL-GT-12-04 Plan de Seguridad y Privacidad de la Información-IDEP.
- PL-GT-12-05 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información - IDEP 2019.
- PL-GT-12-01 Plan Estratégico de Tecnologías de la Información y las Comunicaciones.
- Guía No. 21 para la Gestión y Clasificación de Incidentes de Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.

5. DEFINICIONES.

- **Activo de información:** Es cualquier elemento que tenga valor para la organización y, en consecuencia, debe ser protegido.
- **Amenaza:** Factor externo que aprovecha una debilidad en los activos de información y puede impactar en forma negativa en la entidad.
- **Autenticidad:** Aseguramiento de la identidad respecto al origen cierto de los datos o información que circula por la Red.
- **Cadena de Custodia:** Registro detallado del tratamiento de la evidencia, incluyendo quienes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma.
- **COLCERT:** Grupo de Respuesta a Emergencias Cibernéticas de Colombia.
- **Contención:** Evitar que el incidente siga ocasionando daños.
- **CSIRT:** Por las siglas en inglés de Computer Security Incident Response Team, es el equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRT-PONAL.
- **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales, tales como nombre, apellido, cedula, edad, color de ojos, estatura, fotografía o video de la persona, entre otros.
- **Erradicación:** Eliminar la causa del incidente y todo rastro de los daños.
- **Evento de seguridad:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad y privacidad de la información o una situación desconocida previamente que puede ser pertinente a la seguridad.
- **Gestión de Incidentes:** Es el conjunto de todas las acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, tendientes a evitar y eventualmente responder de manera eficaz y eficiente a incidentes de seguridad que afecten activos de una Entidad. Minimizando su impacto en el negocio y la probabilidad que se repita.
- **Impacto:** Consecuencias que produce un incidente de seguridad sobre la organización.

	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 5 de 18


- **Incidente de seguridad de la información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Log's:** Registro de los sistemas de información que permite verificar las tareas o actividades realizadas por determinado usuario o sistema.
- **Recuperación:** Volver el entorno afectado a su estado natural.
- **Sniffer:** Software que captura los paquetes que viajan por la red para obtener información de la red o del usuario.
- **Suplantación de identidad:** Todas aquellas actividades realizadas por la que una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal.
- **Validación:** Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.
- **Vulnerabilidad:** Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas.

6. CICLO DE VIDA DE LA GESTIÓN Y RESPUESTA A UN INCIDENTE DE SEGURIDAD



La etapa de preparación debe ser apoyada por la dirección de tecnologías de la información o quien haga sus veces, incluyendo las mejores prácticas para el aseguramiento de redes, sistemas, y aplicaciones, por ejemplo:

- **Gestión de Parches de Seguridad:** El IDEP gestiona el despliegue y actualización de (Sistemas Operativos, Bases de Datos, Aplicaciones, Otro Software Instalado), este programa ayudara a los administradores en la identificación, adquisición, prueba e instalación de los parches.
- **Aseguramiento de plataforma:** Se debe configurar la menor cantidad de servicios (principio de menor privilegio) con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios como a otros equipos. Se deben revisar configuraciones por default (usuarios, contraseñas y archivos compartidos). Cada recurso que pueda ser accedido por externos e incluso por usuarios internos debe desplegar alguna advertencia.

	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 6 de 18

Los servidores deben tener habilitados sus sistemas de auditoría para permitir el login de eventos.


- **Seguridad en redes:** Debe existir una gestión constante sobre los elementos de seguridad. Las reglas configuradas en equipos de seguridad como firewalls deben ser revisadas continuamente. Las firmas y actualizaciones de dispositivos como IDS o IPS deben encontrarse al día. Todos los elementos de seguridad y de red deben encontrarse sincronizados y sus logs deben ser enviados a un equipo centralizado de recolección de logs para su respectivo análisis.
- **Prevención de código malicioso:** Todos los equipos de la infraestructura (servidores como equipos de usuario) deben tener activo su antivirus, antimalware con las firmas de actualización al día.
- **Sensibilización y entrenamiento de usuarios:** Usuarios en la entidad incluidos los administradores de TI deben ser sensibilizados de acuerdo a las políticas y procedimientos existentes relacionados con el uso apropiado de redes, sistemas y aplicaciones en concordancia con los estándares de seguridad de la entidad. Los encargados de los sistemas de información deben establecer las necesidades de capacitación de las personas encargadas de la protección de los datos.

La etapa de detección y análisis: identificar las características de un ataque, verificar que realmente ha sucedido y en el caso afirmativo, determinar su tipo y magnitud. No es fácil en todos los casos determinar con precisión si se ha producido o no un incidente de seguridad de la información y si es así, identificar su tipo y evaluar a priori su peligrosidad. La correcta detección de un incidente de seguridad se realiza mediante diferentes fuentes: sistemas antivirus, caídas de servidores, reportes de usuarios, monitoreo, logs y alertas en sistemas de seguridad.

La etapa de contener, erradicar y recuperar: con la contención permite proteger sistemas y redes limitando el daño, en esta fase se detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la infraestructura de tecnología y posteriormente erradicación del incidente o recuperación de los sistemas afectados. por tal motivo es prioritario 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. De esta manera restaurar los sistemas afectados por el incidente a su estado operativo. También contempla la eliminación de los componentes que han provocado el incidente igualmente implementar el PL-GT-12-02 Plan de Contingencia Tecnológica.

La etapa post incidente: Lo más importantes de un plan de respuesta a incidentes de tecnología es aprender del incidente y la mejora continua. Por tal motivo se debe mantener documentación y/o registros que permita conocer exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente. Una vez que se hayan finalizado las fases de documentación y recuperación, debemos revisar el proceso minuciosamente, determinar qué pasos se siguieron correctamente y qué errores se cometieron.

Las actividades en esta fase incluyen:

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 7 de 18


- Escribir el informe de incidente
- Analizar los problemas encontrados durante la respuesta a incidentes.
- Verificar las herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.
- Proponer mejoras basadas en los problemas encontrados
- Presentación del informe a las partes interesadas pertinentes

7. ROLES PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.


Para una adecuada gestión de incidentes de seguridad de la información deben interactuar coordinadamente diferentes roles y responsabilidades, que se describen en la Tabla No. 01.

Tabla 1. Roles para la Gestión de Incidentes.

No.	ROL	RESPONSABILIDADES	RESPONSABLE IDEP
1	Director de tecnología o CIO (Chief Information Officer)	<ul style="list-style-type: none"> • Asesorar a la Dirección General del IDEP en lo que se refiere al aprovechamiento y uso de TICS, para el cumplimiento de la misión. 	Jefe Oficina Asesora de Planeación.
2	Oficial de Seguridad de la Información ante el COLCERT.	<ul style="list-style-type: none"> • Orientar y dar adecuado tratamiento a los incidentes de seguridad de la información detectados o reportados. • Debe hacer un seguimiento periódico a los incidentes de seguridad presentados. 	Técnico Operativo de la Oficina de Planeación.
3	Responsable de Seguridad de la Información para la entidad.	<ul style="list-style-type: none"> • Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo. • Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad. • Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información. • Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido. • Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos. 	Ingenieros de la Oficina de Planeación

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 8 de 18

No.	ROL	RESPONSABILIDADES	RESPONSABLE IDEP
		<ul style="list-style-type: none"> • Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo. • Encarrilar el proyecto hacia el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la entidad. • Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario. • Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos. • Trabajar de manera integrada con el grupo o áreas asignadas. • Asegurar la calidad de los entregables y del proyecto en su totalidad. • Velar por el mantenimiento de la documentación del proyecto, su custodia y protección. • Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el proyecto en cuanto a la documentación de las lecciones aprendidas. • Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto. 	
4	Responsable del tratamiento de los datos personales	<ul style="list-style-type: none"> • Decidir sobre las bases de datos que contengan este tipo de datos. • Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales. • Tramitar las consultas, solicitudes y reclamos. • Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran. • Respetar las condiciones de seguridad y privacidad de información del titular. • Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente. 	Ingenieros de la Oficina de Planeación
5	Personal IDEP.	<ul style="list-style-type: none"> • Reportar oportunamente los incidentes o eventos de seguridad de la información y cualquier comportamiento anormal que se presente en la Entidad o en sus activos de información. • Recibir las capacitaciones y participar en las campañas de sensibilización que se realicen al interior de la entidad referente a seguridad y privacidad de la información. 	Funcionarios y Contratistas.

	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 9 de 18

8. TIPOS DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN.

Los incidentes de seguridad de la información a los que puede estar expuesto el IDEP son:

- Acceso no autorizado a la información.
- Divulgación de información sensible.
- Daño de la información.
- Ataques Informáticos externos o internos.
- Ataques dirigidos y no dirigidos.
- Pérdida o robo de la información.
- Modificación no autorizada de la información.
- Información no actualizada.
- Mala gestión del conocimiento.
- Perdida o daño de la documentación.
- Daños sobre Activos de información.
- Uso indebido de Activos de información.
- Uso Indebido de Software.
- Uso Indebido de Usuarios.
- Suplantación de Identidad.

9. POLÍTICAS DE OPERACIÓN PARA LA GESTIÓN DE INCIDENTES.


Los posibles incidentes de seguridad de la información detectados por los funcionarios o contratistas, deben ser reportados a la Oficina Asesora de Planeación – Proceso de Gestión Tecnológica, a través de algunos de los siguientes canales:

- Enviando un mensaje de correo electrónico con el reporte de la posible incidencia al correo electrónico clinares@idep.edu.co.
- A través de la Mesa de Ayuda del IDEP, en el enlace: <http://www.idep.edu.co/mesadeayuda/>
- Llamando al Técnico Operativo de la Oficina Asesora de Planeación a la Extensión **No. 107**.

El funcionario o contratista que identifique el posible incidente de seguridad debe reunir la información que llevó a determinar que es un posible incidente, la cual podrá ser utilizada en la atención del mismo, Ejemplo: capturas de pantalla, correos electrónicos, fotografías, videos entre otros.

10. PROCEDIMIENTO PARA LA ATENCIÓN DEL INCIDENTE.

10.1. El Técnico Operativo de la OAP o el Ingeniero designado para atender el incidente reportado por alguno de los canales antes mencionado, deberá categorizarlo

	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 10 de 18

acorde con los tipos de incidente de seguridad de la información descritos en el punto anterior y seguir los pasos que a continuación se describen:

- 10.2.** El responsable asignado debe atender de manera inmediata el incidente de Seguridad de la Información y categorizarlo de acuerdo con su impacto y valoración en la herramienta de gestión que disponga el IDEP y de acuerdo al siguiente cuadro: **(FT-GT-12-21 Formato de registro de Incidentes de Seguridad de la Información)**


Tabla 2. Impacto del Incidente de Seguridad.

Impacto	Descripción
Catastrófico o Mayor	Interrumpe seriamente la operación de la entidad, el incidente puede tener velocidad significativa/rápida en su propagación y ocasionar daños de activos. Podría llegar a afectar más de un tipo de activo.
Moderado o Menor	Interrumpe en un periodo corto de tiempo los procesos generales de la entidad, el incidente/evento compromete un activo importante.
Insignificante	No interrumpe los procesos generales de la entidad, el incidente/evento se detecta y se puede controlar fácilmente con recursos existentes en la entidad.

- 10.3.** El responsable de atender el incidente de Seguridad de la Información, debe conocer la siguiente tabla de escalamiento a fin de darle el tratamiento adecuado al mismo.

Tabla 3. Valoración del Incidente y Tratamiento.

Valoración	Tratamiento
Alta	Se escala a los proveedores pertinentes y si es el caso a las autoridades externas competentes. Así mismo, se presenta reporte ante el Comité Institucional de Gestión y Desempeño.
Media	Se implementan acciones en los sistemas de información o activos de información por parte del Técnico Operativo o los Ingenieros Contratistas del Proceso de Gestión Tecnológica del IDEP y si es necesario se escala al proveedor correspondiente.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 11 de 18

Valoración	Tratamiento
Baja	Solo se diligencia el caso en la herramienta de gestión dispuesta por la entidad, o se escala al responsable del activo de información involucrado en caso de ser necesario.

10.4. Dependiendo del Impacto y la Valoración, se pueden reportar incidentes de seguridad de la información a través de los siguientes canales y seguir las indicaciones dadas en el punto 10 de la presente guía:


- ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), reportar al correo electrónico: contacto@colcert.gov.co o al Teléfono: (+571) 2959897.
- CSIRT Gobierno reportar al correo csirtgob@mintic.gov.co.
- Centro cibernético Policial reportar en la siguiente ruta: <https://caivirtual.policia.gov.co/>

11. RELACIÓN DE ACTIVIDADES PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN:


Para la gestión de los posibles incidentes que se puedan presentar en el IDEP se deben seguir los pasos que a continuación se describen:

Tabla 4. Actividades para la gestión de incidentes.


Actividades	Descripción	Responsable
Reportar el incidente de seguridad de la Información	Los funcionarios y contratistas con acceso a información de la entidad nota que se está presentando un ataque a los activos de la entidad, o es conocedor de que alguna persona está violando las políticas de seguridad y privacidad de la información o conoce de riesgos asociados a la información, debe proceder a reportar esta situación como un evento o incidente de seguridad la mesa de ayuda de la entidad, enviar un correo a <i>clinares@idep.edu.co</i> , llamando a la Extensión 107 o informando directamente al Oficial de Seguridad de la información.	Los funcionarios y contratistas del IDEP.
Registrar evento o incidente	El Técnico Operativo o Ingeniero Contratista de la OAP toman los datos necesarios y realiza el registro correspondiente en el FT-GT-12-21 Formato de registro de Incidencias de Seguridad de la	Técnico Operativo o Ingenieros

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 12 de 18


Actividades	Descripción	Responsable
	Información, categorizando si se trata de incidente o evento, fecha y hora, descripción de lo ocurrido, si se puede solucionar de inmediato se documenta la solución aplicada, entre otros.	Contratistas de la OAP.
Evaluar el impacto incidente.	En dado caso el Técnico Operativo o los Ingenieros Contratistas de la OAP no puedan resolver el evento/incidente se escala al Responsable de Seguridad de la Información, quién evaluará que tipo de evento/incidente es el que se presenta, a que activos está afectando, cual es alcance del mismo, que pronóstico tiene de expansión, así como los daños potenciales o reales que se generen. Para evaluar la severidad de los eventos/incidentes considerará la importancia de los activos y el nivel del incidente. Cuando exista la convivencia de más de un activo comprometido y/o más de un incidente o evento, todo el conjunto se valorará de acuerdo a los niveles descritos en la Tablas No. 02.	Técnico Operativo, Ingenieros Contratistas y Jefe de la OAP.
Identificar la valoración del incidente.	Se establecerá la afectación del activo de información, incluyendo el valor económico y la cantidad información relevante para la Entidad contenida en el mismo.	Técnico Operativo, Ingenieros Contratistas y Jefe de la OAP.
Identificar el nivel del incidente	El Técnico Operativo o los Ingenieros Contratistas de la OAP, deberán identificar el nivel de afectación del incidente de acuerdo a los Niveles de Criticidad del Evento/Incidente descritos en la Tabla 2 de la presente guía.	Técnico Operativo, Ingenieros Contratistas - OAP.
Escalar el incidente	Para buscar una solución al incidente el Técnico Operativo o los Ingenieros Contratistas de la OAP, debe tener en cuenta los niveles de escalamientos Tabla 3 de la presente guía.	Técnico Operativo, Ingenieros Contratistas - OAP.
Establecer la estrategia de respuesta de acción ante incidentes de Seguridad de la Información	Para saber cómo actuar ante un incidente el Técnico Operativo y los Ingenieros Contratistas de la OAP, deberán tener claro el nivel de evento/incidente y debe considerar los siguientes tipos de respuesta: <ul style="list-style-type: none"> • Proceder de acuerdo con las instrucciones de la brigada de emergencias y según lineamientos de los cuerpos de socorro, privilegiando la 	Técnico Operativo, Ingenieros Contratistas - OAP.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 13 de 18


Actividades	Descripción	Responsable
	<p>conservación de la vida e integridad del personal tanto de la IDEP como de visitantes.</p> <ul style="list-style-type: none"> En la medida que haya tiempo y recursos, el Técnico Operativo o los ingenieros contratistas deberán adelantar las actividades que tiendan a proteger la información Institucional. 	
Iniciar la estrategia de Contención	<p>El Técnico Operativo y los Ingenieros Contratistas de la OAP, deben tener en cuenta los siguientes factores para la contención del incidente o evento:</p> <ul style="list-style-type: none"> Daño potencial de recursos a causa del incidente. Necesidad de preservación de la evidencia. Tiempo y recursos necesarios para poner en práctica la estrategia. Efectividad de la estrategia. Duración de las medidas a tomar. Criticidad de los sistemas afectados. Características de los posibles atacantes. Si el incidente es de conocimiento público. Pérdida económica. Posibles implicaciones Legales. 	Técnico Operativo, Ingenieros Contratistas OAP.
Recolectar evidencia	<p>Para hacer una correcta recolección de evidencia el Técnico Operativo y los Ingenieros Contratistas de la OAP, deben tener en cuenta lo siguientes criterios para la recolección de evidencia:</p> <ul style="list-style-type: none"> Información basada en la red: Log's de IDSs, logs de monitoreo, información recolectada mediante Sniffers, logs de routers, logs de firewalls, información de servidores de autenticación. Información Basada en el Equipo: Live data collection: Fecha y hora del sistema, aplicaciones corriendo en el sistema, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la tarjeta de red. <p>Otra información: Testimonio de funcionario o contratista que reporta el evento o incidente.</p>	Técnico Operativo, Ingenieros Contratistas - OAP.
Manejar la evidencia	<p>El Técnico Operativo y los Ingenieros Contratistas de la OAP deben darle un correcto manejo a los datos y evidencias recolectadas, los cuales deben ser almacenados para futuras investigaciones e</p>	Técnico Operativo.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 14 de 18

Actividades	Descripción	Responsable
	<p>implementación de controles preventivos o de mejoramiento.</p> <p>La información que debe ser almacenada y custodiada por el Técnico Operativo e incluye:</p> <ul style="list-style-type: none"> • Cantidad de incidentes presentados y tratados. • Tiempo asignado a los incidentes. • Daños ocasionados. • Vulnerabilidades explotadas. • Cantidad de activos de información involucradas. • Frecuencias de ataques. • Pérdidas. <p>Además, debe cumplir con un control de seguridad que garantice la confidencialidad, integridad y disponibilidad de las evidencias retenidas. Para esto, el almacenamiento físico seguro de las evidencias estará custodiado por el Técnico Operativo y el electrónico se almacena la caja fuerte ubicada en la Subdirección Administrativa y Financiera del IDEP.</p>	
Identificar las fuentes de ataque	<p>El Técnico Operativo o los Ingenieros Contratistas de la OAP, deben tener identificadas las posibles fuentes de ataque como:</p> <ul style="list-style-type: none"> • Empleados Descontentos. • Baja Concientización. • Crecimiento de Redes. • Falta de Previsión de Contingencias. • Falta de Políticas. • Desastres Naturales. • Inadecuada protección de la Infraestructura. • Confianza creciente en los sistemas • Virus. • Caballos de Troya. • Explotación de Vulnerabilidades, tanto a nivel de host, como de arquitectura de red (vulnerabilidades de la seguridad perimetral). • Falsificación de identificadores (biométricas, de autenticación o de encabezado de paquetes). • Robo de Información confidencial. • Violación a la privacidad. • Ingeniería social. • Denegación de Servicios. 	Técnico Operativo, Ingenieros Contratistas - OAP.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 15 de 18

Actividades	Descripción	Responsable
	<ul style="list-style-type: none"> Hacking. 	
Establecer la estrategia de Erradicación	<p>El Técnico Operativo o los Ingenieros Contratistas de la OAP, deben tener en cuenta para definir/decidir las estrategias de erradicación los siguientes factores:</p> <ul style="list-style-type: none"> Tiempo y Recursos necesarios para poner en práctica la estrategia. Efectividad de la Estrategia. Pérdida económica. Posibles implicaciones legales. Relación costo-beneficio de la estrategia. Experiencias anteriores. Identificación de los Procedimientos de cada sistema Operativo comprometido. Identificación de Usuarios o servicios comprometidos para proceder a desactivarlos. 	Técnico Operativo, Ingenieros Contratistas - OAP.
Aplicar los procedimientos de Recuperación	<p>El área encargada de gestionar el incidente de seguridad, para definir/decidir las estrategias de recuperación debe tener en cuenta los siguientes factores:</p> <ul style="list-style-type: none"> Cargar la copia de respaldo actualizada del sistema de información, configuración o base de datos. Creación nuevamente de la información digital o física, configuración de sistemas operativos, sistemas de información, cargue manual de la información. Actualización, instalación de parches de seguridad a los sistemas que se vieron comprometidos. Entre otras definidas en el PL-GT-12-02 Plan de Contingencia Tecnológica. 	Técnico Operativo, Ingenieros Contratistas - OAP.
Realizar el análisis Post-Incidentes	<p>El Técnico Operativo, Ingenieros Contratistas y Jefe de la OAP debe garantizar el correcto manejo de las lecciones aprendidas, de la siguiente manera:</p> <ul style="list-style-type: none"> Se busca definir esquemas más efectivos para responder ante situaciones que afecten la seguridad de la información en la entidad. 	Técnico Operativo, Ingenieros Contratistas y Jefe de la OAP.


 ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN <small>Instituto para la Investigación Educativa y el Desarrollo Pedagógico</small>	GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 16 de 18

Actividades	Descripción	Responsable
	<ul style="list-style-type: none"> • Mantener la documentación de los eventos e incidentes de seguridad de la Información. • Integrar los eventos e Incidentes a la Matriz de Riesgos del Proceso de gestión Tecnológica. • Realización de Capacitaciones a los Funcionarios de la entidad en lo relacionado a eventos e incidentes de seguridad de la información. • Analizar los Hechos y tomar decisiones. 	

12. HERRAMIENTAS, PLATAFORMAS Y CONTROLES DE PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS.

En relación con la protección contra códigos maliciosos esta se realiza de las siguientes maneras:

1. La capacitación a los usuarios, ya sea en jornadas de sensibilización o mediante el envío de correos electrónicos. En ambos casos se ilustra sobre las formas más comunes en las cuales se puede ejecutar de forma involuntaria códigos maliciosos que se envían en los correos electrónicos o en medios de almacenamiento externos. Con esto se busca, además de construir una cultura de seguridad informática, que las personas usen de forma cotidiana buenas prácticas de seguridad en el manejo de la información. Se está registrado en ColCERT y en el grupo de Whatsapp de Seguridad de la información de la Alta Consejería Distrital para las TIC, quienes mantienen informado sobre riesgos asociados a la seguridad.
2. Se cuenta con la instalación un equipo de seguridad perimetral (Firewall) que está verificando el tráfico que entra y sale de la Red LAN del IDEP, que realiza principalmente filtrado de acceso a sitios web, control de aplicaciones web, control y prevención de intrusos, así como la revisión de virus. Esta herramienta cuenta con una suscripción hasta el 2021, que permite tener acceso a las actualizaciones de firmas y bases de datos que elabora el fabricante, con la información más reciente de seguridad que usa el firewall para verificar el tráfico y con ello determinar si bloquea o no, el tráfico saliente o entrante a la RED. La suscripción con la que cuenta el firewall, permite que las actualizaciones se realicen de forma automática y con la frecuencia con la que el proveedor considere pertinente, de acuerdo con la identificación de riesgos o ataques que se producen a nivel mundial. La renovación de esta suscripción es muy importante para tener todas las funcionalidades funcionando con firmas y bases de datos actualizadas.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p>GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION</p>	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 17 de 18

El Firewall tiene garantía y soporte por parte del fabricante, para que, en caso de fallo, este sea remplazado por uno nuevo, además de contar con el soporte por parte del fabricante, para el caso de problemas en el funcionamiento. La actualización del IOS o sistema operativo se realiza de forma manual, y se requiere, y se hace, de ser posible, con la intervención del proveedor o con los manuales y página de soporte del fabricante.

Durante el proceso contractual, se grabó la instalación, configuración y renovación de las licencias, complementado por una transferencia de conocimiento de la administración y funcionamiento de la aplicación, por parte del proveedor.


En el siguiente link, se encuentra detalla la información técnica de configuración, administración del equipo de seguridad perimetral:
https://www.google.com/url?q=https://docs.fortinet.com/product/fortigate/6.2&sa=D&source=hangouts&ust=1576774257422000&usg=AFQjCNEb_v-rDTmhVyiiRSOPZZqL9jHMpQ

3. Se cuenta con una herramienta de antivirus instalada en todos los equipos de la entidad, incluyendo los servidores, la cual se encarga de la revisión de los documentos que están allí alojados, revisando de forma automática los archivos que se descargan o los que están en medios externos de grabación que se conectan al equipo. Para la administración de todos los equipos se cuenta con una consola, que gestiona mediante agentes instalados en cada computador que reportan el estado de éstos, permitiendo programar tareas de actualización tanto de la versión del agente, del motor de antivirus y las bases de datos, así como la revisión de cada equipo, con la periodicidad requerida. Esta solución cuenta con la opción de realizar el monitoreo de las actualizaciones y parches en los equipos, permitiendo tener un tablero de control sobre el estado a este respecto. Recientemente se realizó la renovación de la licencia por tres años, quedando hasta el 2021 la protección. De otra parte, el antivirus puede detectar ataques a los equipos y realizar los bloqueos y mensajes de alerta, respectivos. El contrato de renovación de las licencias, cuenta con garantía y soporte básico, durante el mismo periodo de la duración de las licencias.

Durante el proceso contractual, se grabó la instalación, configuración y renovación de las licencias, complementado por una transferencia de conocimiento de la administración y funcionamiento de la aplicación, por parte del proveedor.

En el siguiente enlace, se encuentra la información técnica de soporte, además de los manuales de ésta aplicación:

Para la consola de Antivirus, Security Center
<https://support.kaspersky.com/ksc11?qs=on>

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. EDUCACIÓN Instituto para la Investigación Educativa y el Desarrollo Pedagógico</p>	<p>GUÍA PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION</p>	Código: GU-GT-12-01
		Versión: 3
		Fecha de Aprobación: 20/12/2021
		Página 18 de 18

Para el antivirus instalados en los clientes: <https://support.kaspersky.com/kes11>
<https://support.kaspersky.com/kes10linux>

4. Tanto los sistemas operativos propietarios de los servidores y de todos los equipos de cómputo, así como el software instalado en ellos, está debidamente licenciado, además de encontrarse dentro del ciclo de vida vigente de los mismos. Esto permite acceder a las actualizaciones y parches de seguridad, liberados por los fabricantes (Sistema Operativo y Aplicaciones), los cuales mantienen los equipos con las más recientes actualizaciones tanto de aplicaciones como de seguridad. Para los equipos de cómputo, las actualizaciones se hacen de forma automática y para los servidores, el servicio de alertas de actualización informa sobre la existencia de las actualizaciones, que serán aplicadas por el administrador del servidor.

Para los equipos con sistema operativo no propietario (Libre, ó, GNU), en este caso Linux, se ejecutan manualmente las tareas de actualización tanto del sistema operativo, como de las aplicaciones.

Las páginas de soporte de las aplicaciones y el sistema operativo, se encuentra la información detallada, para ambos casos en los siguientes enlaces:

<https://support.microsoft.com/es-co/hub/4338813/windows-help?os=windows-10>

13. BIBLIOGRAFÍA.

- Guía No. 21 para la Gestión y Clasificación de Incidentes de Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.