TABLA DE CONTENIDO:

1. OBJETIVO:

Establecer el marco conceptual para identificar y clasificar los incidentes/eventos de seguridad de la información, con el fin de darles el tratamiento adecuado y evitar que vuelva a repetirse.

2. ALCANCE:

La guía comprende el marco conceptual de todos los incidentes de seguridad de la información y eventos detectados por colaboradores y terceros que afecten o puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información de la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología - ATENEA.

3. DEFINICIONES

Evento de seguridad de la información: Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la política de seguridad y privacidad de la información, una falla en los controles o una situación previa desconocida hasta el momento y que puede ser relevante para la seguridad.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información.

Gestión de incidentes de seguridad de la información: Procesos para la detección, reporte, evaluación, respuesta, tratamiento y aprendizaje de incidentes de seguridad de la información.

Sistema de Información: Aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar información.

4. NORMATIVIDAD ASOCIADA:

Resolución 500 del 10 de marzo de 2021 del Ministerio de Tecnologías de la Información y Comunicaciones.

5. DESARROLLO:

A continuación, se plantea una serie de conceptos para dar cumplimiento con el ciclo de gestión y respuesta a un incidente de seguridad.

Prevención

La función de prevención admite la capacidad de limitar un posible incidente de seguridad de la información, por tal motivo se debe velar por la disposición de recursos y herramientas necesarias

para implementar buenas prácticas con el fin de asegurar las redes, sistemas de información, servicios tecnológicos y demás recursos institucionales.

Por lo anterior se adoptarán las siguientes medidas:

- **Fuga de información:** Se realizarán las actividades necesarias, encaminadas a la implementación de una herramienta que permita prevenir la fuga de información clasificada y reservada, conforme lo reportado en la matriz de activos de información

- **Gestión y documentación de seguridad sobre la plataforma tecnológica:** Se gestionará los elementos de seguridad necesarios tales como Firewall, IPS, SIEM, protección contra código malicioso, aplicación de parche de seguridad para proteger los servicios y recursos tecnológicos institucionales y realizar la documentación con el fin de mantener las rutas y acciones correspondientes.

- **Recursos documentados:** Se mantendrá documentados los puertos habilitados, diagramas de red actualizados, información de servidores con sus respectivos parches y usuarios configurados, contando así con la ubicación rápida de los recursos existentes

- **Sensibilización de colaboradores:** A través del plan de sensibilización y apropiación, se incorporarán los elementos necesarios en materia de seguridad de la información que permita socializar a los colaboradores de la Entidad las políticas y procedimientos existentes.

Detección

Descubrir que posiblemente un incidente ha ocurrido, se evidencia generalmente a través de los siguientes eventos:

- Reportes de usuarios y proveedores
- Funcionamiento anormal del software o hardware (equipos que se apagan/encienden sin interacción humana, apertura de ventanas en el navegador de internet, desaparición de documentos, entre otros)
- Alertar de las herramientas de seguridad informática.
- Pérdida total o parcial de los servicios institucionales.

Análisis

Una vez considerados los eventos, se puede dar uso de diversas fuentes de información que permitan analizar el origen y futuras ocurrencias, para ello se emplearán, pero sin limitar:

- **Registros a nivel de red:** logs del Firewall, Proxy, SIEM, IPS, conexiones a protocolos y destinos a nodos con reputación maliciosa.
- **Registros del usuario:** archivos adjuntos
- **Registros a nivel de equipo:** logs de accesos, cargas excesivas de disco/memoria, DLP, archivos ocultos y huérfanos, antivirus, antispam, procesos de escucha y conexión con puertos/host extraños
- **Registros a nivel de aplicación:** logs de auditoría y accesos no autorizados, acciones realizadas en la aplicación con fecha-hora-usuario, verificación de la sincronización de los relojes.
- **Registro de base de conocimiento:** Mantener registradas las lecciones aprendidas en el manejo de incidentes.

Clasificación

Conforme a la infraestructura institucional se identifican, pero no se limitan las posibles clasificaciones

TIPO	DESCRIPCIÓN
Compromiso de la Información	Actividad exitosa de destrucción, corrupción, o fuga de información sensible, sensitiva o propiedad intelectual Agencia.
Contenido Abusivo	Mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva
Disponibilidad	Actividad realizada de manera intencional con el fin de mantener indisponible los servicios institucionales
Fraude	Actividad basada en el engaño de forma intencional originada por persona u organización con el propósito de recibir dinero u otro beneficio que no le corresponde
Intrusiones	Ataque o acto directo o indirecto, que causa daño al nombre o marca de la Agencia.
Obtención de Información	Compromiso de la información afectando su integridad y confidencialidad a través de escaneos, phishing e ingeniería social
Política de Seguridad	Uso y acceso no autorizado de recursos, violación de derechos de autor, entre otros.
Virus	Engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

Tabla No. 1 Incidentes

Se relacionan posibles eventos por tipo que pueden ser reportados

TIPO	DESCRIPCIÓN
Actividades de reconocimiento	Cualquier Tipo de actividad detectada que genere alguna alerta con el cual se está realizando reconocimiento de la plataforma (escaneo de puertos, identificación de sistema, conexiones especiales a servicios) o detección de búsquedas recursivas dentro de servicios o aplicaciones.
Intento fallido de conexiones	Intentos de autenticación fallida a servicios de administración remota o portales de autenticación a servicios.
Infiltración Lógica	Cualquier intento o probable acceso lógico no autorizado dependiente de los niveles de autorización y autenticación determinados para cualquier servicio, aplicación, sistema de información, servidor o equipo, originado desde una red considerada como confiable, interna de la organización o del mismo rango en el que se encuentra el equipo al cual se realiza el acceso lógico no autorizado.
Uso Inadecuado de recursos	Uso de cualquier tipo de recursos involucrado con cualquier tipo de información, que intente una violación en contra del respeto por los derechos de información, creación intelectual, privacidad, divulgación, accesibilidad de información y uso adecuado determinado dentro de un ambiente establecido.
Falla de Hardware	Cualquier detección de fallas de componentes electrónicos o componentes electromecánicos (e.j. discos, cintas) que puedan causar una afectación a la confidencialidad, integridad y/o disponibilidad de la información
Falla de Software	Cualquier detección de fallas en el diseño de software y/o error de codificación de software que puedan causar una afectación a la confidencialidad, integridad y/o disponibilidad de la información.
Falla en las Comunicaciones	Cualquier detección de falla de comunicaciones bien sea generada al interior de la organización o por terceros que pueda causar una afectación a la confidencialidad, integridad y/o disponibilidad de la información.
Perdida de Servicios Esenciales	Cualquier detección de falla en servicios críticos para el negocio que no sean causados por fallas de hardware, software, comunicaciones o negación de servicio y puedan afectar directamente la confidencialidad, integridad y/o disponibilidad de la información.

Tabla No. 2 Eventos

Se relacionan posibles debilidades por tipo que pueden ser reportados

TIPO	DESCRIPCIÓN
Servicios o Configuraciones Vulnerables	La determinación de esta debilidad está dada por la identificación de vulnerabilidades en las plataformas tecnológicas de datos o seguridad que permitan la materialización del riesgo por medio de su explotación.
Falta de Políticas de Seguridad	Determinación de que no existen políticas de seguridad de la información que presenten los lineamientos básicos que rigen el comportamiento de los usuarios, el flujo de procesos y el funcionamiento de tecnologías.
Exposición de Información Sensible	Descubrimiento de información sensible para el negocio de cualquier tipo que no cumple con estándares de clasificación acorde a lineamientos de seguridad de la información
Métodos de autenticación deficiente	Identificación de métodos de autenticación destinado a recursos o información del negocio que no cumplan con estándares de seguridad que protejan el proceso mismo de autenticación
Deficiencia de Salvaguardas	Determinación de fallas en las salvaguardas de protección definidas dentro de plataformas tecnológicas o deficiencia de políticas, que, aunque se encuentren establecidas no generen la protección necesaria de las amenazas que puedan materializar el riesgo.
Configuración por Defecto	Hallazgo de configuraciones por defecto en cualquier servicio, servidor o plataforma que permita que se vea afectada la confidencialidad, disponibilidad o integridad de la información.
Error de Operaciones	Cualquier factor que genere un error relacionado al funcionamiento del sistema, dispositivo y/o procedimiento y que tenga una posibilidad de generación de afectación de la confidencialidad, integridad y/o disponibilidad de la información
Error de mantenimiento de hardware	Cualquier tipo de error dentro de actividades de mantenimiento de cualquier tipo de hardware que pueda generar afectación de la confidencialidad, integridad y/o disponibilidad de la información.
Error de mantenimiento de software	Cualquier tipo de error dentro de actividades de mantenimiento de cualquier tipo de software que pueda generar afectación de la confidencialidad, integridad y/o disponibilidad de la información.
Error de Usuario	Cualquier error en entrada u operación realizado por un usuario legítimo que pueda generar afectación de la confidencialidad, integridad y/o disponibilidad de la información.
Error de Diseño	Cualquier error funcional dentro de un diseño que genere afectación de la confidencialidad, integridad y/o

TIPO	DESCRIPCIÓN
	disponibilidad de la información.
Otros Errores Reales	Cualquier otro tipo de error no contemplado dentro de los anteriores que pueda generar algún tipo de afectación de la confidencialidad integridad y/o disponibilidad de la información.

Tabla No. 3 Debilidades

Evaluación, priorización y tiempo de respuesta

Conforme a la importancia dentro del proceso se prioriza en una primera instancia al momento de registrar el incidente, esta puede ser modificada en la medida que el incidente evolucione y su impacto pueda ser mayor.

Los tiempos expresados en la siguiente tabla son un acercamiento al tiempo máximo en que el incidente debe ser atendido, y no al tiempo en el cual el incidente debe ser solucionado. Esto se debe a que la solución puede variar dependiendo del caso.

PRIORIDAD	DESCRIPCIÓN
Crítica	Afecta un gran número de sistemas, usuarios o infraestructuras críticas de la Entidad. Compromete datos personales de niños, niñas, adolescentes y datos sensibles.
Alta	Afecta por lo menos un activo de información catalogados en nivel ALTO. Compromete datos personales.
Media	Afecta uno o más activos de información catalogados en nivel MEDIO. Efectos mínimos sobre sistemas e infraestructuras críticas.
Baja	Afecta los activos de información catalogados en nivel BAJO o sin identificar. Efecto insignificante en sistemas e infraestructuras

Tabla No. 4 Priorización y tiempo de atención

Para evaluar el incidente de seguridad se debe tener en cuenta los niveles de impacto con base en el análisis de riesgos y la clasificación de activos de información. La severidad del incidente puede ser:

EVALUACIÓN	
IMPACTO	**DESCRIPCIÓN**
Alta	El incidente de seguridad afecta activos de información considerados de impacto alto que influyen directamente a los objetivos misionales de la Entidad. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata
Media	El incidente de seguridad afecta activos de información considerados de impacto moderado que influyen directamente a los objetivos de un proceso determinado
Baja	El incidente de seguridad afecta activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

Tabla No. 5 Evaluación

A continuación, se detalla la prioridad con el impacto asociado.

PRIORIDAD	**IMPACTO**	**TIEMPO DE ATENCIÓN Horas**
Crítica	Alto	3
Alta		6
Media	Medio	8
Baja	Bajo	24

Tabla No. 6 Prioridad e Impacto

Contención, erradicación y recuperación

Luego de establecer en los pasos anteriores la identificación del incidente, se deben ejecutar las actividades de contención, erradicación y recuperación, conforme la siguiente descripción:

- Contención: Después de la identificación del incidente de seguridad, se realiza la contención de este, cuyo objetivo es disminuir el impacto del incidente en la Entidad.

Las acciones dependerán del tipo de incidente identificado, algunas de ellas pueden ser:

TIPO	ACCIÓN
Compromiso de la Información	Bloqueos de cuenta Apagado de la máquina Bloqueo de puertos
Contenido Abusivo	Nuevas reglas de filtrado
Disponibilidad	Bloqueo de Puertos Recuperación de servicios Restauración de copias de seguridad
Fraude	Recuperación de servicios Restauración de copias de seguridad
Intrusiones	Restauración de equipos y servicios Recuperación de los Datos Restauración de copias de seguridad
Obtención de Información	Bloqueo de Puertos Nuevas reglas de filtrado Bloqueos de cuenta
Política de Seguridad	Parches de seguridad Gestión de permisos
Virus	Desconexión de la red del equipo afectado Bloqueo de Puertos Actualización de herramientas de detección y bloqueo de software malicioso

Tabla No. 7 Contención

- **Erradicación y recuperación:** En la erradicación del incidente se deberán adoptar los controles para eliminar cualquier rastro de comportamiento inusual en la plataforma TI y activos de información.

Posterior se deben activar las estrategias que se consideren para recuperar y restablecer los servicios afectados.

Aprendizaje

A través del diligenciamiento del formato de reporte de incidentes se espera mantener una gestión del conocimiento con el fin de propender por las mejoras tecnológicas mediante las lecciones aprendidas, evitando así incidentes futuros o la repetición de lo sucedido.

Comunicación

A través del comité o la mesa de incidentes, se tomarán las decisiones que sean necesarias para las comunicaciones internas y externas que se deban emitir con motivo del incidente de seguridad de la información. Así mismo, determinará la necesidad de coordinar todas aquellas denuncias que deban ser instauradas ante los entes de control y vigilancia, aportando para ello las evidencias recaudadas, así como aquellos informes desarrollados con ocasión de la gestión del incidente.

Roles para la gestión de incidentes

A continuación, se realizará una breve descripción de los actores que intervienen y conforman el ciclo de gestión de incidentes de seguridad, con el fin de reportar, evitar y prevenirlos.

- **Usuario:** funcionario, contratista, pasante o terceros con acceso a los servicios y recursos tecnológicos institucionales, quienes deben estar concientizados sobre las gestiones de seguridad de la información. Encargados de reportar los posibles incidentes.

- **Mesa de ayuda:** Primer punto de contacto, encargado de recibir, clasificar y escalar las solicitudes por parte del usuario.
  Es importante tener en cuenta que, no es un actor que realiza la centralización de los incidentes reportado, da una gestión inicial y escala el incidente para que sea tratado.

- **Administrador del sistema o servicio:** Encargado de configurar y mantener un activo informático. Es notificado por Mesa de ayuda sobre un incidente de seguridad con el fin de analizar, identificar, contener y erradicar el incidente. Este debe documentar y notificar a la mesa sobre la solución de este.

- **Administrador plataforma de seguridad informática:** Encargados de configurar y mantener las plataformas de seguridad, tales como, firewall, antispam, sistemas de monitoreo, sistema de prevención de intrusos, entro otros que formen parte de la solución de las herramientas adquiridas por la entidad para la seguridad digital.

- **Subsistema de Gestión de Seguridad de la Información:** Revisa el cumplimiento de los estándares de operación y mejores prácticas, así como responder consultas sobre los incidentes que impacten de forma inmediata.

  También estará en la capacidad de convocar la participación de otras instancias institucionales cuando el incidente lo amerita.

  Finalmente será el encargado de sensibilizar a los actores involucrados en la gestión de incidentes de seguridad de la información y reportar a los entes competentes en la materia.

- **Subgerente de Tecnologías de la Información y las Comunicaciones:** convoca la participación de las instancias institucionales requeridas para la atención y comunicación del incidente.

  Adicional será el encargado de aprobar las acciones que se requieran dentro de la gestión de incidentes en la plataforma tecnológica, así como de activar las contingencias necesarias.

- **Mesa de incidentes:** Estará conformada por el/la subgerente de tecnologías de la información y las comunicaciones, el oficial de seguridad de la información, administradores del sistema/servicios

tecnológicos y cuando se requiera, el responsable del activo de información. Esta mesa se encargará de evaluar, notificar y realizar seguimiento en toda la gestión del incidente.

Reporte ante instancias competentes

Se debe tener en cuenta las siguientes instancias, sin limitarse:

- Cuando haya sido vulnerado o comprometido un componente de la infraestructura tecnológica institucional, se reportará como primera instancia la Subgerencia de Tecnologías de la Información a través del correo electrónico u otros medios establecidos para tal fin
- Se informará el incidente al CSIRT Gobierno a través de correo electrónico para su respectiva gestión y acompañamiento o contactando a la mesa de servicio.
- Si el incidente involucra datos personales se debe notificar a la Superintendencia de Industria y Comercio a más tardar dentro los quince (15) días hábiles siguientes al momento en que se detecte. Este reporte se realizará a través del siguiente enlace: https://rnbd.sic.gov.co/sisi/login en donde será seleccionada la base de datos reportada en el Registro Nacional de Bases de Datos – RNBD. Adicional se debe notificar a los titulares de la información que fue comprometida.
- De ser comprobada la participación mal intencionada de un funcionario o colaborador se reportará al proceso de evaluación y control con el fin de que estos surtan los procedimientos correspondientes.

6. ANEXOS:

No Aplica

7. DOCUMENTOS DE REFERENCIA:

Procedimiento de Gestión de Incidentes

8. RELACIÓN DE FORMATOS:

CODIGO	NOMBRE DEL FORMATO
	No aplica

9. CONTROL DE CAMBIOS:

Fecha	Versión	Descripción del Cambio
06/06/2023	V 2 GTI-GU-01	Se modifica la guía en los siguientes aspectos: Cambio de estructura de presentación de la información, ajuste en el alcance, responsabilidades y cambio en la asignación del código de acuerdo con las directrices establecidas en el Procedimiento de Elaboración, Modificación o Anulación de Documentos y Control de Documentos
16/01/2023	V1 GTI-GU-01	Modificación de pie de página según manual de identidad de Atenea y asignación cuadro control de cambios

VALIDACIÓN	NOMBRE	CARGO	FECHA
Elaboró	**Maria Alejandra Suarez**	**Contratista – Subgerencia TIC**	**19/05/2023**
Revisó	**Lira Jazmin Pineda Moreno**	**Subgerente TIC**	**26/05/2023**
Aprobó	**Lira Jazmin Pineda Moreno**	**Subgerente TIC**	**26/05/2023**