1. OBJETO:

Establecer la metodología y directrices para una respuesta efectiva ante incidentes de seguridad de la información, minimizando su impacto, protegiendo los activos de información, restableciendo la operación a su estado normal y promoviendo la mejora continua del proceso.

2. ALCANCE:

El documento define las etapas de gestión de incidentes, iniciando con la identificación y finaliza con las actividades Post-Incidentes. Aplica para los funcionarios y contratistas de la OTIC.

3. DEFINICIONES:

Activos de información: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes y servicios, edificios o personas) que tenga valor para la organización y por lo tanto se debe proteger.

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

Control: Medida que permite garantizar la reducción del nivel de un riesgo específico o mantenerlo dentro de límites aceptables.

Correlación de eventos: Asociaciones lógicas entre eventos registrados por diferentes aplicaciones, sistemas o dispositivos.

Disponibilidad: Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.

Equipo de respuesta a incidentes (IRT): Equipo interno de una organización designado para gestionar los incidentes de seguridad de la información.

Evento: Cualquier cambio de estado que tenga importancia para la gestión de un servicio o elemento de configuración. Los eventos generalmente se reconocen a través de notificaciones creadas por un servicio TI, elemento de configuración o herramienta de monitoreo.

Evidencia Digital: Prueba electrónica o cualquier dato digital probatorio de la información almacenada o transmitida en formato digital de tal manera que pueda ser utilizada en un juicio para probar un delito informático.

Host: Cualquier equipo conectado a una red de datos que consume u ofrece servicios, recursos o información a los usuarios.

Incidente: Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar, una interrupción o una reducción de la calidad de los servicios prestados por la entidad a los usuarios de este.

Incidente de seguridad de la información: Es un incidente que compromete las diferentes operaciones comerciales y la seguridad de la información en sus tres pilares, Confidencialidad, Integridad y Disponibilidad.

Información: Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada.

Integridad: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento deben ser exactos.

Mesa de Servicios: Es un conjunto de recursos tecnológicos y humanos, encargado de recibir, gestionar y resolver las solicitudes y problemas de los usuarios en una organización, brindando soporte y asistencia técnica de manera eficiente y efectiva

como principal y único punto de contacto con la Oficina de Tecnologías de la Información y Comunicaciones.

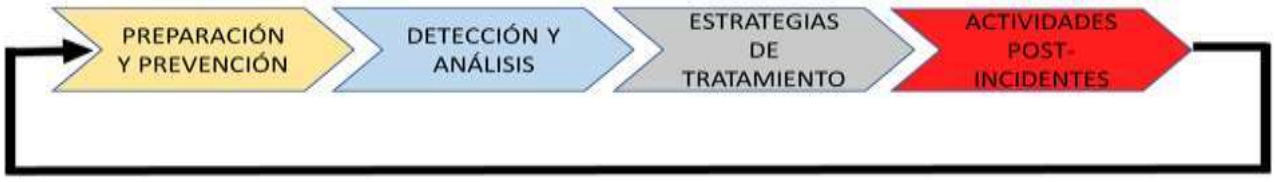
Log o Logs: Registro o Registros. Termino técnico usado para los datos que se genera en los sistemas (Servidores, Aplicaciones, Programas, etc) en forma de trazas textuales en el que constan cronológicamente los acontecimientos que afectan a un sistema o el conjunto de cambios que generan.

4. GENERALIDADES

La gestión de incidentes de seguridad de la información en la UAESP plantea una serie de etapas basadas en las recomendaciones del MinTIC, Guía 21 para la Gestión y Clasificación de Incidentes de Seguridad de la Información, la cuales son:

1. Preparación y prevención.
2. Detección y Análisis.
3. Estrategias de Tratamiento
4. Actividades Post-Incidentes

Figura 1 Etapas para la gestión de incidentes



Fuente: Adoptado Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información – MinTIC

La Oficina TIC junto con la Mesa de Servicios, será el grupo encargado de definir los procedimientos a la atención de incidentes y realizar las siguientes acciones:

- **Detección**: Monitorear y verificar elementos de control con el fin de detectar un posible incidente de seguridad de la información.

- **Atención**: Recibir y resolver los incidentes de seguridad de la información de acuerdo con el procedimiento de Gestión de Incidentes.

- **Recolección y Análisis de Incidentes de Seguridad**: Recolección de la documentación y análisis de la evidencia, cuando sea requerida.

- **Clasificar y Priorizar**: Identificar servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.

- **Anuncios de Seguridad**: Se debe informar a todos los funcionarios y contratistas sobre nuevas vulnerabilidades, actualizaciones, recomendaciones de seguridad informática y lecciones aprendidas a través de comunicaciones internas, como el correo electrónico o radicados en Orfeo.

- **Comunicaciones Internas y Externas**: Manejar las relaciones con los entes interno o externos en materia de incidentes de seguridad de la información.

Notificación de Incidentes

Todos los funcionarios y contratistas tienen la responsabilidad de realizar el reporte de cualquier evento tecnológico o incidente de seguridad que observen o experimenten.

La notificación de los incidentes permite responder a los mismos en forma sistemática, minimizar su ocurrencia, facilitar una recuperación rápida y eficiente de las actividades minimizando la pérdida de información, la interrupción de los servicios y manejar correctamente los aspectos legales que pudieran surgir durante este proceso.

5. PREPARACIÓN

El responsable de la atención de incidentes de seguridad, la Oficina TIC y la Mesa de Servicios, deben velar por la disposición de recursos, herramientas e implementación de buenas prácticas para atender las etapas de la gestión de incidentes.

A continuación, se nombrarán las actividades que buscan prevenir la ocurrencia de incidentes de seguridad de la información.

Aseguramiento de servicios y plataformas: Se deben configurar los servicios con la menor cantidad de privilegios posibles con el fin de proveer únicamente los servicios necesarios a usuarios y equipos. Para esto se cuenta con el procedimiento GTI-PC-03 Gestión de Usuarios y las políticas de seguridad definidas por la Entidad.

Seguridad en Redes: Se deben gestionar los elementos de seguridad. El Profesional Universitario / Especialista, Técnico o Contratista debe revisar y monitorear constantemente el funcionamiento de la red de comunicaciones y las reglas de los firewalls, los elementos de seguridad informática y la red de datos, sus logs deben estar sincronizados para permitir realizar una correlación de eventos y análisis respectivo.

Para esto, los servidores de la Entidad se configuran para estar sincronizados con la hora colombiana, de forma que los registros o logs, independiente del sistema, se encuentren sincronizados para su respectivo análisis de eventos cuando se requiera.

Prevención de código malicioso: Se debe garantizar que todos los equipos de la infraestructura, como servidores y equipos de usuario final, deben tener instalado el antimalware actualizado. La Oficina TIC realiza el seguimiento a la compra o renovación de licenciamiento de antivirus, adicional, se cuenta con el procedimiento PC-10 Administración de Antivirus para la gestión del software para este fin.

Sensibilización de usuarios: La Entidad con el apoyo de la Oficina TIC realizará sensibilizaciones a los usuarios finales de acuerdo con su perfil sobre las políticas,

procedimientos y recomendaciones asociadas al uso apropiado de redes, sistemas y aplicaciones en concordancia con los estándares de seguridad de la entidad.

Equipo de respuesta a incidentes (IRT)

La conformación de un equipo de respuesta a incidentes (IRT) es fundamental para una gestión efectiva de incidentes de seguridad de la información. El IRT estará compuesto por miembros clave, cada uno con roles y responsabilidades específicas. A continuación, se detallan los roles propuestos para el IRT:

Tabla 1 Roles Equipo respuesta incidentes

MIEMBRO	ROL
Líder: Jefe Oficina TIC	• Coordina las actividades del equipo de respuesta a incidentes. • Toma decisiones estratégicas y establece las prioridades. • Actúa como punto de contacto principal para la comunicación interna y externa.
Oficial de Seguridad de la Información	• Responsable de la seguridad de la información y de la gestión de incidentes. • Supervisa la implementación y el cumplimiento de las políticas de seguridad. • Participa en la coordinación y respuesta a incidentes de seguridad.
Oficial de Datos Personales	• Responsable de garantizar el cumplimiento de las regulaciones de protección de datos personales. • Colabora en la evaluación de impacto en la privacidad y en la gestión de incidentes relacionados con datos personales.
Administrador de Infraestructura	• Responsable de administrar y mantener la infraestructura tecnológica de la organización. • Participa en la identificación y mitigación de incidentes relacionados con la infraestructura.

MIEMBRO	ROL
Administrador Mesa de Servicio	• Encargado de recibir y gestionar los reportes de incidentes de los usuarios. • Coordinar y priorizar la resolución de incidentes de menor gravedad y escalado de aquellos más complejos al equipo de respuesta a incidentes.
Administradores Funcionales de Sistemas y Aplicativos	• Responsables de la administración y mantenimiento de los sistemas y aplicativos de la entidad. • Participan en la identificación y mitigación de incidentes relacionados con los sistemas y aplicativos bajo su responsabilidad.
Administrador de Base de Datos	• Responsable de administrar y mantener las bases de datos de la organización. • Participa en la identificación y respuesta a incidentes relacionados con las bases de datos.

Fuente: Elaboración propia UAESP 2023.

El nivel de participación y convocatoria del equipo de respuesta a incidentes (IRT) puede variar según la naturaleza y la criticidad del incidente. Se convocará a los miembros necesarios según sus roles y habilidades específicas.

Es importante mantener una comunicación constante y clara entre los miembros del equipo, ya sea que estén reunidos por completo o involucrados de manera progresiva, para garantizar una respuesta efectiva y evitar la duplicación de esfuerzos.

Recursos de Comunicación

Para la asignación o escalamiento de reporte de incidentes, la Mesa de Servicios debe tener la siguiente información disponible.

- Información de Contacto: Información de cada una de las personas que conforman el grupo de gestión de incidentes o quienes realicen sus funciones, información de

las autoridades y proveedores o fabricantes. Esta información se usará para el escalamiento de incidentes.

- Información de los administradores de la plataforma tecnológica.
- Contacto de la dependencia encargada de procesos disciplinarios para realizar las investigaciones que haya a lugar cuando esté involucrado un funcionario o contratista.

Recursos para el análisis de incidentes

El equipo de respuesta a incidentes de seguridad deberá contar, entre otros elementos, con:

- El diagrama de red para tener la ubicación rápida de los recursos existentes.
- Información de Servidores (Nombre, IP, Aplicaciones, Parches, Usuarios Configurados, responsable de cambios) para conocer el funcionamiento normal del mismo y realizar una identificación más acertada de un incidente.
- Información puertos utilizados por los protocolos de red, horarios de utilización, direcciones IP que generan un mayor tráfico, direcciones IP que reciben mayor número de peticiones u otros que consideren necesarios para el análisis.
- Inventario de activos de información y su clasificación.

Lo anterior se encuentra documentado en la plantilla Sistemas de Información.

Recursos para la mitigación y remediación

Se deben considerar los elementos básicos para la contención de un posible incidente, Backup de base de datos, información, imágenes de servidores, y cualquier información base que pueda recuperar el funcionamiento normal del sistema.

6. DETECCIÓN Y ANÁLISIS

Se deben establecer canales de reporte de incidentes o eventos. Teniendo en cuenta las condiciones de trabajo en casa y posibles afectaciones de los diferentes servicios, la Mesa de Servicios ha establecido tres canales para realizar el reporte de incidentes y se encuentran descritos en las actividades del Procedimiento de Gestión de incidentes; Estos son: correo electrónico, plataforma mesa de servicios y el canal telefónico.

6.1 Detección, Identificación y Gestión de Elementos Indicadores de un Incidente

Una de las principales fuentes del reporte de incidentes son los funcionarios o contratistas, siguiendo con la revisión continua de la infraestructura por parte del encargado o quien haga sus veces.

Los indicadores son los eventos que nos señalan que posiblemente un incidente ha ocurrido, generalmente algunos de estos elementos son:

- Alertas en sistemas de seguridad.
- Caídas de servidores.
- Entradas sospechosas en el registro de Windows.
- Servicios y procesos inusuales.
- Cargas excesivas en memoria o discos.
- Sesiones abiertas de manera remota.
- Archivos con permisos inusuales.
- Archivos ocultos.
- Cuentas de usuario con permisos inusuales.

- Bloqueo o lentitud prolongada en los servicios prestados.
- Ingreso no autorizado a los centros de datos de la entidad.
- Fallas en los controles ambientales en los centros de datos.0
- Tráfico de red inusual especialmente en horas no habituales.
- Informes generados por el Antivirus.
- Otros funcionamientos fuera de lo normal del sistema.

La identificación y gestión de elementos que alertan sobre un incidente nos proveen información que puede alertarnos sobre la futura ocurrencia de este y preparar procedimientos para minimizar su impacto. Algunos de estos elementos pueden ser:

- Logs de servidores.
- Logs de aplicaciones.
- Logs de herramientas de seguridad.
- Cualquier otra herramienta que permita la identificación de un incidente de seguridad.

6.2 Análisis

Las actividades de análisis de un incidente involucran los siguientes aspectos:

- Tener conocimientos de las características en funcionamiento normal a nivel de red de datos y comunicaciones y de los sistemas de información tecnológica.
- Los administradores de la infraestructura tecnológica deben tener conocimiento sobre los comportamientos de la Infraestructura que están administrando.

- Toda información que permita realizar análisis al incidente debe estar centralizada (Logs de servidores, redes, aplicaciones).

- Es importante efectuar correlación de eventos, ya que por medio de este proceso se pueden descubrir patrones de comportamiento anormal y poder identificar de manera más fácil la causa del incidente.

- Tener documentado la información de los servicios habilitados y las experiencias con incidentes anteriores.

- Crear matrices de diagnóstico que faciliten identificar similitudes en incidentes.

6.2.1 Categorización

Cuando el reporte sea clasificado como tipo "Incidente de Seguridad de la Información", quien realice la gestión o el seguimiento en la herramienta de la Mesa de servicios y de acuerdo con el procedimiento de gestión de Incidentes, deberá categorizar el tipo incidente de acuerdo con la siguiente tabla:

TIPOS DE INCIDENTES	DESCRIPCIÓN
Malware o software malicioso	Presencia, uso, adquisición, envió, introducción de software malicioso u otros programas dañinos que tienen la intención de realizar actividades prohibidas como robo, alteración, destrucción o captura de información y recursos.
Phishing	Intento o substracción no autorizada de información sin autorización o consentimiento del propietario o custodio, a partir de la sustitución de la identidad o mediante el uso de técnicas de ingeniera social.
Ataque DDoS	Ataque, intento de ataque o cualquier conducta ilegal, no ética o no autorizada que involucra la obstrucción de las actividades de la Entidad

TIPOS DE INCIDENTES	DESCRIPCIÓN
	mediante la interrupción de un recurso de red o servicios de la UAESP.
Violación de datos personales	Toda violación de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
Acceso abusivo o no autorizado	Acción en la que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático, incluyendo bases de datos, servicios o áreas físicas, protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.
Indisponibilidad de servicios	Afectación a los servicios o aplicativos por eventos relacionados con los recursos de la Entidad.
Siniestro o Desastre Natural	Eventos causados por fenómenos naturales.

Fuente: Elaboración propia UAESP 2023.

6.2.1 Evaluación de Incidentes

Los incidentes reportados se deben evaluar con el fin de permitir una atención adecuada según la necesidad.

Para determinar el nivel de prioridad, se deben evaluar los incidentes teniendo en cuenta el impacto que ocasiona y los insumos entregados por el análisis de riesgos y la clasificación de activos de información de la entidad. La siguiente tabla muestra la clasificación de los incidentes.

Tabla 2 Clasificación por niveles de Impacto

Impacto	Descripción del impacto
Muy Grave	*Afectación a sistemas y activos de información críticos que sostienen servicios misionales*: Interrumpe en gran parte la operación de la entidad, el incidente ocasiona daños de activos. Podría llegar a afectar más de un tipo de activo. Pueden comprometer los objetivos misionales de la Entidad, involucra aspectos legales y sanciones de entes externos de control, afectación a la imagen de la Entidad a nivel nacional e internacional o pérdidas económicas catastróficas.
Grave	*Afectación a sistemas y activos de información que pertenecen a la Oficina TIC y apoyan a más de una dependencia o proceso de la entidad:* Interrumpe en corto tiempo un objetivo determinado de la entidad. Compromete un activo importante. Pueden involucrar aspectos legales y sanciones de entes externos de control, afectación a la imagen de la Entidad a nivel nacional, daño severo a la infraestructura y pérdidas económicas moderadas.
Menos Grave	*Afectación a sistemas y activos de información que apoyan a una sola dependencia*: No interrumpe los procesos generales de la entidad. Se detecta y se puede controlar fácilmente con recursos existentes en la entidad. Afecta un activo de información de valoración baja. Puede afectar la imagen de la Entidad a nivel interno, sanciones a nivel de Oficina de Control Interno o Subdirección de Asuntos Legales, daños parciales o mínimo a la infraestructura, pérdidas económicas mínimas.
Menor	*Afectación a sistemas o activos de información que apoyan a funcionarios con funciones no críticas*: No interrumpe los procesos generales de la entidad. Puede afectar la imagen a nivel de proceso o área, daño mínimo a la infraestructura o llamados a nivel

Impacto	Descripción del impacto
	de grupos de trabajo.

Fuente: Elaboración propia UAESP 2023.

6.2.1 Priorización y tiempos de respuesta.

Para el caso de la atención de incidentes de seguridad se han establecido unos tiempos límites para dar respuesta al incidente según la prioridad de este.

Tabla 3 Priorización - tiempos de respuesta

Nivel de Prioridad	Impacto del incidente	Restablecimiento a la Operación Normal.
Alta	Muy Grave	6 horas
Media	Grave	10 horas
Baja	Menos Grave	16 horas
	Menor	

Fuente: Elaboración propia UAESP 2023.

7. ESTRATEGIAS DE TRATAMIENTO

Es importante implementar una estrategia que permita tomar decisiones oportunamente para evitar la propagación del incidente y así mitigar los daños a los recursos tecnológicos y la pérdida de la confidencialidad, integridad y disponibilidad de la información.

Esta fase contempla las siguientes estrategias:

Contención: Esta actividad proporciona tiempo para desarrollar o aplicar una estrategia a medida, buscando que no se propague el incidente o amenaza y pueda generar más daños a la información o a la arquitectura de TI.

Erradicación: Después contener el incidente, puede ser necesario erradicarlo o eliminar cualquier rastro para solventar afectaciones a la seguridad de la información. También sirve para identificar y mitigar las vulnerabilidades que hayan sido explotadas.

Recuperación: El propósito de la esta estrategia es el restablecimiento del servicio a su operación normal.

Se procede a la recuperación a través de la restauración de los sistemas o servicios afectados para lo cual se debe evitar, en la medida de lo posible, que suceda nuevamente el incidente por la misma causa.

El Oficial de Seguridad conformará el grupo de atención a cada incidente con el personal que sea necesario o apropiado para dar respuesta y realizar las acciones necesarias para contener, erradicar o recuperar.

7.3 Plan de Respuesta a Malware – Endpoint

Tabla 4 Plan de respuesta a malware-endpoint

No	ACTIVIDADES	RESPONSABLE
	CONTENCIÓN	
1	Identificación mediante una alerta emitida por la herramienta antimalware, por comportamientos sospechosos en el equipo asignado, por mensajes de ventanas emergentes, por abrir aplicaciones de dudoso origen o por alguna duda razonable que indique su equipo este infectado, de manera inmediata notificar a la mesa de servicios por los siguientes canales. ▪ Correo: mesa.servicios@uaesp.gov.co ▪ Teléfono: 601 3580400 Extensión 911 ▪ Aplicación mesa de servicios	Usuario final / soporte técnico / mesa de servicios Correo electrónico, apertura de caso
2	Verificación del estado de las actualizaciones del	

No	ACTIVIDADES	RESPONSABLE
	sistema operativo al día y la no instalación de programas no permitidos en el equipo del usuario final.	Soporte técnico / mesa de servicios
3	Verificación del estado de la instalación, correcta conexión con la consola central y actualizaciones de las firmas del agente antimalware en el equipo de usuario final.	
4	Verificación de los logs del agente antimalware en la máquina del usuario final.	
5	Identificación de la infección tipo malware, spyware, gusano, virus, ransomware, etc., en el equipo de usuario final.	
6	Localizar y aislar el equipo de usuario comprometido por la infección malware.	
7	Informar el incidente de seguridad al administrador de la infraestructura del antimalware de la entidad.	Soporte técnico / mesa de sevicios
8	Informar el incidente de seguridad al oficial de seguridad de la información de la entidad.	Administrador antimalware entidad
ERRADICACIÓN		
9	Instalación de parches de seguridad del sistema operativo y aplicaciones permitidas en el equipo de usuario final.	Soporte técnico / mesa de servicios
10	Desinstalación de las aplicaciones no permitidas en los equipos de usuario final.	Soporte técnico / mesa de servicios
11	Ejecución de la herramienta antimalware actualizada en firmas a la fecha en la estación del usuario final comprometido.	Soporte técnico / mesa de servicios
12	Generación del informe del resultado de la desinfección realizada en el equipo de usuario final.	Soporte técnico / mesa de servicios

No	ACTIVIDADES	RESPONSABLE
13	Revisión, evaluación del informe enviado por mesa de servicios o soporte técnico sobre el estado de la actividad de desinfección desarrollada en el equipo de usuario final para ser enviado a seguridad de la información.	Administrador antimalware entidad (informe)
14	Si se ha identificado al responsable, con intencionalidad, contactar con las autoridades de ciberseguridad o en caso de ser un ataque interno, reportarlo a la Oficina de Control Disciplinario Interno.	Oficial de Seguridad de la información
RECUPERACIÓN		
15	Generar autorización para dar de alta el equipo de usuario final que estuvo infectado con el malware una vez solucionado el incidente.	Oficial de Seguridad de la información
16	Restablecimiento del servicio del equipo recuperado de la amenaza malware.	Soporte técnico / mesa de servicios
17	Elaborar plan de acción para evitar que se presente de nuevo el incidente (base de conocimiento).	Administrador antimalware entidad. Oficial de Seguridad de la información
18	Documentar las lecciones aprendidas en la bitácora de gestión de incidentes.	Oficial de Seguridad de la información
19	Generación del informe final del incidente de seguridad presentado.	Oficial de Seguridad de la información
20	Cerrar caso mesa de servicios / soporte técnico	Soporte técnico / mesa de servicios Administrador antimalware entidad. Oficial de Seguridad

No	ACTIVIDADES	RESPONSABLE
		de la información

Fuente: Elaboración propia UAESP 2023.

7.4 Plan de Respuesta Malware – Servidores

Tabla 5 Plan de respuesta malware-servidores

No	ACTIVIDADES	RESPONSABLE
CONTENCIÓN		
1	Verificar en la plataforma del software antimalware a nivel de servidores el tipo de amenaza detectada o notificada del servidor o servidores afectados.	Administrador de infraestructura
2	Revisar documentación existente del malware detectado y bloquear los puertos o medios de comunicación por los que se propaga o actúa, de tal forma que se bloquee el malware sin afectar los servicios del servidor afectado.	Administrador de infraestructura
ERRADICACIÓN		
3	Escanear el servidor o servidores para eliminar el malware.	Administrador de infraestructura
4	Revisar los logs de la consola del antimalware para verificar que el proceso de eliminación haya sido exitoso.	Administrador de infraestructura
RECUPERACIÓN		
5	Verificar la actualización de la base de datos del agente antimalware y los endpoint, y asegurar que están recibiendo las políticas desde las consolas de administración.	Administrador de infraestructura
6	Revisar y actualizar, de ser necesario, los parches de seguridad del servidor o servidores.	Administrador de infraestructura
7	Informar el incidente de seguridad al oficial de seguridad	Administrador de

No	ACTIVIDADES	RESPONSABLE
	de la información de la entidad.	infraestructura
8	Restaurar las copias de seguridad o respaldo, en caso de ser necesario, siguiendo el procedimiento GTI-PC-11 Gestión de Respaldos.	Administrador de infraestructura

Fuente: Elaboración propia UAESP 2023.

7.5 Plan de Respuesta a phishing

Tabla 6 Plan de respuesta a phishing

No	ACTIVIDADES	RESPONSABLE
CONTENCIÓN		
1	Bloquear las direcciones IP y cuentas que envían el correo de phishing.	Administrador de infraestructura / Administrador Office 365
2	Bloquear direcciones IP y cuentas de donde se envía el correo de phishing (Firewall, y cualquier dispositivo de detección de intrusos), cuando aplique.	
3	Si aplica, enviar boletín informativo o advertencia de posible suplantación en el sitio web, intranet, o fondo de escritorio de los equipos conectados al dominio de la Entidad.	
4	Identificar otros posibles hosts afectados.	
ERRADICACIÓN		
4	Si el correo electrónico posee alguna URL, realizar el bloqueo y cualquier otro elemento relacionado	Administrador de infraestructura / Administrador Office 365
5	Borrar el correo de la bandeja de entrada del usuario	
RECUPERACIÓN		
6	Revisar que la dirección suplantada o fraudulenta fue	Oficial de Seguridad

No	ACTIVIDADES	RESPONSABLE
	inhabilitada.	de la información
7	En caso de detectar una página fraudulente, mantenerla en observación y seguimiento para reportar su baja	Administrador de infraestructura / Web Master
8	Retirar advertencia o boletines informativos de los sitios web, intranet o fondo de escritorios de los equipos de cómputo conectados al dominio de la Entidad.	Administrador de infraestructura / Web Master

Fuente: Elaboración propia UAESP 2023.

7.6 Plan de Respuesta a DDoS

Tabla 7 Plan de respuesta a DDoS

No	ACTIVIDADES	RESPONSABLE
CONTENCIÓN		
1	Analizar el tipo de ataque DDoS, su objetivo, el flujo y componentes de infraestructura asociados.	Administrador de infraestructura / Web Master Administrador de infraestructura
2	Desactivar las características afectadas de forma temporal.	
3	Aplicar bloqueos por medio de los dispositivos de seguridad perimetral.	
4	Bloqueo direcciones IP comprometidas. Configure DNS alternos y canales de comunicación alterno (Servidores – Dirección IP)	
ERRADICACIÓN		
5	Contactar con el ISP, informar del ataque y solicitar aplicar medidas correctivas desde su infraestructura.	Administrador de infraestructura
6	Si se ha identificado al responsable, contactar con las	Oficial de Seguridad

No	ACTIVIDADES	RESPONSABLE
	autoridades de ciberseguridad o en caso de ser un ataque interno, reportarlo a la Oficina de Control Disciplinario Interno.	de la información
7	De ser necesario, ajustar las reglas del firewall.	Administrador de infraestructura o responsable
RECUPERACIÓN		
8	Monitorear y verificar que el ataque DDoS haya finalizado o que las medidas de contención y erradicación fueron efectiva, caso contrario volver a la actividad No. 1.	Oficial de Seguridad de la información
9.	Subir o restituir los servicios desactivados temporalmente o afectados.	Administrador de infraestructura / Web Master
10.	Documentar las lecciones aprendidas en la bitácora de gestión de incidentes.	Oficial de Seguridad de la información

Fuente: Elaboración propia UAESP 2023.

7.7 Plan de Respuesta a Violación de Datos Personales

Tabla 8 Plan de respuesta a violación de datos personales

No	ACTIVIDADES	RESPONSABLE
CONTENCIÓN		
1	A fin de contener la brecha, evento o Incidente de Seguridad, el Oficial de Datos Personales deberá: - Recuperar el control de los datos afectados o neutralizar al máximo el impacto. - Limitar cualquier daño que pueda ocasionar la	Oficial de protección de datos personales

No	ACTIVIDADES	RESPONSABLE
	Brecha de Seguridad a la Entidad o a los interesados afectados. - En su caso, tratar de recuperar la posesión de los equipos físicos o documentos que contengan los datos personales que se han visto afectados.	
2	Realiza una investigación inicial sobre el evento u ocurrencia.	Oficial de protección de datos personales
3	Evaluar los riesgos e impactos asociados con el incidente	Oficial de protección de datos personales
4	Identificar los daños para las personas y organizaciones involucradas en el incidente.	Oficial de protección de datos personales
ERRADICACIÓN		
5	Eliminar o anonimizar los datos expuestos, en caso de ser por información publicada por la Entidad, subsanando la vulnerabilidad de los datos personales privados o sensibles.	Oficial de protección de datos personales en conjunto con los procesos correspondientes
6	Notificar a la Superintendencia de Industria y Comercio, de acuerdo con la normativa legal vigente y la política de tratamiento de datos personales de la UAESP.	Oficial de protección de datos personales
7	Comunicar a los titulares de la información, cuando corresponda, de acuerdo con la política de tratamiento de datos personales.	Oficial de protección de datos personales
RECUPERACIÓN		
8	Documentar las lecciones aprendidas y el resultado de la investigación del paso 2, que lleven a mejorar los controles internos, los programas de capacitación o	Oficial de protección de datos personales

No	ACTIVIDADES	RESPONSABLE
	cualquier control operativo técnicos y permitan evitar futuros incidentes de seguridad	

Fuente: Elaboración propia UAESP 2023.

7.8 Plan de Respuesta Acceso Abusivo o no Autorizado

Tabla 9 Plan de respuesta a acceso abusivo o no autorizado

No	ACTIVIDADES	RESPONSABLE
	CONTENCIÓN	
1.	Reconocer y confirmar la existencia de un acceso no autorizado, ya sea lógico o físico.	Administradores funcionales Administrador de base de datos Administrador de infraestructura Administrador de plataformas Responsable de áreas o seguridad física
2.	Bloquear o cancelar el acceso a los aplicativos, dispositivos, sistemas de información o servicios de red del usuario afectado. De ser necesario, aislar y contener el incidente, desconectando o bloqueando los sistemas, dispositivos o áreas físicas afectadas. En caso de tratarse de un acceso físico, retirar del sitio con servicios del personal de vigilancia.	
3.	Documentar y preservar las pruebas relevantes del incidente, como registros de acceso, registros de actividad y cualquier otro tipo de evidencia digital o física.	
	ERRADICACIÓN	
4.	Investigar para determinar el alcance y la causa raíz del acceso no autorizado, identificando las vulnerabilidades o brechas que permitieron el incidente.	Soporte técnico / mesa de servicios / Personal de

No	ACTIVIDADES	RESPONSABLE
		Seguridad de la Entidad/ Responsable del Activos Involucrados
5.	Restringir y controlar la asignación y uso de derechos de acceso privilegiado tanto físico como lógico.	Administradores funcionales/ Personal de Seguridad de la Entidad/ Responsable del Activos Involucrados
6.	Aplicar parches de seguridad, actualizaciones de software y realizar cambios en la configuración para cerrar las brechas y fortalecer las medidas de seguridad.	Administradores funcionales y de plataformas. Administrador de Infraestructura
RECUPERACIÓN		
7.	Restablecer los accesos a sistemas, dispositivos o áreas afectadas a su estado normal de operación, verificando su adecuado funcionamiento.	Administradores funcionales y de plataformas. Administrador de Infraestructura
8.	Realizar una revisión post-incidente para identificar las lecciones aprendidas, mejorar los controles de seguridad existentes y actualizar las políticas y procedimientos para evitar futuros incidentes similares.	Oficial de Seguridad de la información

No	ACTIVIDADES	RESPONSABLE
9.	Notificar a las autoridades competentes, clientes, proveedores u otras partes afectadas, cuando aplique.	Jefe de la Oficina TIC Oficial de Seguridad de la información
10.	Generación del informe final del incidente de seguridad presentado.	Oficial de Seguridad de la información

Fuente: Elaboración propia UAESP 2023.

7.9 Plan de respuesta por indisponibilidad de los servicios.

Activar el procedimiento GTI-PC-05 Soporte de mesa de servicio.

7.10 Plan de respuesta por siniestro o desastre natural

En caso de desastre natural, la prioridad debe ser la seguridad y el bienestar de las personas involucradas. Una vez garantizada esa seguridad, se deberá seguir lo establecido en el Plan de Continuidad del Negocio -BCP-.

8. METODOLOGÍA PARA LA RECOLECCIÓN DE EVIDENCIAS DIGITALES

Además de elegir la estrategia de tratamiento de acuerdo con el daño potencial, tiempo y recursos, disponibilidad del servicio y efectividad de la solución, es importante llevar a cabo una correcta identificación, recolección, análisis y manipulación de datos en caso de materializarse un incidente de seguridad de la información que requiera evidencias digitales para su investigación.

En caso de que la Entidad no cuente con los recursos necesarios para la recolección y análisis de evidencias, como herramientas forenses, se recomienda solicitar apoyo, asesoramiento o instrucciones al CSIRT Gobierno o CCP (Equipo de Respuesta a Incidentes de Seguridad del Gobierno o Centro de Coordinación de Respuesta a Incidentes) para esta etapa del proceso de evidencias digitales. Es fundamental asegurar

la escena del incidente hasta obtener el apoyo del CSIRT Gobierno o CCP y seguir sus recomendaciones.

8.1 Confirmación

Es importante establecer si ha ocurrido o no un incidente que afecte la seguridad de los activos de información de la Entidad.

Una vez confirmada la existencia o materialización de un incidente de seguridad de la información se debe definir si se requiere recolectar evidencia digital para su respectiva investigación o judicialización ante la autoridad competente. Para esto se debe seguir los siguientes criterios, de acuerdo con el impacto del incidente:

Tabla 10 Criterios para recolección de evidencia digital

CRITERIO DE IMPACTO	REQUIERE EVIDENCIA DIGITAL	NO REQUIERE EVIDENCIA DIGITAL
Muy Grave / Grave	X (Cuando se requiera un proceso de judicialización)	
Menos Grave / Menor		X

Fuente: Elaboración propia UAESP 2023.

8.2 Aislamiento de la escena

Una vez identificado el incidente de seguridad de la información se debe asegurar la escena, es decir, restringir el acceso a la zona donde se produjo el incidente con el fin de evitar cualquier contaminación o manipulación accidental o deliberada de evidencia.

Para aislar la escena, en primera instancia informe y coordine con el CSIRT Gobierno o CCP y, si es posible, el oficial de seguridad de la información o el líder del equipo IRT deberá:

a) Tomar fotografías del equipo o sitio del incidente antes de tener contacto directo con los elementos involucrados.

b) Establecer un perímetro de seguridad con una cinta de peligro o cuerda que permita delimitar la zona para que nadie se acerque, si es necesario solicitar el apoyo del personal de seguridad física o personal de vigilancia.

c) Si los equipos se encuentran encendidos, no los apague. Asegúrese de mantener encendido los equipos involucrados, adicional:

   I. Sellar con cinta cualquier puerto USB, firewire, Unidades lectoras ópticas y cualquier otro que pueda alterar la evidencia.

   II. Realizar un registro fotográfico de lo que se ve en pantalla.

d) Si los equipos se encuentran apagados, no los encienda.

e) Listar los dispositivos (periféricos, unidades de almacenamiento, networking, seguridad perimetral, cámaras de seguridad, entre otros) que tuvieron contacto o interacción con los equipos involucrados en el incidente.

f) Llevar bolsas sellables, cajas de cartón, rótulos o etiquetas, elementos para realizar backup, entre otros.

g) Use guantes de látex o quirúrgicos para minimizar el riesgo de contaminar la escena.

8.3 Custodia

Es importante garantizar la autenticidad e integridad de las evidencias encontradas, es decir, que lo mismo que se encontró en la escena, es lo mismo que se está presentando a la autoridad competente o comité disciplinario, si aplica.

Para esto se debe contar mínimo con la siguiente información:

a) Almacene cualquier información original en un sitio con acceso restringido, para garantizar la cadena de custodia de la información.

b) Una hoja de ruta, donde se anotarán los datos principales para describir la evidencia, fechas, horas, custodio, identificaciones, testigos, cargos y firmas de quien recibe y entrega.

c) Para mantener la cadena de custodia se debe diligenciar recibos personales que guarda cada custodio y donde están datos similares a los de la hoja de ruta.

d) Rótulos o etiquetas diligenciadas antes de ser pegadas a los empaques de las evidencias (bolsas, cajas, sobre papel o manila, entre otros)

Es importante registrar en la hoja de ruta y recibos personales cada acción tomada desde que se recolecta, almacena, se guarda, quien lo hace y la hora exacta, que herramientas se han utilizado para la recolección, entre otras, en especial si la evidencia va a utilizarse para fines legales.

8.4 Identificación de fuentes de información

Se debe identificar fuentes potenciales de información de donde se puedan extraer datos para el proceso de evidencias.

Las fuentes más comunes son:

- Computadores
- Servidores
- Dispositivos de almacenamiento en red y en la nube.
- Medios internos y externos como: Dispositivos USB, Firewire, DC/DVD, PCMI, Discos ópticos y Magnéticos, Discos Duros Extraíbles, Memorias SD y MicroSD, entre otros.

- Dispositivos móviles como celulares, tablets, PDA's, Cámaras digitales o grabadoras de video y audio.
- Logs o registros de dispositivos de networking o seguridad perimetral.
- Logs o registros de aplicaciones o sistemas de información.
- Logs o registros de proveedores de servicio, cuando sea posible.

8.5 Recolección y Análisis de Evidencias

Una vez obtenido el apoyo de las autoridades competentes, proporcione los detalles pertinentes sobre el incidente, la naturaleza de la evidencia y cualquier información adicional que pueda ser relevante para una respuesta efectiva. Mantener la integridad de la evidencia y seguir las instrucciones del equipo especializado ayudará a garantizar la calidad y la validez de las pruebas recopiladas.

Si existen los recursos de la Entidad así lo permiten y el equipo IRT tiene los conocimientos y habilidades necesarios, es importante realizar una copia de la memoria volátil o RAM si el computador o equipo se encuentra encendido y siga los lineamientos del Anexo 1 Guía No. 13 del MinTIC Evidencia Digital, para la recolección de evidencias de acuerdo con el listado de posibles fuentes y las herramientas disponibles en la Entidad.

En todos los casos, es necesario crear y mantener un registro de hallazgos, ya sea en formato físico o electrónico, conocido como Bitácora. Esta Bitácora debe contener un historial detallado de todas las actividades realizadas durante el proceso de gestión de incidentes, así como los hallazgos encontrados. Su objetivo principal es permitir la reconstrucción del caso en cualquier momento, proporcionando una visión completa de las acciones tomadas y los resultados obtenidos

9 ACTIVIDADES POST-INCIDENTES

Las actividades Post-Incidente se componen de:

a) **Informe del Incidente**: Después que el servicio ha sido reestablecido debe prepararse un informe del evento tecnológico o incidente de seguridad de la información que indique lo que paso, como se resolvió, elementos implicados, el tiempo que demoro la solución y el tiempo sin servicio.

La Herramienta Mesa de servicios no cuenta con un campo específico para declarar la información antes mencionada, por lo que podrá realizarse dentro del campo observaciones o adjuntarse como documento cuando sea posible.

Adicional se deberá llenar la bitácora de incidentes de seguridad de la información que contenga la descripción de las actividades desarrolladas en la gestión de estos y el número de ticket o identificación del incidente gestionado.

b) **Lecciones aprendidas**: Con el objetivo de mejorar la toma de decisiones en futuros incidentes, mejorar los procesos y procedimientos, identificar fortalezas o debilidades, el responsable de la atención de incidentes de seguridad con el equipo o grupo de personas encargadas de la respuesta a incidentes debe documentar el conocimiento o entendimiento sobre la experiencia del análisis y tratamiento de incidentes de seguridad de la información. No solo se debe documentar las experiencias positivas, también las deficiencias en las acciones implementadas para mejorar en el futuro, esto permite conocer:

- 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.

c) **Establecimiento de medidas disciplinarias y penales de ser necesarias**:

De ser necesario se debe comunicar a las entidades competentes.

- Cuando el incidente de seguridad de la información sea evaluado con un impacto Muy Grave o Grave se deberá reportar ante el CSIRT Gobierno a través de los canales dispuesto por este, para su apoyo y coordinación en la gestión del incidente.

- Los incidentes catalogados como Menos Grave y Menor se comunicarán al CSIRT Gobierno a través de los canales dispuesto por este, una vez sean gestionados, con el fin de llevar una estadística de incidentes y conocer la tipología de estos.

- Cuando se tenga evidencia de un incidente informático la UAESP se podrá contactar con el CAI Virtual de la Policía Nacional o el Centro Cibernético Policial de la Policía Nacional a través de los canales dispuesto para ello, para recibir asesoría del caso en particular y posterior judicialización.

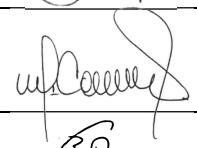
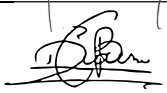
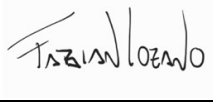
d) **Registro de los indicadores**: Es importante registrar y actualizar los indicadores de gestión de incidentes.

10 CONTROL DE CAMBIOS:

Versión	Fecha	Descripción de la modificación
1	06/08/2021	Creación del documento.
2	10/07/2023	Se ajusta el nombre del instructivo, de “Respuesta de incidentes de seguridad de la información” a

Versión	Fecha	Descripción de la modificación
		"Tratamiento de incidentes de seguridad de la información". Se ajusta la clasificación de los incidentes, se incluye el plan de respuesta a los tipos de incidentes definidos y se definen los roles y responsabilidades del equipo de respuesta interna a incidentes de seguridad de la información.

11 AUTORIZACIONES:

	NOMBRE	CARGO	FIRMA
Elaboró	Juan Sebastián Perdomo Méndez	Profesional Universitario OTIC	
	Maria Consuelo Torres Pinto	Contratista - OTIC	
	Daniel Contreras Bolaños	Contratista - OTIC	
	Fabian Andres Lozano Aguilar	Contratista - OTIC	
Revisó	Cesar Mauricio Beltrán López	Jefe Oficina de Tecnologías de Información y las Comunicaciones	
	Luz Mary Palacios Castillo	Profesional Universitario - Oficina Asesora de Planeación	
Aprobó	Yesly Alexandra Roa Mendoza	Jefe Oficina Asesora de Planeación	Alexandra Roa Mendoza Firmado digitalmente por Alexandra Roa Mendoza Fecha: 2023.07.07 19:05:11 -05'00'