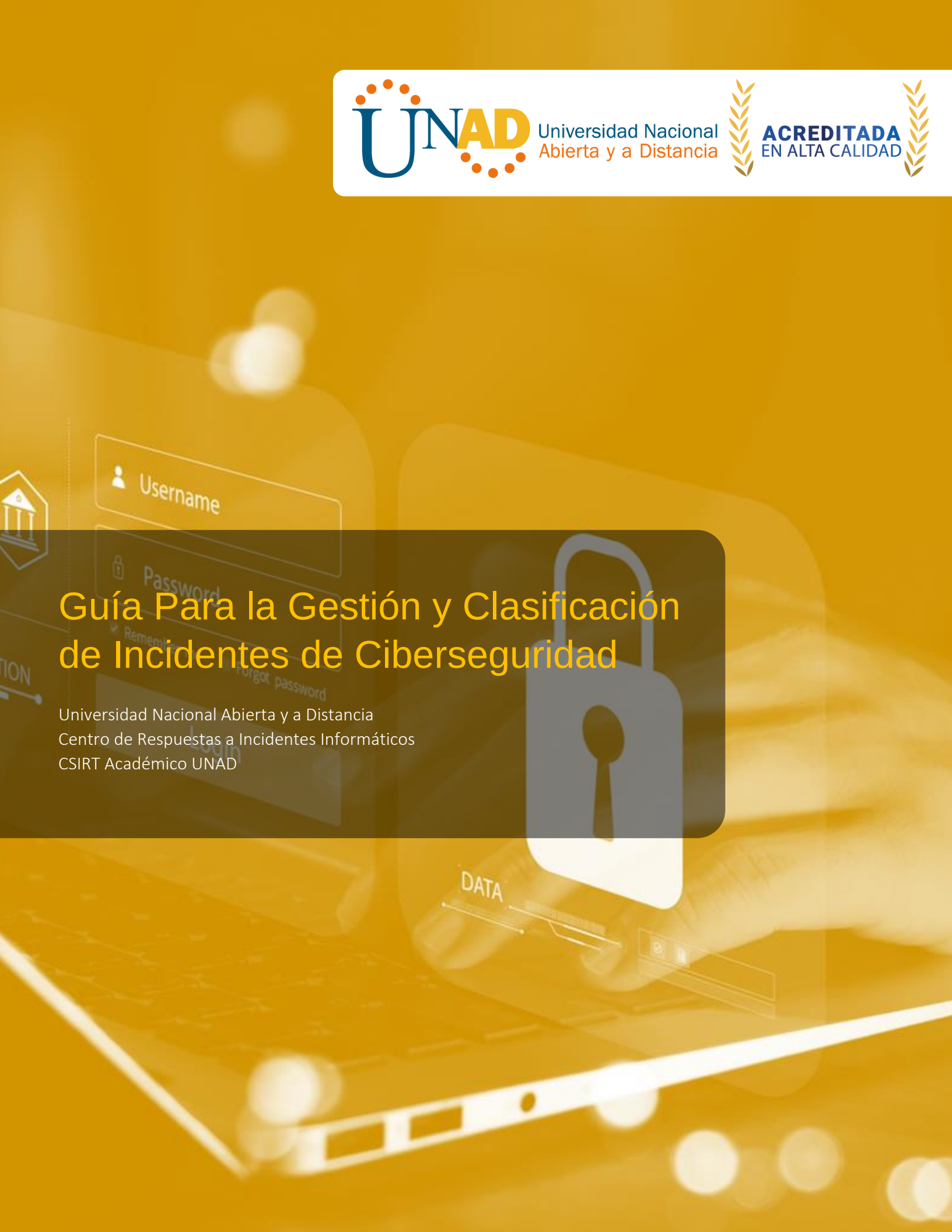


Guía Para la Gestión y Clasificación de Incidentes de Ciberseguridad

Universidad Nacional Abierta y a Distancia
Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Universidad Nacional Abierta y a Distancia
(UNAD)

Vicerrectoría de Innovación y Emprendimiento - VIEM
Ing. Andrés Ernesto Salinas
Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería - ECBTI
Ing. Claudio Camilo González Clavijo
Decano

Especialización en Seguridad Informática - ESI
Ing. Sonia Ximena Moreno Molano
Líder de Programa

Modelo de Seguridad
y Privacidad de la Información

Grupo de Investigación Byte InDesign
Semillero de Investigación Ceros y Unos

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD
Luis Fernando Zambrano Hernández
Líder

Licencia Atribución – Compartir

Libardo Cárdenas Corral
Analista 3

Hernando Peña Hidalgo
Analista 2

Néstor Raúl Cárdenas
Analista 3

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Versión	Observaciones
Versión 1.0 - 17/06/2024	Guía para la Gestión y Clasificación de Incidentes de Seguridad. Universidad Nacional Abierta y a Distancia - UNAD

La gestión de incidentes de ciberseguridad es un componente fundamental para garantizar la protección de los activos y la continuidad de las operaciones. Con base en las normas ISO/IEC 27035, 27001, la Guía 21 del Ministerio de Tecnologías de la Información y Comunicación de Colombia y el Marco NIST SP 800-61r2, se destacan varios aspectos que resaltan la importancia de una gestión eficaz respecto a un incidente de ciberseguridad. En este sentido, la gestión de un incidente permite identificar y responder de manera oportuna a amenazas e incidentes que se puedan presentar, dado que la detección temprana y la respuesta adecuada son fundamentales para minimizar el impacto de estos, mitigar sus consecuencias y evitar la propagación del ataque en nuestra infraestructura.

Establecer un proceso formal y estructurado para la gestión de incidentes promueve la colaboración y la comunicación efectiva entre las diferentes unidades de nuestro Metasistema. Esto, sin duda alguna, facilita la toma de decisión rápida, eficiente y oportuna durante un incidente y minimiza el tiempo de inactividad y los impactos operativos.

Este documento está dirigido a directivos, administrativos, líderes de procesos, estudiantes, docentes y en general a toda la comunidad UNADISTA la cual día a día trabaja en pro de la construcción de un entorno digital más seguro.

Contenido

Marco Legal, Normatividad y Estándares

Para la construcción del marco de juicio y legal del Modelo de Seguridad y Privacidad UNADISTA, se tiene presente:

Marco Legal

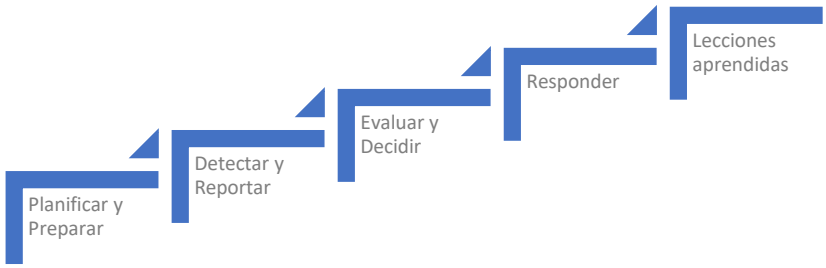
Tabla 1: Normatividad que se debe tener presente para la implementación del MSPI en la UNAD

Constitución Política de Colombia: Artículos 15, 209 y 269	
Leyes	
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1273 de 2009	Por medio de esta Ley se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "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, entre otras disposiciones
RESOLUCIÓN No. 007298 DE 10 DE MAYO DE 2023	
CONPES	
CONPES 3854 de 2016	Política Nacional de Seguridad digital
Estándares	
Modelo de Seguridad y Privacidad de la Información - MSPI	
ISO/IEC 27001:2013	Seguridad de la Información
ISO/IEC 27035	Gestión de Incidentes de Seguridad
Guía 21 MINTIC	Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información

Contexto de la Gestión de Incidentes de Seguridad

ISO 27035

La norma ISO/IEC 27035 de Gestión de Incidentes de Seguridad[1] plantea cinco etapas para la gestión de incidentes de Seguridad:



Elaboración propia

Planificar y preparar: En esta etapa, una organización se prepara para gestionar incidentes de seguridad a través de la planificación y la preparación. Los aspectos clave incluyen:

- Desarrollo de políticas y procedimientos
- Formación y concienciación
- Establecimiento de un equipo de respuesta
- Preparación de herramientas y tecnologías

Detectar y Reportar: Esta fase se centra en la identificación y el reporte de incidentes de seguridad. Las actividades incluyen:

- Monitoreo continuo
- Recolección de información
- Notificación rápida

Evaluar y Decidir: En esta etapa una organización evalúa el incidente para determinar su naturaleza y decidir la respuesta adecuada. Los elementos por considerar son:

- Evaluación del impacto
- Clasificación del incidente
- Decisión de la respuesta incluyendo la activación de planes de contingencia y comunicación con las partes interesadas

---

1 https://repository.udistrital.edu.co/bitstream/handle/11349/7273/BocanegraDiazFabianEnrique2015.pdf;jsessionid=53311F646010F67DF7561D32F39B6165?sequence=1 (Pág. 25)

Responder: La etapa de respuesta implica la implementación de acciones para manejar y mitigar el impacto del incidente. A partir de:

- Contención
- Erradicación
- Recuperación

Lecciones Aprendidas: Después de que el incidente ha sido resuelto, la organización debe analizar lo ocurrido para mejorar sus procesos. Las acciones en esta fase incluyen:

- Revisión post-incidente
- Identificación de mejoras
- Actualización de la documentación
- Capacitación y concienciación continua

Marco de Trabajo NIST

Por su parte, el marco de trabajo NIST 800 propone cinco funciones. "*Estas cinco funciones fueron seleccionadas porque representan los cinco pilares principales para un programa de ciberseguridad exitoso y holístico. Ayudan a las organizaciones a expresar fácilmente su gestión del riesgo de ciberseguridad a un alto nivel y posibilitan decisiones de gestión de riesgos*"[2]

Ilustración 1: Marco de Trabajo NIST

Recuperado de: https://www.nist.gov/news-events/news/2023/08/nist-drafts-major-update-its-widely-used-cybersecurity-framework

[2] https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf (Pág. 5)

Funciones del Marco de Trabajo NIST CSF

Identificar: Tiene como objetivo comprender el contexto organizacional para gestionar el riesgo de ciberseguridad y enfocar los recursos de manera efectiva. En el ejercicio de la identificación se debe considerar:

- Inventariar los activos físicos y virtuales.
- Evaluar el riesgo de ciberseguridad asociado con los activos, datos y capacidades.
- Establecer políticas y procedimientos que definan claramente las responsabilidades y procesos para la gestión de la ciberseguridad.
- Identificar el entorno de riesgo y las relaciones externas que podrían afectar a la ciberseguridad.

Proteger: Tiene como objetivo implementar medidas de salvaguarda para garantizar [D] Disponibilidad, [I] Integridad y [C] Confidencialidad de los servicios críticos y proteger los activos. En esta fase, se debe considerar:

- Limitar el acceso a recursos y sistemas.
- Educar al personal sobre las políticas y procedimientos de seguridad.
- Implementar medidas para asegurar la integridad y privacidad de la información.
- Establecer procedimientos operativos de seguridad para proteger los sistemas y activos.
- Asegurar que la infraestructura y los sistemas tecnológicos sean seguros y gestionados adecuadamente.

Detectar: Tiene como objetivo implementar las actividades necesarias para identificar la ocurrencia de eventos de ciberseguridad de manera oportuna. Aquí se debe tener en cuneta:

- Supervisar los sistemas y redes en busca de anomalías y actividades no autorizadas.
- Establecer procesos para identificar y registrar eventos de ciberseguridad.
- Evaluar la información de los eventos para determinar la naturaleza y el impacto del incidente.

Responder: Tiene como objetivo implementar las actividades necesarias para responder a los incidentes de ciberseguridad y mitigar sus efectos. Por lo tanto, es preciso:

- Desarrollar y mantener planes de respuesta a incidentes.
- Coordinar la comunicación interna y externa durante y después de un incidente.
- Realizar análisis post-incidente para mejorar la respuesta futura.
- Contener y erradicar el incidente para minimizar el daño.
- Aprender de los incidentes y actualizar los planes y procedimientos en consecuencia.

Recuperar: Tiene como objetivo desarrollar y ejecutar actividades para restaurar las capacidades o servicios que se vieron afectados por incidentes de ciberseguridad. Las acciones por realizar pueden ser:

- Establecer y ejecutar estrategias y planes de recuperación.
- Implementar mejoras basadas en las lecciones aprendidas de los incidentes.
- Coordinar y comunicar actividades de recuperación con todas las partes interesadas.

Gobernanza en NIST

Respecto a la Gobernanza, este es un elemento transversal que se integra todas las funciones del marco asegurando que la gestión de la ciberseguridad esté alineada con los objetivos estratégicos de la organización y que las responsabilidades y los procesos estén claramente definidos y gestionados. Esto implica:

- El desarrollo y mantenimiento de políticas de seguridad que guíen todas las actividades de ciberseguridad.
- La definición clara de las funciones y responsabilidades dentro de la organización para gestionar la ciberseguridad.
- El garantizar que la organización cumpla con las regulaciones y normativas aplicables en ciberseguridad.
- El supervisar y revisar el monitoreo periódico de las actividades de ciberseguridad para garantizar la efectividad y hacer ajustes según sea necesario.

Guía 21 MINTIC

La guía 21 del MINTIC indica que "*Es recomendable que las entidades creen un equipo de atención de incidentes de seguridad en cómputo CSIRT o un grupo que haga sus veces, quienes se encargaran de definir los procedimientos a la atención de incidentes, realizar la atención, manejar las relaciones con entes internos y externos, definir la clasificación de incidentes, y además de esto se encargaran de la:*

- *Detección de Incidentes de Seguridad: Monitorear y verificar los elementos de control con el fin de detectar un posible incidente de seguridad de la información.*
- *Atención de Incidentes de Seguridad: Recibe y resuelve los incidentes de seguridad de acuerdo con los procedimientos establecidos.*
- *Recolección y Análisis de Evidencia Digital: Toma, preservación, documentación y análisis de evidencia cuando sea requerida.*
- Anuncios de Seguridad: Deben mantener informados a los funcionarios, contratistas o terceros sobre las nuevas vulnerabilidades, actualizaciones a las plataformas y recomendaciones de seguridad informática a través de algún medio de comunicación (Web, Intranet, Correo).

- Auditoria y trazabilidad de Seguridad Informática: El equipo debe realizar verificaciones periódicas del estado de la plataforma para analizar nuevas vulnerabilidades y brechas de seguridad.
- Certificación de productos: El equipo verifica la implementación de las nuevas aplicaciones en producción para que se ajusten a los requerimientos de seguridad informática definidos por el equipo.
- Configuración y Administración de Dispositivos de Seguridad Informática: Se encargaran de la administración adecuada de los elementos de seguridad informática.
- Clasificación y priorización de servicios expuestos: Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.
- Investigación y Desarrollo: Deben realizar la búsqueda constante de nuevos productos en el mercado o desarrollo de nuevas herramientas de protección para combatir brechas de seguridad, y la proposición de nuevos proyectos de seguridad de la información.”[3]

[3] https://gobiernodigital.mintic.gov.co/692/articles-5482_G21_Gestion_Incidentes.pdf

Adopción del Marco de Trabajo NIST Para la Gestión de la Cibersguridad UNADISTA

La Universidad Nacional Abierta y a Distancia (UNAD) adoptar el marco de trabajo NIST Cybersecurity Framework (CSF) para la gestión de eventos e incidentes de ciberseguridad debido a su enfoque integral y adaptable a diversas necesidades.

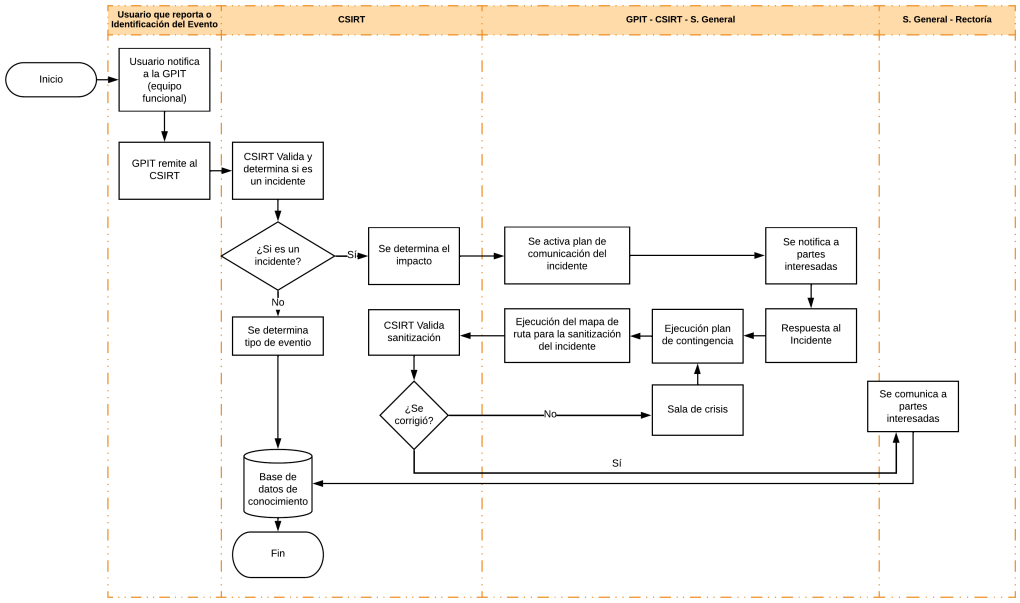
Este marco proporciona un lenguaje común y un conjunto de procesos que facilitan la identificación, protección, detección, respuesta y recuperación ante incidentes de ciberseguridad, lo que permite alinear la estrategia de Seguridad y Ciberseguridad de la Universidad con el fin de garantizar la [D] Disponibilidad, [Integridad] Integridad y [C] Confidencialidad de sus activos de información. Este marco, ampliamente reconocido y utilizado a nivel internacional, permite a la UNAD no solo cumplir con los requisitos normativos nacionales, como los establecidos en la Guía 21 del MINTIC y las leyes colombianas, sino también adherirse a estándares globales de ciberseguridad. La orientación proporcionada por el NIST CSF complementa y refuerza la implementación de otros marcos normativos como la ISO 27001 y la ISO 27034, asegurando un enfoque robusto y holístico en la gestión de ciberseguridad. Además, la estructura flexible del marco permite a la UNAD adaptarse a la evolución constante del panorama de amenazas cibernéticas y mantener una postura de seguridad proactiva.

Esta adopción refleja el compromiso de la UNAD con la calidad en la gestión de riesgos de ciberseguridad y la protección continua de la información crítica y sensible, asegurando que la universidad pueda operar de manera segura y resiliente en el entorno digital.

Gestión y Clasificación de Incidentes de Ciberseguridad Presentados en el Entorno UNADISTA

Teniendo presente lo anterior, y con base en el Marco de Referencia del Sistema de Gestión de Seguridad de la Información – SGSI RESOLUCIÓN No. 007298 DE 10 DE MAYO DE 2023 Unadista, establece el capítulo XI: DE LA GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, el cual tiene como objetivo: "*prevenir, detectar, contener, dar respuesta y evaluar los incidentes de seguridad de la información que puedan afectar la disponibilidad y la continuidad de los servicios, los procesos y procedimientos que se encuentran soportados por la Infraestructura lógica, física y tecnológica con la que cuenta la UNAD*"[4], *es* la Gerencia de Plataformas e Infraestructura Tecnológica quien recepcione alguna notificación de evento o incidente de ciberseguridad y esté remitirá al CSIRT Académico UNAD para validar su impacto. Una vez de determinado el impacto, el CSIRT comunicará a la Gerencia de Plataformas e Infraestructura Tecnológica a través de los medios establecidos para que esté pueda: *"atender, analizar, clasificar, responder, mitigar e investigar los incidentes de seguridad informática, a fin de ejercer controles sobre los activos tecnológicos y de información de la institución, respetando la cadena de custodia y demás elementos legales que permitan preservar la integridad y autenticidad de la evidencia en caso de un proceso jurídico y/o judicial".* La siguiente ilustración muestra el debido proceso para la gestión de un evento o un incidente.

Ilustración 2: Gestión para el reporte y validación de un incidente de ciberseguridad (Ver Anexo 2)



[4] https://gpit.unad.edu.co/images/Documentos/Resolucin_7298_Mayo_2023_Marco_referencia_SGSI.pdf

Nota. * El diagrama de flujo proporcionado detalla el procedimiento de gestión de eventos e incidentes de ciberseguridad en la Universidad Nacional Abierta y a Distancia.

A continuación, se describen los pasos clave y roles involucrados en el proceso:

Inicio del Proceso

Usuario que Reporta o Identificación del Evento

- Notificación a GPIT: Un usuario detecta y notifica un evento de ciberseguridad al equipo funcional de la GPIT - Gerencia de Plataformas e Infraestructura Tecnológica.
- Remisión al CSIRT: La GPIT remite el evento al CSIRT Académico UNAD para su validación y análisis.

Validación

Evaluación del Evento: El CSIRT valida si el evento (Ver Anexo 1: Posibles tipos de eventos de ciberseguridad) reportado es realmente un incidente de ciberseguridad.

Si es un Incidente: El proceso sigue el camino para gestionar el incidente.

Si no es un Incidente: Se determina el tipo de evento y se registra en la base de datos para la construcción del conocimiento para referencia futura.

Determinación del Impacto

- Evaluación del Impacto: Si se confirma como un incidente, el CSIRT determina el impacto del incidente en los activos y operaciones de la universidad y procede a:

Activación de Planes de Acción

- Activar el plan de comunicación[5] para informar a las partes interesadas relevantes.
- Se notifica a todas las partes interesadas sobre el incidente y las acciones que se están tomando.

Respuesta al Incidente

- Se ejecuta el plan de contingencia para mitigar los efectos del incidente.
- Si es requerido, se convoca a sala de crisis para una respuesta más coordinada y efectiva.

Sanitización del Incidente

El CSIRT Académico UNAD verifica si las acciones tomadas han resuelto completamente el incidente.

---

5 https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Plan_de_Comunicaciones_del_Incidente.pdf

- Si el incidente es corrigió, el proceso se cierra y se actualiza la base de datos de conocimiento con la información del incidente y su resolución.
- Si no se corrigió se vuelve a ejecutar el mapa de ruta para la sanitización del incidente hasta que se corrija.

Cierre del Incidente:

Una vez resuelto el incidente, se comunica a las partes interesadas sobre la resolución y se concluye el proceso. La siguiente tabla, presenta que roles se asocian en cada una de las etapas

Tabla 2

Asociación de roles por etapa para la gestión de un incidente

Etapa del Proceso	Acción	Rol Responsable
Inicio del Proceso	Usuario detecta y notifica un evento	Usuario
	GPIT recibe la notificación y remite el evento al CSIRT	GPIT
Validación por CSIRT	CSIRT valida si el evento es un incidente	CSIRT
	Si no es un incidente, determina el tipo de evento y lo registra	CSIRT
Determinación del Impacto	CSIRT evalúa el impacto del incidente	CSIRT
Activación de Planes de Acción	Activación del plan de comunicación del incidente	GPIT – Secretaría General
	Notificación a partes interesadas sobre el incidente	GPIT - CSIRT - Secretaría General
Respuesta al Incidente	Ejecución del plan de contingencia	GPIT - Responsable del activo
	Convocatoria a la sala de crisis si es necesario	Rectoría - Secretaría General - VIEM
Sanitización del Incidente	CSIRT valida la sanitización del incidente	CSIRT
	Si no se corrige, ejecutar nuevamente el mapa de ruta	GPIT - Responsable del activo
	Si se corrige, actualizar la base de datos de conocimiento	CSIRT
Cierre del Incidente	Comunicación final sobre la resolución del incidente	Rectoría - Secretaría General - VIEM

Elaboración propia

La guía de Roles y Responsabilidades de la Gestión de la Información UNADISTA, expone cuales son los roles que están establecidos al interior de la Universidad para dar respuesta a un evento o a un incidente de ciberseguridad.

Comunicación del Incidente[6]

INCIBE indica que *"La comunicación es parte fundamental del proceso de respuesta. Es importante que únicamente tengan conocimiento de lo sucedido aquellas personas o departamentos que puedan ser de ayuda en la solución de este. Por esa razón, únicamente el personal designado a dar respuesta debe estar en conocimiento de lo sucedido".*[7] En este sentido, la comunicación se debe realizar teniendo presente **la guía para el Plan de Comunicación del Incidente**[8] la cual tiene como alcance: la identificación de partes interesadas que requieren ser informadas sobre el incidente (Sistemas: de alta política, misional, funcional y operacional, aspirantes, estudiantes, egresados, proveedores, socios comerciales, autoridades regulatorias, medios de comunicación y público en general).

Gestión y Clasificación del Incidente

La Universidad Nacional Abierta y a Distancia UNAD define:

Evento:

Acción que puede comprometer la seguridad de un activo de información. Estos deben ser analizados para descartar intentos de ataques o daños en los activos de información.

Ejemplo. Infección de un equipo de cómputo a través de una USB infectada por malware

Incidente:

Acción provocada por un evento que afecta la [D] Disponibilidad, [I] Integridad o [C] Confidencialidad del activo de información comprometido de forma negativa[9].

Ejemplo. Daño o borrado de la información a causa del malware ejecutado a través de la USB

En este sentido los incidentes se clasifican así:

---

6 https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Plan_de_Comunicaciones_del_Incidente.pdf

7 https://www.incibe.es/empresas/blog/primeros-pasos-respuesta-incidentes

8 https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Plan_de_Comunicaciones_del_Incidente.pdf

9 https://selloeditorial.unad.edu.co/images/2022/boletines-cip-csirt/Boletin_13.pdf

Tabla 3

Clasificación de incidentes de ciberseguridad

N°	Categoría	
1	Código malicioso o Malware	Infecciones por software diseñado para infiltrarse o dañar un sistema sin el consentimiento del usuario
2	Correos peligrosos	Recepción de emails que contienen enlaces maliciosos, adjuntos infectados o intentos de phishing
3	Caída masiva de la red LAN de la universidad	Interrupciones extensas y significativas en la conectividad de la red local de la universidad.
4	Suplantación de identidad	Actos de hacerse pasar por otra persona o entidad para obtener acceso ilegítimo o información confidencial
5	Acceso no autorizado a sistemas de información	Entradas ilegítimas a sistemas informáticos para robar, alterar o examinar datos sin permiso.
6	Modificación o alteración no autorizada de la información.	Cambios ilegítimos en datos o software, alterando su estado original sin permiso
7	Ingreso de medios de almacenamiento no autorizado.	Uso de dispositivos de almacenamiento externos como USBs o discos duros sin autorización previa
8	Daño, Pérdida, o eliminación no autorizada de información	Destrucción o desaparición ilegítima de datos críticos o confidenciales
9	Fuga y/o robo de información física o digital.	Divulgación o sustracción no autorizada de datos, ya sea en formato físico o digital
10	Pérdida o alteración de registros de base de datos.	Desaparición o cambio no planificado de información en las bases de datos, afectando la integridad de los datos
11	Espionaje y divulgación de información	Observación o liberación ilegal de información confidencial o protegida
12	Robo de credenciales mediante Phishing.	Adquisición de datos de acceso como nombres de usuario y contraseñas a través de tácticas engañosas
13	Escaneo de redes y análisis de flujo de datos por personal no autorizado	Revisión ilegal de la red y análisis de tráfico de datos por individuos no autorizados
14	Acceso no autorizado a servidores	Entradas ilegales a servidores para obtener control, robar datos o realizar actividades maliciosas
15	Modificación de la configuración de los activos tecnológicos por personal no autorizado	Cambios no autorizados en hardware, software o configuraciones de red

16	Comportamiento anormal del computador y/o sistema de información.	Actividades inusuales que pueden indicar la presencia de malware o accesos no autorizados
17	Tráfico enviado desde o hacia lugares desconocidos	Movimientos de datos inesperados que pueden señalar intentos de intrusión o exfiltración de información
18	Comportamiento inusual de cuentas de usuarios privilegiadas	Actividades atípicas en cuentas con elevados niveles de acceso que pueden indicar compromisos de seguridad
19	Denegación de servicios	Ataques que buscan hacer un recurso de computadora inaccesible a los usuarios intentados, típicamente saturando el servicio con numerosas solicitudes

Elaboración propia

Detección, Evaluación y Análisis

La UNAD a través del CSIRT Académico y el Grupo Funcional de Seguridad de la GPIT realizan procesos de monitorización y alertamiento correlacionando eventos de seguridad que son reportados. Este ejercicio permite detectar de forma rápida amenazas que pueden ser contenidas mediante un análisis de seguridad.

Respecto a la evaluación, la UNAD evalúa los niveles de impacto de incidentes teniendo presente lo planteado en la Guía 21 del MINTIC

Tabla 4:

Nivel de severidad del incidente

Alto Impacto	Indica que el incidente afecta activos de información tangibles, intangibles o reputacionales que influyen de forma directa con el cumplimiento de los objetivos misionales de la Universidad La respuesta debe ser INMEDIATA
Medio Impacto	Indica que el incidente afecta activos de información a los objetivos de un proceso del SIG determinado
Bajo Impacto	Indica que el incidente afecta activos de información considerados como menores o insignificantes. Se recomienda la monitorización constante de estos activos con el fin de que se presente un cambio en el impacto

Recuperado de: https://gobiernodigital.mintic.gov.co/692/articles-5482_G21_Gestion_Incidentes.pdf

Priorización del Incidente

Nivel de criticada del Impacto: Hace referencia a la evaluación de la gravedad y el alcance de las consecuencias causadas por un incidente de seguridad. Este indica el grado de daño potencial que puede sufrir un activo de información. La UNAD clasifica la criticidad en cinco niveles diferentes

Tabla 5: Criticidad del impacto

Nivel	Valor	Definición
Inferior	0,1	Activos de información no críticos, como estaciones de trabajo de usuarios con funciones no críticas
Bajo	0,25	Activos de información que apoyan a una sola dependencia o proceso de una entidad.
Medio	0,5	Activos de información que apoyan más de una dependencias o proceso de la entidad.
Alto	0,75	Activos de información pertenecientes al área de Tecnología y estaciones de trabajo de usuarios con funciones críticas.
Superior	1	Activos de información Críticos

Recuperado de: https://gobiernodigital.mintic.gov.co/692/articles-5482_G21_Gestion_Incidentes.pdf

Nivel de impacto actual: Hace referencia a la evaluación de la magnitud y las consecuencias que está teniendo el incidente en tiempo real, indicando la gravedad y el alcance de los daños causados por el incidente en ese momento específico. El nivel de impacto actual puede variar según el tipo de incidente y la infraestructura o sistema afectado. A continuación, se relacionan algunos factores a considerar para determinar el nivel de impacto actual:

- Disponibilidad:
  - ¿El incidente está afectando la disponibilidad de los sistemas y servicios?
  - ¿Hay interrupciones en la operación normal?
- Integridad:
  - ¿Se ha comprometido la integridad de los datos o sistemas?
  - ¿Se han alterado o manipulado de alguna manera?
- Confidencialidad:
  - ¿Se ha violado la confidencialidad de la información sensible?
  - ¿Se han accedido o filtrado datos confidenciales?
- Alcance:
  - ¿El incidente está afectando solo a un sistema o a múltiples sistemas y/o redes?
  - ¿Está impactando a un departamento o a toda la organización?
- Consecuencias:

- ¿Qué tipo de daños se están produciendo como resultado del incidente?
- ¿Hay pérdida de datos, pérdida financiera, interrupción del negocio u otras consecuencias significativas?

La evaluación del nivel de impacto actual es esencial para tomar decisiones informadas sobre la respuesta y mitigación del incidente, ya que esta brinda información para asignar recursos adecuados y el establecimiento de prioridades correctas para minimizar los efectos negativos con el fin de recuperarse lo más rápido posible. La UNAD clasifica el nivel de impacto actual en cinco niveles:

Tabla 6

Descripción del nivel de impacto actual

Nivel	Valor	Definición
Inferior	0,1	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo
Bajo	0,25	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo
Medio	0,5	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo
Alto	0,75	Impacto moderado en uno o más componentes de más de un sistema de información
Superior	1	Impacto alto en uno o más componentes de más de un sistema de información

Recuperado de: https://gobiernodigital.mintic.gov.co/692/articles-5482_G21_Gestion_Incidentes.pdf

Nivel de impacto futuro: Hace referencia a la evaluación de las posibles consecuencias y el alcance que el incidente puede tener en el futuro si no se toman medidas adecuadas para mitigar y resolver el problema. El nivel de impacto futuro se basa en una evaluación de los riesgos potenciales y la proyección de cómo podría evolucionar el incidente si no se toman acciones correctivas. A continuación, se relacionan algunos factores que a considerar al determinar el nivel de impacto futuro:

- Propagación:
  - ¿Existe el riesgo de que el incidente se propague a otros sistemas, redes o departamentos de la organización?
- Expansión:
  - ¿Es posible que el incidente se agrave y cause daños adicionales o afecte a más usuarios o recursos críticos?
- Persistencia:

    - ¿El incidente puede persistir o prolongarse en el tiempo si no se toman las medidas adecuadas?
    - ¿Puede haber un impacto continuo o recurrente?
- Vulnerabilidades:
    - ¿Existen vulnerabilidades conocidas o brechas de seguridad que podrían agravar el incidente o dar lugar a nuevos incidentes relacionados?
- Consecuencias a largo plazo:
    - ¿Cuáles podrían ser las implicaciones a largo plazo del incidente en términos de pérdidas financieras, daño reputacional o cumplimiento normativo?

La UNAD clasifica el nivel de impacto futuro en cinco niveles

Tabla 7: Nivel de impacto futuro

Nivel	Valor	Definición
Inferior	0,1	Impacto leve en uno de los componentes de cualquier sistema de información o estación de trabajo
Bajo	0,25	Impacto moderado en uno de los componentes de cualquier sistema de información o estación de trabajo
Medio	0,5	Impacto alto en uno de los componentes de cualquier sistema de información o estación de trabajo
Alto	0,75	Impacto moderado en uno o más componentes de más de un sistema de información
Superior	1	Impacto alto en uno o más componentes de más de un sistema de información

Recuperado de: https://gobiernodigital.mintic.gov.co/692/articles-5482_G21_Gestion_Incidentes.pdf

Evaluar el nivel de impacto futuro es crucial para la toma de decisiones estratégicas en la gestión de incidentes de ciberseguridad. Ayuda a anticipar los posibles escenarios y a implementar las medidas necesarias para prevenir o reducir el impacto negativo a largo plazo. Esto incluye la implementación de controles de seguridad adicionales, actualizaciones de sistemas, capacitación del personal y otras acciones para fortalecer la postura de seguridad de la Universidad.

Nivel de prioridad: Hace referencia a la clasificación de los incidentes según su importancia y urgencia relativa. Esto indica la atención y los recursos que se deben asignar a cada incidente en función de su impacto, criticidad y a otros factores relevantes. La prioridad de un incidente se determina considerando varios factores, que pueden incluir:

- Impacto: La evaluación del impacto del incidente en términos de disponibilidad, integridad y confidencialidad de los sistemas y datos. Cuanto mayor sea el impacto, mayor será la prioridad.

- **Criticidad**: La gravedad del incidente y su potencial para causar daños significativos a la organización, como pérdidas financieras, interrupción del negocio o violación de la seguridad.
- **Urgencia**: La necesidad de una acción inmediata para contener y mitigar el incidente. Algunos incidentes pueden requerir respuestas rápidas para evitar un mayor deterioro de la situación.
- **Alcance**: La extensión del incidente y su capacidad para afectar a múltiples sistemas, redes o usuarios. Incidentes que tienen un alcance más amplio pueden tener una prioridad más alta.
- **Valor del activo de información**: La importancia y el valor de los activos o recursos que están en riesgo. Esto puede incluir información crítica, datos sensibles o sistemas clave para el funcionamiento de la organización.

Con el fin de priorizar esfuerzos y recursos para asegurar que los incidentes más críticos y urgentes se manejen de manera oportuna y efectiva, la UNAD utiliza la escala de clasificación que se presenta en la siguiente tabla.

Tabla 8: Clasificación de los niveles de prioridad

Nivel de prioridad	Valor
Inferior	00,00 - 02,49
Bajo	02,50 - 03,74
Medio	03,75 - 04,99
Alto	05,00 - 07,49
Superior	07,50 - 10,00

Recuperado de: https://gobiernodigital.mintic.gov.co/692/articles-5482_G21_Gestion_Incidentes.pdf

Es importante destacar que la prioridad puede cambiar a medida que se recopila más información sobre el incidente o a medida que evoluciona la situación. Por lo tanto, se deben realizar evaluaciones periódicas y se debe ajustar la prioridad según sea necesario durante todo el proceso de gestión del incidente.

El nivel de prioridad se calcula a partir de la siguiente formula:

Nivel Prioridad = (Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad del Sistema * 5)

Tiempo de respuesta

Hace referencia al período de tiempo en el cual se debe tomar acción para abordar un incidente desde el momento en que es detectado o reportado. Este indica la rapidez que se debe dar para iniciar la respuesta y se tomen medidas para contener, mitigar y resolver el incidente. El tiempo de respuesta es crítico en la gestión de incidentes de ciberseguridad, ya

que un retraso en la respuesta puede permitir que el incidente se propague, cause mayores daños o prolongue la interrupción de servicios impactando así de forma futura.

El tiempo de respuesta eficaz se caracteriza por:

- Detectar el incidente lo más pronto posible a través de sistemas de monitoreo, detección de intrusiones u otras técnicas de seguridad.
- Informar de forma rápida a la GPIT y partes interesadas sobre la existencia del incidente teniendo presente el Plan de Comunicación del Incidente.
- Realizar una evaluación inicial para comprender el alcance, la naturaleza y la gravedad de este. Esto permite tomar decisiones informadas sobre las acciones a seguir.
- Iniciar la respuesta y las medidas de contención y mitigación tan pronto como sea posible, para evitar que el incidente se propague y cause mayores daños. Para la UNAD, el Mapa de Ruta para la Sanitización del Incidente se convierte en un instrumento que orienta la respuesta
- Asignar los recursos adecuados, como personal especializado, herramientas y tecnologías, para abordar el incidente de manera efectiva.
- Realizar un seguimiento continuo del incidente a partir de lo planteado Plan de avance ante la respuesta a un incidente, donde se implementan acciones correctivas con el fin de trabajar para su resolución completa en el menor tiempo posible.

Tiempo de respuesta para socializar la sanitización del incidente

Hace referencia al período durante el cual se llevan a cabo las actividades necesarias para eliminar completamente las amenazas y vulnerabilidades, restaurar la integridad y la seguridad de los sistemas, y mitigar cualquier impacto residual. Este tiempo de sanitización se construye a partir de un cronograma de trabajo que involucra a todas las partes interesadas en el proceso de respuesta. Las partes interesadas, son quienes apoyan la ejecución de tareas específicas, como análisis forense, eliminación de malware, actualización de sistemas, restauración de datos y parcheo de vulnerabilidades. El cronograma de trabajo establece los plazos y la secuencia de las actividades, asegurando una coordinación efectiva y una asignación adecuada de recursos. La duración del tiempo de sanitización puede variar según la complejidad y la gravedad del incidente, pero es esencial para garantizar que los sistemas y datos estén completamente protegidos y seguros antes de reanudar las operaciones normales. En este ejercicio se requiere socializar todo el proceso desde el de Mapa de Ruta para la Sanitización del Incidente, Teniendo siempre presente que en este punto se debe mitigar o reducir el impacto presentado

Tabla 9:Timepos estimados para socializar el mapa de ruta para la sanitización del incidente

Nivel de prioridad	En días hábiles	
Inferior	4	**Entrega del** Mapa de Ruta para la Sanitización del Incidente
Bajo	4	
Medio	4	
Alto	4	
Superior	4	

Elaboración propia

El tiempo de respuesta puede variar según las políticas y los acuerdos de nivel de servicio (SLA)[10] establecidos por la Universidad, así como las capacidades y la preparación del equipo que dé respuesta al incidente. Es esencial establecer acciones realistas y contar con procedimientos claros para garantizar una respuesta oportuna y eficiente.

La siguiente tabla, presenta el nivel de prioridad para dar respuesta a un incidente de ciberseguridad

Tabla 10: Niveles de prioridad para dar respuesta a un incidente

Nivel de prioridad	Valor (horas)	en Días	
Inferior	96	4 hábiles	Ejecución del plan de contingencia y aplicación del libro de Jugadas (Play Book)[11]
Bajo	96	4 hábiles	
Medio	72	3 hábiles	
Alto	48	2 calendario	
Superior	24	1 calendario	

Elaboración propia

Riesgos Máximos Aceptados por la UNAD

El nivel de criticidad de afectación del incidente puede ser soportado a partir de la tabla de riesgos máximos que permiten determinar el nivel de criticidad de un incidente. La siguiente tabla, representa los riesgos máximos que pueden afectar y generar un impacto de ciberseguridad en Universidad

[10] https://www.cisco.com/c/es_mx/support/docs/availability/high-availability/15117-sla.html#crea_slas

[11] Conjunto de procedimientos predefinidos y documentados que describen las acciones y las mejores prácticas a seguir durante la respuesta a un incidente. Es una guía paso a paso que ayuda a los equipos de respuesta a incidentes a manejar de manera eficiente y efectiva diferentes tipos de incidentes de seguridad.

Tabla 11: Niveles de riesgos máximos

Tabla de Riesgos Máximos	
Superior	Afecta de forma considerable la continuidad de la operación UNADISTA
	Afecta a más del 75% de los sistemas de la Universidad
	Interrupción en la prestación del servicio superior a 24 horas o superior al 50% de los usuarios
	El incidente requiere resolverse durante más de un mes
	El impacto económico es superior al 0.1% sobre los ingresos institucionales
	Afecta la reputación en el orden internacional de forma apreciable con cobertura en medios de comunicación
Alto	Afecta un servicio o Unidad esencial
	Afecta a más del 50% de los sistemas de la Universidad
	Interrupción en la prestación del servicio superior a 8 horas y/o superior al 25% de los usuarios
	El incidente requiere resolverse entre 15 y 30 días
	El impacto económico es superior al 0.05% sobre los ingresos institucionales
	Afecta la reputación en el orden nacional de forma apreciable con cobertura en medios de comunicación
Medio	Afecta a más del 25% de los sistemas de la Universidad
	Interrupción en la prestación del servicio superior a 3 horas y superior al 15% de los usuarios
	El incidente requiere resolverse entre 3 y 14 días
	El impacto económico es superior al 0.02% sobre los ingresos institucionales
	Afecta la reputación en el orden nacional con eco mediático y afectación de la reputación de terceros
Bajo	Afecta a entre el 0% y el 24% de los sistemas de la Universidad
	Interrupción en la prestación del servicio superior a 1 hora y superior al 5% de los usuarios
	El incidente requiere resolverse entre 3 y 14 días
	El impacto económico es superior al 0.005% sobre los ingresos institucionales
	Afecta la reputación en el orden nacional con eco mediático y afectación de la reputación de terceros
inferior	Afecta a los sistemas de la organización
	Interrupción de la prestación de un servicio
	Daños reputacionales puntuales, sin eco mediático

Elaboración propia

Nivel de Peligrosidad del Incidente

La UNAD establece los criterios para la determinación del nivel de peligrosidad que aplican para cualquiera de los niveles que se plantean a continuación:

Tabla 12: Tabla de nivel de peligrosidad del incidente

Tabla de Nivel de Peligrosidad del Incidente		
Nivel	Clasificación	Tipo de Incidente
Superior	Amenaza Persistente Avanzada	APT[12]
Alto	Código malicioso	Distribución de malware Configuración de malware
	Intrusiones	Robo
	Indisponibilidad de servicios	Sabotaje Interrupciones
Medio	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado Discurso de odio
	Código malicioso	Sistema infectado Servidor C&C (Mando y Control)
	Intrusión	Compromiso de aplicaciones Compromiso de cuentas con privilegios Explotación de vulnerabilidades conocidas Intento de acceso con vulneración de credenciales
	Intento de intrusión	Ataque desconocido
	Indisponibilidad de servicios	DoS - DDoS
	Compromiso de la información	Acceso no autorizado a información Modificación no autorizada de información Pérdida de datos
	Fraude	Phishing Uso no autorizado de recursos Derechos de autor Suplantación
	Obtención de información	Ingeniería social
	Disponibilidad	Mala configuración
	Vulnerabilidad	Sistema vulnerable Revelación de información Servicio con acceso potencial no deseado Amplificador DDoS a través de DNS[13] Criptografía débil
Bajo	Contenido abusivo	Spam
	Obtención de información	Análisis de paquetes - Escaneo de red
	Otros	Otros

Elaboración propia

[12] https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats
[13] https://www.cloudflare.com/es-es/learning/ddos/dns-amplification-ddos-attack/

Declaración y Notificación del Incidente

El CSIRT Académico UNAD en conjunto con la Gerencia de Plataformas e Infraestructura Tecnológica - GPIT disponen el siguiente canal para la comunicación un incidente[14]:

Correo: seguridad.información@unad.edu.co

Dado el caso de presentarse un incidente de ciberseguridad, se deberá diligenciar **el Formato para el reporte de un incidente de ciberseguridad ante la UNAD,** el cual contiene la siguiente información:

Tabla 134. Detalle para la notificación de un incidente a través del Formato para el reporte de un incidente de ciberseguridad ante la UNAD

Información Inicial	
1. Reporte N°	Indica el número de reporte asignado por el CSIRT Académico UNAD en su mesa de ayuda. Este dato lo brinda el CSIRT
2. TLP (Traffic Light Protocol)[15]:	Esquema usado para el intercambio de información sensible de ciberseguridad. Indica el nivel de confidencialidad del reporte. A continuación, se relaciona el código de colores aprobado actualmente por FIRST[16] TLP: RED : Se usa cuando la información es se limita a un grupo de personas en específico, teniendo presente que los receptores no deben compartir información con ningún tercero fuera del ámbito donde se expuso de forma inicial TLP: AMBAR : Se usa cuando la información requiere ser distribuida de forma limitada. El receptor puede compartir la información solamente con funcionarios de la universidad, clientes o proveedores que requieran conocer el contenido y estar al tanto para evitar daños. TLP: GREEN : Se usa cuando la información resulta ser útil para toda la Universidad y/o todas sus partes interesadas. Es preciso indicar que el receptor puede compartir la información con otras organizaciones, pero nunca a través de canales públicos. TLP: CLEAR : Se usa cuando la información no genera ningún riesgo de mal uso y pueda ser difundido de forma pública. En este sentido, la información puede ser distribuida sin restricciones, pero sujeta a controles de derechos de autor

[14] https://selloeditorial.unad.edu.co/images/2022/boletines-cip-csirt/Boletin_13.pdf
[15] https://www.incibe.es/incibe-cert/sobre-incibe-cert/tlp
[16] https://www.first.org/

3. Fecha de elaboración del reporte:	Se debe indicar la fecha y hora en la que se construye el reporte
4. ¿El incidente se había presentado?	Se debe indicar si el incidente se había presentado de forma previa, para esto el analista puede hacer uso de la información de la mesa de ayuda
Datos de contacto CSIRT Académico UNAD o Persona Quien Reporta el Incidente	
5. Nombre de quien reporta	Se debe indicar el nombre del analista, funcionario o persona quien está reportando el incidente
6. Rol:	Se debe indicar el rol que desempeña dentro o fuera de la universidad, quien está realizando el reporte
7. Celular / teléfono	Se debe indicar el número telefónico de contacto (celular o teléfono)
8. Correo electrónico	Se debe indicar el correo electrónico institucional
Datos de contacto Unidad que presenta el Incidente	
9. Fecha y hora del descubrimiento	Se debe indicar la fecha y hora del descubrimiento del incidente
10. Unidad	Se debe indicar la unidad responsable del activo de información
11. Responsable del activo	Se debe indicar el nombre del responsable del activo de información (Quien administra le administra)
12. Celular / teléfono	Se debe indicar el número telefónico de contacto (celular o teléfono)
13. Correo electrónico	Se debe indicar el correo electrónico institucional
Activo de Información Afectado	
14. Nombre del activo	Se debe indicar el nombre del activo tal como se encuentra relacionado en el inventario de activos de información
15. Dirección IP	Indique la URL o dirección IP donde se encuentra en servicio el activo de información
16. Ubicación	Se debe indicar la ubicación del activo Si es virtual, indicar en que segmento de red se encuentra ubicado Si es físico, indicar en que parte locativa de la Universidad se encuentra ubicado
17. Tipo de activo	Se debe indicar el tipo de activo de información según metodología MAGERIT. La Guía para el Inventario y Clasificación de Activos de Información, indica como se puede catalogar un activo de información
18. Tabla de Riesgos máximos	Se debe indicar como se encuentra catalogado el activo de información, teniendo presente la tabla de riesgos máximos de la universidad

19. Método de detección	Se debe indicar a través de que instrumento o medio se detectó el incidente. Este se puede dar por: • Reportes de Usuario • Sistemas de monitoreo de la UNAD • Otro
20. Debido al incidente	Se debe indicar con respuesta afirmativa, o de No determinado si: Alguien no autorizado tuvo acceso a la información Se ha impedido a algún usuario el acceso a la información Se ha borrado, modificado y eliminado alguna información
21. Posible causa raíz	Se debe indicar una posible causa raíz que ocasiono el incidente. A continuación, se relacionan algunas de estas como ejemplo: • Falta de actualizaciones y parches • Contraseñas débiles o filtradas • Falta de educación y concienciación en ciberseguridad • Falta de políticas y procedimientos de seguridad • Falta de control de acceso adecuado • Configuración incorrecta de sistemas • Ejecución de malware • Ingeniería social • Vulnerabilidades desconocidas • Escasez de recursos de seguridad • Falta de monitoreo y detección • Amenazas internas • Proveedores no seguros • Cumplimiento deficiente de políticas de seguridad • Falta de preparación para incidentes
22. Clasificación del Incidente	Se debe indicar el tipo de clasificación del incidente. La UNAD Clasifica posibles incidentes de ciberseguridad en la tabla 2 de este documento
23. Táctica	Se debe indicar la posible táctica usada en el incidente. La UNAD, adopta el marco de trabajo Mitre ATT&CK el cual plantea Tácticas, Técnicas y Conocimiento Común de Adversarios
24. Técnica	Se debe indicar la técnica asociada con la táctica propuesta por el marco de trabajo de Mitre ATT&CK
Nivel de Prioridad:	
25. Impacto actual	Se debe indicar el impacto actual teniendo en cuenta la cantidad de daño que ha provocado el incidente en el momento de ser detectado (ver tabla 5). El valor que se asigna al nivel corresponde al planteado en la tabla 5

26. Impacto futuro	Se debe indicar el impacto futuro teniendo presente la cantidad de daño que pueda causar el incidente si no es contenido, ni erradicado. (ver tabla 6) El valor que se asigna al nivel corresponde al planteado en la tabla 6
27. Criticidad del sistema	Se debe indicar la criticidad del sistema teniendo presente la tabla 10 de niveles de riesgos máximos. * Es preciso indicar que esta información se encuentra en la catalogación e identificación del activo de información
28. Prioridad	El nivel de prioridad esta dado por la formula: Nivel Prioridad = (Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad del Sistema * 5)
29. Tiempo de respuesta	A partir del resultado de nivel de prioridad, se debe establecer el tiempo de respuesta tal como se indica en la tabla 8
30. Tiempo para socializar el mapa de ruta de sanitización	Se debe indicar el tiempo para la socialización del mapa de ruta donde se establece el periodo en el cual se realizarán las acciones necesarias para solventar el incidente. Ver tabla 9
31. Impacto	Luego de la indagación inicial que se realiza que se debe determinar si se presentó impacto de orden: • Financiero • Reputacional • Operacional • Legal
32. Acciones realizadas	Se debe indicar de forma detallada las acciones realizadas en el momento para la comunicación y respuesta al incidente. Algunas acciones para realizar son: • Aislar el sistema o red afectada si es posible, con el fin de evitar que el incidente se propague aún más y cause más daño. • Detener actividades maliciosas que estén en curso, esto podría implicar apagar un servidor comprometido o desconectar un dispositivo de la red o los que sean requeridos. (Art 30 Medidas de emergencia RESOLUCIÓN No. 007298 DE 10 DE MAYO DE 2023) • Recopilar información relevante sobre el incidente, incluyendo registros de actividad, archivos sospechosos y cualquier otro detalle que pueda ayudar en la investigación y resolución. • Notificar a partes interesadas teniendo presente el TLP asignado para el reporte, incluyendo el equipo de

	respuesta a incidentes, el personal de TI y la alta dirección. • Preservar la evidencia necesaria para una investigación posterior o para tomar medidas legales. Esto puede incluir imágenes del disco duro, registros de red, logs, registro de acceso físicos y cualquier otro tipo de prueba. • Identificar y cerrar posibles puertas de entrada que los atacantes podrían haber utilizado para ingresar al sistema o la red comprometida. Tener presente cambiar contraseñas, parchear vulnerabilidades o desactivar servicios no esenciales. • Informar a las autoridades competentes, dependiendo de la gravedad del incidente y la normatividad vigente, el Plan de Comunicación del Incidente detalla la forma de cómo podría realizarse esta acción • Evaluar el alcance del incidente para determinar qué datos o sistemas se vieron comprometidos y qué daño se ha causado. • Si el incidente involucra datos personales o información sensible del usuario, es necesario notificar a los afectados de teniendo presente el Plan de Comunicación del Incidente. Esto puede incluir medios de comunicación
33. Acciones pendientes	Indique las acciones pendientes por realizar. Alguna de ellas puede ser: • Realizar una investigación exhaustiva del incidente para determinar cómo ocurrió, cuáles fueron las causas raíz y qué sistemas o datos se vieron afectados. Esto implica examinar registros, registros de actividad y cualquier otro tipo de evidencia digital relevante. • Documentar todos los aspectos del incidente, incluyendo las acciones tomadas durante la respuesta inicial, los hallazgos de la investigación y las lecciones aprendidas. Esto servirá como referencia en el futuro y para cumplir con los requisitos de informes. • Evaluar el impacto del incidente en la organización, incluyendo cualquier pérdida de datos, tiempo de inactividad, costos asociados y daños a la reputación. • Determinar las causas subyacentes del incidente. Esto podría implicar identificar las vulnerabilidades explotadas, las debilidades en las políticas de seguridad

	o las prácticas de los empleados que contribuyeron al incidente. • Con base en las lecciones aprendidas y la base de datos de conocimiento, tomar medidas correctivas para abordar las vulnerabilidades y debilidades detectadas. • Ajustar el plan de respuesta a incidentes de la organización en función de lo que se aprendió del incidente • Revisar la arquitectura de seguridad de la organización para garantizar que esté diseñada para resistir amenazas similares en el futuro. • Mantener un monitoreo continuo de la red y los sistemas para detectar cualquier actividad anómala o futuros intentos de ataque. • Capacitar y concienciar a la plataforma humana UNADISTA y artes interesadas con el fin de optimizar la ciberseguridad de nuestro entorno digital. • Si el incidente involucró a terceros o proveedores, revisar sus prácticas de seguridad para mitigar futuros riesgos. • Preparar informes internos y externos, incluyendo un resumen del incidente, las acciones tomadas y las medidas preventivas futuras. • Ejercicio de Simulacros: Considere realizar ejercicios de simulacros de incidentes para que el personal pueda practicar la respuesta a situaciones similares en el futuro. • Revisión Continua: Mantenga una revisión continua de la postura de seguridad cibernética de la organización y ajuste las medidas de seguridad según sea necesario.
34. Se identifico el responsable	Se debe indicar si se identifica algún responsable del incidente. Si la respuesta es afirmativa, indique el nombre del grupo o persona que está involucrada en esté.
35. Archivos adjuntos	Indique los archivos adjuntos. Estos deberán encontrarse en el sitio que determine el CSIRT Académico UNAD para su gestión y consulta

Elaboración propia

Plan para el Avance y la Respuesta a un Incidente de Ciberseguridad

"*Es importante para la entidad implementar una estrategia que permita tomar decisiones oportunamente para evitar la propagación del incidente y así disminuir los daños a los recursos de TI y la pérdida de la confidencialidad, integridad y disponibilidad de la información***"**[17]

Iniciar un proceso de contención, erradicación y recuperación en un incidente de ciberseguridad es crucial para limitar y revertir el daño causado por un ataque. La contención permite aislar rápidamente los sistemas afectados, evitando la propagación del incidente y minimizando el impacto en la infraestructura de TI. Tras la contención, la erradicación se centra en eliminar completamente la amenaza del sistema, asegurando que no queden residuos que puedan reiniciar la infección y cerrando las vulnerabilidades explotadas para restaurar la seguridad operativa. Finalmente, la recuperación implica restaurar los sistemas y datos a un estado operativo normal de manera segura, revisando y fortaleciendo las políticas de seguridad para prevenir futuros incidentes. Este proceso es fundamental para mantener la confianza en los sistemas de TI y proteger la confidencialidad, integridad y disponibilidad de la información, evitando daños prolongados y costosos y asegurando la continuidad del negocio.

A continuación, se relacionan algunos aspectos laves a considerar en el momento de llevar a cabo o ejecutar el plan para el avance ante la respuesta a un incidente de ciberseguridad:

[17] https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Contención Erradicación y Recuperación

Contención:

- La contención debe ser inmediata para evitar que el incidente se propague aún más. Esto implica identificar y aislar las áreas afectadas de la red o sistemas.
- Identifique y detenga las actividades maliciosas en curso. Esto puede incluir la desconexión de sistemas comprometidos o la eliminación de archivos maliciosos.
- Trabaje para minimizar el impacto del incidente en la operatividad de la organización mientras se preserva la evidencia para futuras investigaciones.
- Determine si es necesario involucrar a equipos de respuesta incidentes externos o a terceros expertos en ciberseguridad para ayudar con la contención y la indagación.
- Notifique a los equipos y partes interesadas pertinentes dentro de la organización sobre la situación y las medidas tomadas para contener el incidente.
- Establezca una monitorización continua para asegurarse de que la amenaza esté realmente contenida y no haya recaídas (PoC)[18].

Erradicación:

- Realice una indagación detallada para identificar las causas raíz del incidente. Determine cómo el adversario logra ingresar y qué debilidades exploto.
- Elimine completamente cualquier malware u otras amenazas de los sistemas afectados. Esto puede requerir la sanitización de sistemas comprometidos y la aplicación de parches para corregir vulnerabilidades.
- Cambie todas las contraseñas comprometidas y refuerce las políticas de contraseñas para prevenir futuros ataques.
- Revise y refuerce la seguridad de la infraestructura y sistemas para evitar futuros incidentes similares. Esto puede incluir la actualización de sistemas, la implementación de medidas de seguridad adicionales y la revisión de la política de seguridad.
- Considere si se necesita una reestructuración más profunda de la arquitectura de seguridad para evitar futuros ataques (Defensa en profundidad)[19].
- Genere espacios de concienciación y educación que contribuya en la mejora de toma de conciencia de seguridad.

Recuperación:

- Una vez que se ha erradicado la amenaza y se han implementado mejoras de seguridad, trabaje en la restauración de la operatividad normal de los sistemas y servicios afectados.

---

[18] https://learn.microsoft.com/es-es/azure/architecture/serverless-quest/poc-pilot
[19] https://www.cloudflare.com/es-es/learning/security/glossary/what-is-defense-in-depth/

- Antes de restaurar sistemas, asegúrese de que estén seguros y de que se hayan corregido todas las vulnerabilidades identificadas.
- Realice pruebas de continuidad de negocio para asegurarse de que la Universidad pueda funcionar sin problemas después de un incidente.
- Si es necesario, comunique la resolución del incidente a partes interesadas, como clientes, proveedores o socios comerciales y comunidad UNADISTA.
- Prepare informes detallados que incluyan un resumen del incidente, las acciones tomadas y las medidas preventivas futuras.
- Documente las lecciones aprendidas.
- Realice una revisión exhaustiva de todo el incidente, desde la detección hasta la recuperación, para identificar áreas de mejora y ajustar las políticas y procedimientos de seguridad.
- Mantenga una evaluación continua de la seguridad cibernética de la organización y ajuste las medidas de seguridad según sea necesario para prevenir futuros incidentes.

La siguiente tabla presenta ejemplos de cómo actuar en términos de contención, erradicación y recuperación ante un incidente

Tabla 14

Forma de actuar para la contención, erradicación y recuperación ante un incidente de ciberseguridad

Incidente de Ciberseguridad	Contención	Erradicación	Recuperación
Ataque de Ransomware	Aísle la red o sistema afectado para evitar la propagación.	Identifique y elimine el ransomware de los sistemas.	Restaure los archivos cifrados desde copias de seguridad. Tenga presente la política de copias de respaldo, RESOLUCIÓN No. 007298 DE 10 DE MAYO DE 2023, Resolución No. 367 de 17 de enero de 2019 y Resolución 8547 de sep. 8 de 2016.
Phishing de Empleados	Identifique y bloquee los correos electrónicos de phishing y notifique a los empleados.	Genere espacio de educación en ciberseguridad con los usuarios sobre cómo identificar el phishing y actualice las contraseñas comprometidas.	Monitoree de forma continua para detectar posibles amenazas Tenga presente la política de copias de respaldo, RESOLUCIÓN No. 007298 DE 10 DE MAYO DE 2023, Resolución No. 367 de 17 de

			enero de 2019 y Resolución 8547 de sep. 8 de 2016.
Infiltración de Malware	Aísle el sistema infectado y desactive el malware.	Elimine completamente el malware y aplique parches para cerrar las vulnerabilidades explotadas.	Restaure el sistema afectado desde una imagen de disco limpia y mejore la seguridad de la red y de los sistemas. Tenga presente la política de copias de respaldo, RESOLUCIÓN No. 007298 DE 10 DE MAYO DE 2023, Resolución No. 367 de 17 de enero de 2019 y Resolución 8547 de sep. 8 de 2016.
Brecha de Datos	Identifique la fuente de la brecha y aísle la información comprometida.	Cierre la brecha de seguridad, determine la causa raíz y notifique a las partes afectadas.	Cumpla con las regulaciones de notificación de violación de datos y fortalezca las medidas de seguridad para proteger datos sensibles. Tenga presente la política de copias de respaldo, RESOLUCIÓN No. 007298 DE 10 DE MAYO DE 2023, Resolución No. 367 de 17 de enero de 2019 y Resolución 8547 de sep. 8 de 2016.
Ataque de DDoS	Implemente medidas para mitigar el ataque DDoS, como el filtrado de tráfico.	Identifique la fuente del ataque y bloquee el tráfico malicioso.	Evalúe la resistencia de la red a futuros ataques DDoS y mejore las medidas de mitigación.
Compromiso de Cuentas de Usuario	Restablezca contraseñas comprometidas y active la autenticación multifactor.	Identifique y cierre la entrada de los atacantes, revise las políticas de contraseñas y realice un análisis de seguridad exhaustivo.	Genere espacio de educación en ciberseguridad con los usuarios sobre buenas prácticas de seguridad y mantenga un monitoreo continuo. Tenga presente la política de copias de respaldo, RESOLUCIÓN No. 007298 DE 10 DE MAYO DE 2023, Resolución No. 367 de 17 de

			enero de 2019 y Resolución 8547 de sep. 8 de 2016.
Fuga de Datos Interna	Detenga la fuga de datos y aísle la información comprometida.	Identifique al empleado involucrado y tome medidas disciplinarias, revise los controles de acceso y realice una auditoría de registros.	Notifique a las partes afectadas según sea necesario y refuerce las políticas de seguridad y la capacitación de empleados.
Ataque a la Infraestructura en la Nube	Aísle la infraestructura comprometida y cambie las credenciales de acceso.	Identifique y elimine el malware o la actividad maliciosa, y refuerce la seguridad de la infraestructura.	Monitoree de forma continua la infraestructura y ajuste la política de seguridad en la nube.
Acceso no Autorizado a Servidores	Revise y cierre las posibles puertas de entrada utilizadas por los atacantes.	Identifique y elimine cualquier acceso no autorizado, cambie las contraseñas y aplique parches.	Fortalezca la seguridad del servidor y revise las políticas de acceso y autenticación.

Elaboración propia

Actividades post Incidente

Las actividades posteriores a un incidente de ciberseguridad son esenciales y desempeñan un papel crítico en la gestión completa de la situación.

A continuación, se relacionan actividades posteriores a realizar frente a un incidente:

- Las actividades posteriores permiten a una organización aprender de la experiencia. Identificar las causas raíz, las debilidades en las políticas y prácticas de seguridad, y las lecciones aprendidas ayuda a la organización a mejorar su postura de seguridad cibernética. Sin una revisión post-incidente, es más probable que ocurran incidentes similares en el futuro.
- Las investigaciones posteriores a incidentes ayudan a identificar las causas subyacentes que permitieron que el incidente ocurriera en primer lugar. Esto es crucial para abordar las debilidades en la infraestructura, los procesos o el personal que podrían haber contribuido al incidente.
- En muchos casos, hay obligaciones legales y regulatorias para investigar y notificar incidentes de ciberseguridad. Realizar una revisión post-incidente ayuda a la organización a cumplir con estas obligaciones y a demostrar su compromiso con la seguridad de los datos.

- La revisión post-incidente a menudo conduce a la actualización y el fortalecimiento de las políticas y procedimientos de seguridad. Esto puede incluir cambios en las políticas de contraseñas, en la gestión de accesos, en la capacitación de empleados y en la gestión de parches, entre otros.
- A medida que se identifican y se corrigen las debilidades, la organización se vuelve más preparada para futuros incidentes. Esto incluye la mejora de la capacidad de detección y respuesta a incidentes, así como la implementación de medidas preventivas más sólidas.

Gestión de la Reputación: La forma en que una organización maneja un incidente de ciberseguridad puede tener un impacto significativo en su reputación. Las actividades posteriores a un incidente, como la notificación a las partes afectadas y la comunicación transparente, ayudan a mantener la confianza del público y de los clientes.

Recopilación de Evidencia: En casos en los que sea necesario llevar a cabo acciones legales, como investigaciones criminales o litigios, las actividades posteriores ayudan a recopilar evidencia valiosa para apoyar los procedimientos legales.

Seguridad Proactiva: Las lecciones aprendidas de incidentes anteriores pueden ayudar a la organización a fortalecer su postura de seguridad antes de que ocurran futuros incidentes. Esto incluye la implementación de controles de seguridad más efectivos y la adopción de mejores prácticas de seguridad cibernética.

La siguiente tabla presenta algunos ejemplos de cómo realizar acciones posts incidentes teniendo presente el marco de trabajo Mitre ATT&CK[20].

Tabla 15

Relación de tácticas Mitre con ejemplos para el desarrollo de actividades post incidente

Táctica de MITRE ATT&CK	Ejemplo de Táctica	Actividades Posteriores al Incidente
Reconocimiento	Un atacante recopila información sobre la red objetivo.	Realizar una revisión exhaustiva de la exposición de información de la universidad y tomar medidas para reducirla. Actualizar las políticas de seguridad para limitar la información pública.
Ejecución	Un atacante ejecuta código malicioso en un sistema.	Identificar y detener el código malicioso en ejecución, luego eliminarlo de los sistemas afectados. Revisar y mejorar las políticas de ejecución de programas y control de acceso.

[20] https://attack.mitre.org/

Persistencia	Un atacante mantiene acceso persistente a un sistema.	Identificar y eliminar las puertas traseras y los mecanismos de persistencia utilizados por el atacante. Reforzar los controles de acceso y monitorear la actividad para detectar futuros intentos de persistencia.
Escalación de Privilegios	Un atacante aumenta sus privilegios en un sistema.	Identificar cómo se logró la escalada de privilegios y tomar medidas para cerrar las vulnerabilidades. Reforzar la autenticación y los controles de acceso.
Defensa y Evasión	Un atacante intenta evadir la detección y el análisis.	Mejorar las capacidades de detección y respuesta a incidentes para identificar técnicas de evasión. Reforzar las políticas de seguridad y la formación del personal.
Descubrimiento de Información	Un atacante busca información sensible o valiosa.	Evaluar el alcance del acceso a la información y notificar a las partes afectadas según sea necesario. Reforzar las políticas de seguridad de datos y la capacitación.
Movimiento Lateral	Un atacante se mueve lateralmente a través de la red.	Identificar el movimiento lateral y cerrar las rutas utilizadas por el atacante. Reforzar la segmentación de red y los controles de acceso.
Recolección de Información Sensible	Un atacante recopila información confidencial.	Determinar qué datos se recopilaron y notificar a las partes afectadas si es necesario. Reforzar las políticas de seguridad de datos y mejorar la detección de la exfiltración de datos.
Impacto	Un atacante causa daño a los sistemas o datos.	Evaluar el alcance del daño causado y tomar medidas para restaurar la operatividad normal. Realizar una revisión post-incidente exhaustiva y fortalecer las defensas para evitar futuros impactos.

Elaboración propia

Lecciones Aprendidas

La construcción de lecciones aprendidas después de un incidente de ciberseguridad se convierte en un insumo fundamental para mejorar la postura de seguridad de la Universidad y prevenir futuros incidentes similares. A

continuación se relacionan aspectos claves para tener en cuenta en esta etapa:

- Antes de poder aprender de un incidente, es fundamental tener una comprensión completa de lo que sucedió. Por tal motivo se debe documentar todos los aspectos del incidente, incluyendo cómo se detectó, las tácticas utilizadas por el adversario, el impacto en la Universidad y las medidas tomadas para responder.
- Indagar a fondo las causas subyacentes del incidente tales como:
    - ¿Cómo ocurrió el ataque? o
    - ¿Qué debilidades o vulnerabilidades se explotaron?

  Esta acción es crucial para abordar los problemas subyacentes.

- Revisar cómo se manejó el incidente desde su detección hasta su resolución, Identificando y documentando lo que funcionó bien y lo que podría haberse mejorado en términos de procesos, procedimientos y recursos.
- Destacar los aspectos positivos de la respuesta al incidente, reconozca las acciones efectivas y las mejores prácticas que se aplicaron durante el proceso de manejo del incidente, contribuyen el mantener motivado al equipo de trabajo y en presentar soluciones tempranas y efectivas que permitan cerrar las brechas explotadas por el adversario.
- Identificar las áreas en las que la respuesta al incidente podría haber sido más efectiva e incluir deficiencias en la detección, tiempos de respuesta prolongados o falta de capacitación y entrenamiento.
- Evaluar si las políticas y procedimientos de seguridad cibernética existentes son adecuadas o si necesitan ajustes, teniendo presente que los resultados se pueden reflejar en las lecciones aprendidas y las mejores prácticas de respuesta a incidentes.
- Generar espacios de educación en ciberseguridad a toda la comunidad UNADISTA y de entrenamiento a los equipos de respuesta a incidentes con el fin de abordar las áreas de mejora identificadas. Esto contribuirá en mejorar la conciencia de seguridad en toda la Universidad.
- Revisar y actualizar el plan de respuesta a incidentes de la organización en función de las lecciones aprendidas, teniendo presente que el plan refleje las mejores prácticas y las tácticas que usan los adversarios en términos de amenazas persistentes avanzadas - APT.
- Llevar a cabo ejercicios de simulacro de incidentes para practicar la respuesta a situaciones similares en el futuro, Esto con el fin de que la comunidad UNADISTA esté preparado para identificar y gestionar incidentes reales de manera efectiva.
- Compartir las lecciones aprendidas dentro de la Universidad para asegurarse de que todos los departamentos y equipos estén al tanto de las mejoras y cambios en las políticas y procedimientos de seguridad.
- Si es necesario, comunicar las lecciones aprendidas a las partes interesadas y/o comunidades objetivo, esto con el fin de mostrar un compromiso con la mejora de la seguridad de nuestro entorno digital.

Referentes Bibliográficos Usados

[1] https://repository.udistrital.edu.co/bitstream/handle/11349/7273/BocanegraDiazFabianEnrique2015.pdf;jsessionid=53311F646010F67DF7561D32F39B6165?sequence=1 (Pág. 25).

[2] https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf (Pág. 5)
[3] https://gobiernodigital.mintic.gov.co/692/articles-5482_G21_Gestion_Incidentes.pdf
[4] https://gpit.unad.edu.co/images/Documentos/Resolucin_7298_Mayo_2023_Marco_referencia_SGSI.pdf
[5] https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Plan_de_Comunicaciones_del_Incidente.pdf
[6] https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Plan_de_Comunicaciones_del_Incidente.pdf
[7] https://www.incibe.es/empresas/blog/primeros-pasos-respuesta-incidentes.
[8] https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Plan_de_Comunicaciones_del_Incidente.pdf.
[9] https://selloeditorial.unad.edu.co/images/2022/boletines-cip-csirt/Boletin_13.pdf.
[10] https://www.cisco.com/c/es_mx/support/docs/availability/high-availability/15117-sla.html#crea_slas.
[12] https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats.
[13] https://www.cloudflare.com/es-es/learning/ddos/dns-amplification-ddos-attack/.
[14] https://selloeditorial.unad.edu.co/images/2022/boletines-cip-csirt/Boletin_13.pdf.
[15] https://www.incibe.es/incibe-cert/sobre-incibe-cert/tlp.
[16] https://www.first.org/
[17] https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf.
[18] https://learn.microsoft.com/es-es/azure/architecture/serverless-quest/poc-pilot.
[19] https://www.cloudflare.com/es-es/learning/security/glossary/what-is-defense-in-depth/
[20] https://attack.mitre.org/

Anexo 1: Posibles tipos de eventos de ciberseguridad

Tipo de Evento	Descripción del Evento	Ejemplo del Evento	Impacto Potencial	Medidas de Prevención/Respuesta
Phishing	Engaño para que los usuarios revelen datos personales o credenciales.	Un email falso solicitando datos de acceso para verificar la cuenta del usuario.	Robo de identidad y acceso no autorizado a cuentas.	Educación de usuarios sobre identificación de correos fraudulentos.
Ransomware	Malware que cifra los datos del usuario y exige un rescate para desbloquearlos.	Software malicioso que bloquea el acceso a los archivos críticos de una empresa.	Pérdida de datos importantes, costos económicos elevados.	Copias de seguridad regulares, actualizaciones de software antivirus.
Data Breach	Acceso no autorizado a datos confidenciales.	Intrusión ilegal en la base de datos de clientes de una empresa.	Exposición de información sensible, multas legales.	Implementación de seguridad robusta en la red, auditorías de seguridad.
DDoS Attack	Inundación del sistema objetivo con tráfico para hacerlo inaccesible.	Sobrecarga de servidores web con solicitudes maliciosas.	Interrupción de servicios, pérdida de ingresos.	Protecciones contra DDoS, balanceo de carga.
Man-in-the-Middle (MitM)	Interceptación de la comunicación entre dos partes sin su conocimiento.	Interceptación de datos de una transacción de tarjeta de crédito en línea.	Robo de información financiera o personal.	Uso de conexiones HTTPS, VPN para transacciones seguras.
Malware	Software diseñado para infiltrarse o dañar un sistema sin el consentimiento del usuario.	Instalación de un keylogger en un sistema para registrar pulsaciones de teclas.	Daño a los sistemas, robo de información.	Actualizaciones regulares de seguridad, educación en ciberseguridad.

Ingeniería Social	Manipulación de individuos para que realicen acciones o revelen información confidencial.	Engaño para que un empleado revele contraseñas a través de una llamada falsa.	Acceso no autorizado, brechas de seguridad.	Capacitación de empleados en protocolos de seguridad.
Exploit de Software	Uso de vulnerabilidades de software para llevar a cabo ataques.	Explotación de un fallo en el sistema operativo para ganar control sobre un sistema.	Compromiso de sistemas, pérdida de control.	Parcheo y actualización de software regularmente.
Ataque de Fuerza Bruta	Intento de descifrar contraseñas o claves a través del ensayo sistemático.	Intentos repetidos de acceso a una cuenta usando diferentes combinaciones de claves.	Acceso no autorizado a cuentas y datos.	Uso de políticas de contraseñas fuertes, limitación de intentos de acceso.
SQL Injection	Inserción de código malicioso en bases de datos a través de aplicaciones web vulnerables.	Inyección de SQL en un formulario web para obtener acceso a la base de datos de usuarios.	Extracción no autorizada de datos.	Validación y sanitización estricta de entrada de datos en aplicaciones web.
Cross-Site Scripting (XSS)	Inserción de scripts maliciosos en sitios web para ejecutarlos en el navegador del usuario.	Publicación de un comentario en un sitio que contiene un script XSS que roba cookies de sesión.	Robo de sesiones y datos personales.	Implementación de políticas de Content Security Policy (CSP).
Spear Phishing	Phishing dirigido y personalizado hacia individuos específicos.	Email que parece venir de un colega solicitando información confidencial con detalles	Robo de información altamente sensible.	Verificación de la fuente antes de compartir información sensible.

		personales exactos.		
Ataques a la Cadena de Suministro	Ataques a través de software de terceros o proveedores comprometidos.	Malware introducido a través de una actualización de software de un proveedor comprometido.	Compromiso de múltiples sistemas a través de un único punto.	Evaluación de seguridad de terceros y gestión de riesgos.
Zero-Day Exploit	Explotación de una vulnerabilidad no conocida previamente por el software afectado.	Ataque que aprovecha una vulnerabilidad no parcheada recién descubierta en un navegador popular.	Amplio rango de compromiso antes de la detección.	Uso de software de detección de intrusiones y respuestas rápidas.
Ataque de Repetición	Reenvío malicioso o repetición de una transmisión válida de datos.	Captura y retransmisión de una solicitud de autenticación para acceder a un servicio como si fuera legítimo.	Acceso no autorizado a servicios.	Implementación de tokens de un solo uso y tiempos de expiración.
Ataque de Directorio	Navegación no autorizada y acceso a directorios o archivos.	Explotación de una configuración insegura en un servidor web para acceder a archivos confidenciales.	Pérdida de datos confidenciales.	Configuración adecuada de permisos y acceso a directorios.
Side-Channel Attack	Ataque basado en información obtenida de la implementación de un sistema.	Análisis de tiempos de ejecución de cifrado para determinar claves	Extracción de información crítica.	Uso de algoritmos y prácticas criptográficas robustas.

		privadas en una aplicación criptográfica.		
Ataque de Desconfiguración	Explotación de configuraciones defectuosas o inseguras de sistemas.	Acceso a un panel de administración de un sitio web a través de credenciales por defecto sin cambiar.	Compromiso total del sitio web y sus datos.	Revisión regular de configuraciones de seguridad y uso de auditorías.
Tampering	Modificación maliciosa de productos o software antes de su entrega o durante su uso.	Alteración de firmware de un dispositivo antes de su instalación en una red corporativa.	Introducción de vulnerabilidades y brechas de seguridad.	Inspección y validación de integridad de hardware y software.
Eavesdropping	Escucha clandestina de comunicaciones privadas.	Intercepción de transmisiones de Wi-Fi en un café para capturar datos de acceso.	Pérdida de privacidad, robo de datos.	Uso de redes seguras, VPN, y encriptación de comunicaciones.

Elaboración propia

Anexo 2: Gestión y Validación de un Incidente de Ciberseguridad