Guía Para la Gestión de Vulnerabilidades 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

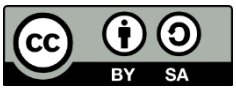
Grupo de Byte InDesign
Semillero de Investigación Ceros y Unos

Gerencia de Plataformas e Infraestructura Tecnológica - GPIT

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

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 de Vulnerabilidades de Ciberseguridad. Universidad Nacional Abierta y a Distancia - UNAD

La gestión de vulnerabilidades de ciberseguridad es fundamental para la Universidad Nacional Abierta y a Distancia (UNAD); esto debido a que contribuye en la protección de datos sensibles, reduce el riesgo de explotación y asegura la disponibilidad operativa.

Identificar y mitigar vulnerabilidades previene accesos no autorizados a información confidencial, salvaguardando la integridad y continuidad de los servicios educativos y administrativos. Cumplir con normativas como la Ley 1581 de 2012, la ley 1273 de 2009 y la resolución 1519 de 2020 del MINTIC, permiten dar una gestión robusta de vulnerabilidades y proteger la reputación y confianza de nuestra plataforma humana frente a nuestros aliados estratégicos, evitando así afectación reputacional y costos asociados a brechas de seguridad promoviendo una cultura cibernética proactiva.

En este sentido, adoptar mejores prácticas recomendadas por marcos como el NIST CSF y la ISO 27001, permite a la UNAD no solo prevenir ataques, sino también mejorar continuamente su postura de seguridad, adaptándose a las amenazas emergentes y fortaleciendo su resiliencia operativa en el entorno digital.

Establecer un proceso formal y estructurado para la gestión de vulnerabilidades 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 y minimiza la probabilidad de una explotación.

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 UNADSITA, se tiene presente:

Marco Legal

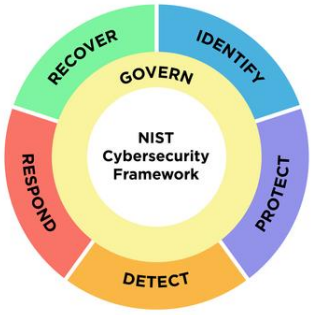
Tabla 1: Normatividad que se debe tener presente para la implementación del MSPI en la UNAD

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 del 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*"[1]

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

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.

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

- 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.

Gestión de las Vulnerabilidades de Ciberseguridad Presentadas en el Entorno Digital 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*"[2], la gestión de vulnerabilidades de ciberseguridad es un componente esencial en la protección de los sistemas de información y activos digitales de cualquier organización y es especialmente crucial para la Universidad Nacional Abierta y a Distancia- UNAD. A continuación, se explican las razones clave por las cuales la gestión de vulnerabilidades es vital:

Protección de Datos Sensibles y Confidenciales: Debido a que las vulnerabilidades pueden exponer datos sensibles a accesos no autorizados, comprometiendo la confidencialidad de la información. Para la UNAD, la protección de la información personal de los estudiantes, personal académico y administrativo, así como los datos institucionales, es de máxima prioridad

Reducción del Riesgo de Explotación: El Identificar y corregir vulnerabilidades minimiza las oportunidades para que los atacantes exploten puntos débiles en los sistemas. Esto debido a que en nuestro entorno digital que depende de sistemas digitales para la enseñanza y la gestión operativa, reducir el riesgo de explotación

Mantenimiento de la Disponibilidad Operativa: La gestión de vulnerabilidades previene interrupciones en los sistemas críticos causadas por ataques cibernéticos. En este sentido, La UNAD necesita asegurar la continuidad operativa para proporcionar una educación ininterrumpida a nuestros estudiantes y para soportar sus procesos administrativos. La identificación y mitigación de vulnerabilidades protegen contra interrupciones costosas y perjudiciales.

Cumplimiento Normativo y Legal: La gestión de vulnerabilidades ayuda a cumplir con las leyes y regulaciones sobre seguridad de la información.

Preservación de la Reputación y Confianza: Al mitigar vulnerabilidades, se protege la reputación de la organización y mantiene la confianza de sus partes interesadas. Cualquier brecha de seguridad puede dañar la confianza de nuestra comunidad, por tal motivo una

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

gestión robusta de vulnerabilidades demuestra un compromiso con la seguridad y la responsabilidad.

Alineación con las Mejores Prácticas de Ciberseguridad: La gestión de vulnerabilidades es una práctica recomendada por los principales marcos de ciberseguridad, como el NIST CSF[3] y la ISO 27001[4]. El adoptar estas mejores prácticas posiciona a la UNAD en un estándar alto de seguridad, reduciendo los riesgos y mejorando su resiliencia.

Prevención de Costos Asociados a Brechas de Seguridad: La gestión proactiva de vulnerabilidades previene perdida en costos financieros y operativos asociados con la recuperación de incidentes de seguridad. En este sentido, la UNAD puede evitar gastos significativos en la recuperación de datos, la reparación de sistemas y la mitigación de daños post-incidente, gracias a una gestión preventiva y eficaz de vulnerabilidades.

Facilitación de la Mejora Continua: El proceso continuo de identificación y remediación de vulnerabilidades permite mejorar constantemente la postura de seguridad. De esta forma la UNAD puede adaptarse a las nuevas amenazas y desafíos de ciberseguridad mediante la mejora continua basada en la gestión de vulnerabilidades, asegurando que sus sistemas y procesos estén siempre protegidos contra riesgos emergentes.

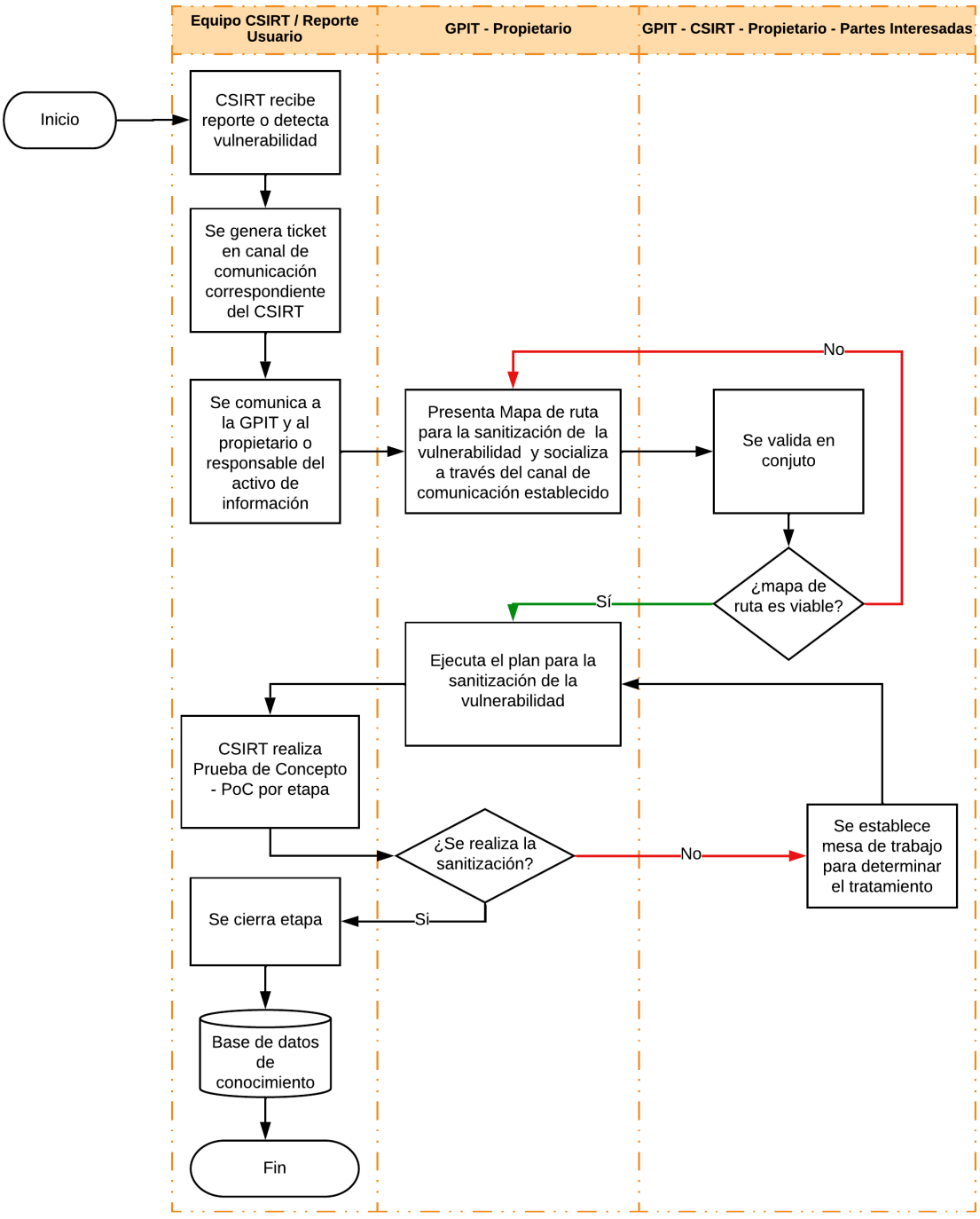
Fortalecimiento de la Cultura de Ciber seguridad: Implementar una gestión eficaz de vulnerabilidades fomenta una cultura organizacional de concienciación, educación y responsabilidad en ciberseguridad. Así, se promueve entre los estudiantes y la plataforma humana UNADISTA una comprensión profunda de la importancia de la seguridad digital y la responsabilidad de mantener un entorno seguro

Con base en lo anterior, la Universidad Nacional Abierta y a Distancia propone el siguiente esquema para la gestión de sus vulnerabilidades de seguridad y ciberseguridad.

[3] https://csrc.nist.gov/News/2023/nist-releases-cybersecurity-framework-2-0-draft
[4] https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion-2/

Identificación y Sanitización de Vulnerabilidades

Ruta para el tratamiento de una vulnerabilidad



Nota. * El diagrama de flujo proporcionado describe el proceso de identificación y gestión de vulnerabilidades por el CSIRT Académico UNAD. A continuación, se presenta un análisis de las etapas clave y los roles involucrados en el proceso:

Detección y Reporte de Vulnerabilidades: El CSIRT recibe reporte de un usuario o detecta una vulnerabilidad.

Responsable: Equipo CSIRT - Reporte de Usuario.

El reporte Puede ser notificado por un usuario o detectado por las acciones de monitoreo del CSIRT Académico UNAD.

Generación de Ticket: Se genera un ticket en el canal de comunicación correspondiente del CSIRT.

Responsable: Equipo CSIRT.

El ticket se utiliza para el seguimiento y la gestión de la vulnerabilidad.

Comunicación de la Vulnerabilidad: El CSIRT notifica la vulnerabilidad a la GPIT y al propietario o responsable del activo de información para que se tomen las acciones necesarias.

Responsable: Equipo CSIRT.

Socialización del Mapa de Ruta para la sanitización de la vulnerabilidad: El mapa de ruta es esencial para garantizar que todas las vulnerabilidades de ciberseguridad en la UNAD sean gestionadas de manera estructurada y documentada. Permite una planificación clara y detallada de las acciones necesarias para mitigar las vulnerabilidades y asegura que todos los actores relevantes estén informados y coordinados. Además, facilita la validación y seguimiento de la eficacia de las medidas implementadas, contribuyendo a la mejora continua de la seguridad de la información en la Universidad.

El uso e implementación de este mapa asegura la transparencia y la trazabilidad en el proceso de gestión de vulnerabilidades, alineándose con las mejores prácticas internacionales y las normas aplicables como el marco de trabajo NIST y la ISO 27001. Esto no solo mejora la postura de ciberseguridad de la UNAD, sino que también garantiza el cumplimiento de las normativas locales y el fortalecimiento de la resiliencia operativa.

En este sentido, el propietario del activo de información y la GPIT socializan el mapa de ruta para la sanitización de la vulnerabilidad y se comunica a través del canal de comunicación establecido. Esto con el fin de obtener retroalimentación para su ejecución

Responsable: GPIT - Propietario.

Validación del Mapa de Ruta para la Sanitización de la Vulnerabilidad: Se valida en conjunto si el mapa de ruta es viable.

Responsable: GPIT - CSIRT - Propietario - Partes Interesadas.

Si este esté es viable se procede con su ejecución, si no, se deberá ajustar y validar nuevamente

Ejecución del Plan de Sanitización: El plan de ejecución para la sanitización de la vulnerabilidad es fundamental ya que permite documentar de manera detallada y sistemática el avance de la ejecución del plan de sanitización de vulnerabilidades de ciberseguridad en la UNAD. Proporciona, además, una herramienta para monitorear y evaluar cada etapa del proceso de mitigación, asegurando que se logren los objetivos previstos y que cualquier desvío o imprevisto se registre adecuadamente. La implementación de este plan facilita la transparencia en la rendición de cuentas ya que cada actividad y su correspondiente resultado son documentados y revisados. Esto no solo garantiza que las vulnerabilidades se aborden de manera efectiva, sino que también promueve la mejora continua en los procesos de gestión de ciberseguridad. Además, al proporcionar un registro detallado de todas las acciones y evidencias, el plan asegura el cumplimiento con las normas y regulaciones internas y externas, contribuyendo a la resiliencia operativa y a la protección de los activos de información críticos de la universidad. En este sentido, se ejecuta el plan para el avance de la sanitización de una vulnerabilidad con el fin de corregirla.

Responsable: GPIT – propietario del activo.

Prueba de Concepto (PoC): En el contexto de la UNAD, donde la protección de la información y la continuidad operativa son factor fundamental, la PoC se convierte en un paso crítico para asegurar que las soluciones de seguridad implementadas sean efectivas, seguras y no disruptivas. Este enfoque proactivo y meticuloso en la gestión de vulnerabilidades contribuye significativamente a la resiliencia de la universidad frente a las amenazas cibernéticas.

En este sentido, El CSIRT realiza pruebas de concepto por etapa para validar la corrección de la vulnerabilidad, generando así su respectivo reporte.

Responsable: CSIRT Académico UNAD.

Si no se corrige la vulnerabilidad o se realiza la sanitización: Se establece una mesa de trabajo para determinar el tratamiento adicional.

Responsable: GPIT - CSIRT - Propietario.

En esta fase se realiza una planificación adicional y se ajustan las estrategias para resolver la vulnerabilidad.

Cierre del Proceso: Si la sanitización se realiza con éxito, se cierra la etapa y se registra en la base de datos de conocimiento y las lecciones aprendidas.

Responsable: CSIRT Académico UNAD - GPIT

Fin del Proceso: El proceso concluye una vez que la vulnerabilidad ha sido tratada y documentada.

Responsable: CSIRT - GPIT

Para un buen desarrollo en la identificación, reporte y sanitización de la vulnerabilidad, es preciso:

- Tener claridad y eficiencia en la respuesta ya que evita posibles confusiones y garantiza que cada persona involucrada tenga claro lo que debe hacer. Esto permite una respuesta más rápida y eficiente.
- Coordinar de forma efectiva la sanitización de la vulnerabilidad, el evento o el incidente ya la sinergia entre las partes involucradas se constituye en factor fundamental de la respuesta.
- Maximizar la utilización de recursos de tal forma que se pueda optimizar la utilización de lo que se tiene disponibles.
- Generar caneles de comunicación efectivos entre las partes involucradas agiliza la transmisión de información relevante durante el incidente. Una comunicación efectiva es crucial para tomar decisiones rápidas y precisas.
- Reducir errores, esto debido a que cada persona involucrada tiene un rol y un conjunto específico de responsabilidades.

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.

Proceso de Valoración y Evaluación de la Vulnerabilidad

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 una vulnerabilidad así:

Tabla 2

Nivel de severidad de la vulnerabilidad[5]

Alto Impacto	Indica que la vulnerabilidad puede afectar 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 la vulnerabildiad puede afectar activos de información asociados a los objetivos de un proceso del SIG

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

Bajo Impacto	Indica que la vulnerabilidad puede afectar activos de información considerados como menores o insignificantes. Se recomienda la monitorización constante de estos activos.

Priorización de la vulnerabilidad

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

Tabla 3

Criticidad del impacto que puede generar una vulnerabilidad

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 unidad o proceso
Medio	0,5	Activos de información que apoyan más de una unidad o proceso
Alto	0,75	Activos de información relacionados con los procesos de alto impacto o 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 puede tener la vulnerabilidad, indicando la gravedad y el alcance de los daños que pueda causar de llegar a ser explotada la vulnerabilidad. El nivel de impacto actual puede variar según el tipo de vulnerabilidad y la infraestructura o sistema afectado. A continuación, se relacionan algunos factores a considerar para determinar el nivel de impacto actual:

- Disponibilidad:
  - ¿la vulnerabilidad puede afectar la disponibilidad de los sistemas y servicios?
  - ¿Puede darse una interrupción en la operación normal?
- Integridad:
  - ¿Puede comprometerse la integridad de los datos o sistemas?
  - ¿Se podrían alterar o manipular de alguna manera?
- Confidencialidad:
  - ¿Se podría violar la confidencialidad de la información sensible?
  - ¿Se podría acceder o filtrar datos confidenciales?
- Alcance:
  - ¿La vulnerabilidad podría afectar a un sistema o a múltiples sistemas y/o redes?

    - ¿Puede impactar una unidad o a toda la universidad?
- Consecuencias:
    - ¿Qué tipo de daños se puede producir como resultado de un incidente?
    - ¿Podría presentarse pérdida de datos, pérdida financiera, interrupción de las operaciones u otras consecuencias significativas?

La evaluación del nivel de impacto actual de la vulnerabilidad es esencial para tomar decisiones informadas respecto a su mitigación y sanitización ya que esta brinda información para asignar recursos adecuados y el establecimiento de prioridades correctas para minimizar posibles efectos negativos con el fin de solucionar lo más rápido posible. La UNAD clasifica el nivel de impacto actual en cinco niveles:

Tabla 4

Descripción del nivel de impacto actual de la vulnerabilidad

Nivel	Valor	Definición
Inferior	0,1	Impacto leve en uno de los componentes de cualquier sistema de información
Bajo	0,25	Impacto moderado en uno de los componentes de cualquier sistema de información
Medio	0,5	Impacto alto en uno de los componentes de cualquier sistema de información
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 la vulnerabilidad 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 la vulnerabilidad si no se toman acciones correctivas. A continuación, se relacionan algunos factores que a considerar al determinar el nivel de impacto futuro:

- Propagación: ¿Puede existir el riesgo de que la vulnerabilidad permita la propagación a otros sistemas, redes o departamentos de la Universidad?
- Expansión: ¿Es posible que la vulnerabilidad se agrave y pueda causar daños adicionales o afecte a más usuarios o recursos críticos?
- Persistencia: ¿la vulnerabilidad puede persistir o prolongarse en el tiempo si no se toman las medidas adecuadas? ¿Puede haber un impacto continuo o recurrente?

- **Vulnerabilidades**: ¿Se han presentado vulnerabilidades conocidas o brechas de seguridad que podrían agravar la vulnerabilidad o dar lugar a un incidente?
- **Consecuencias a largo plazo**: ¿Cuáles podrían ser las implicaciones a largo plazo de la vulnerabilidad en términos de pérdidas financieras, daño reputacional o cumplimiento normativo?

La UNAD clasifica el nivel de impacto futuro en cinco niveles

Tabla 5

Descripción del Nivel de impacto futuro

Nivel	Valor	Definición
Inferior	0,1	Impacto leve en uno de los componentes de cualquier sistema de información
Bajo	0,25	Impacto moderado en uno de los componentes de cualquier sistema de información
Medio	0,5	Impacto alto en uno de los componentes de cualquier sistema de información
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 vulnerabilidades 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 y educación de la plataforma humana UNADISTA 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 vulnerabilidad en función de su impacto, criticidad y a otros factores relevantes. La prioridad que se debe dar a una vulnerabilidad se determina considerando varios factores, que pueden incluir:

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

- **Criticidad**: La gravedad de la vulnerabilidad y su potencial para causar daños significativos a la Universidad, como pérdidas financieras, interrupción de los servicios o violación de la seguridad.
- **Urgencia**: La necesidad de una acción inmediata para mitigar la vulnerabilidad. Algunas vulnerabilidades pueden requerir respuestas rápidas para evitar un mayor deterioro de la situación.
- **Alcance**: La extensión de la vulnerabilidad y su capacidad para afectar a múltiples sistemas, redes o usuarios. Vulnerabilidades 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 los servicios de la Universidad.

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

Tabla 6

Clasificación de los niveles de prioridad para dar respuesta a una vulnerabilidad

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 la vulnerabilidad 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.

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 sanitizar la vulnerabilidad 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 resolverla.

El tiempo de respuesta es crítico en la gestión de vulnerabilidad, ya que un retraso en la respuesta puede permitir que se genere un incidente.

El tiempo de respuesta eficaz se caracteriza por:

- Detectar la vulnerabilidad 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 de la vulnerabilidad comunicando a través de los canales establecidos.
- 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 sanitización y mitigación tan pronto como sea posible, para evitar que la vulnerabilidad se propague y pueda causar un daño. El **Formato de 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 la vulnerabilidad de manera efectiva.
- Realizar un seguimiento continuo de la vulnerabilidad a partir de lo planteado en el **Mapa de ruta para la sanitización de una vulnerabilidad** donde se implementan acciones correctivas con el fin de trabajar para su resolución completa en el menor tiempo posible.

El tiempo de respuesta puede variar según las políticas y los acuerdos de nivel de servicio (SLA)[6] establecidos por la Universidad, así como las capacidades y la preparación del equipo que dé respuesta a la vulnerabilidad. Es esencial establecer acciones realistas y contar con un plan de sanitización claro para garantizar una respuesta oportuna y eficiente.

La siguiente tabla, presenta el nivel de prioridad para dar respuesta a una vulnerabilidad de ciberseguridad

Tabla 7

Niveles de prioridad para dar respuesta a una vulnerabilidad

Nivel de prioridad	Valor (horas)	en Días
Inferior	96	4 hábiles
Bajo	96	4 hábiles
Medio	72	3 hábiles
Alto	48	2 calendario
Superior	24	1 calendario

Elaboración propia

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

Tiempo de respuesta para socializar la sanitización de la vulnerabilidad: Hace referencia al período durante el cual se llevan a cabo las actividades necesarias para eliminar completamente las amenazas y vulnerabilidades. 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

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 de la vulnerabilidad, pero es esencial para garantizar que los sistemas y datos estén completamente protegidos y seguros para seguir dando continuidad a las operaciones normales.

En este ejercicio se requiere documentar todo el proceso a partir del **Plan para el avance de la sanitización de la vulnerabilidad**.

Tabla 8

Tiempos estimados para socializar el mapa de ruta para la sanitización de la vulnerabilidad

Nivel de prioridad	en días hábiles	Entrega del Mapa de Ruta para la Sanitización de la vulnerabilidad a través del canal de comunicación establecido por el CSIRT
Inferior	4	
Bajo	4	
Medio	4	
Alto	4	
Superior	4	

Elaboración propia

Clasificación de la vulnerabilidad

La identificación de vulnerabilidades es fundamental para garantizar la seguridad y la resiliencia de nuestra infraestructura tecnológica. En un entorno cada vez más digitalizado, donde los ataques cibernéticos son una amenaza constante y creciente, comprender y catalogar las posibles debilidades de los sistemas es crucial. La identificación proactiva de vulnerabilidades permite anticiparnos a posibles incidentes, implementar medidas preventivas y reaccionar rápidamente ante cualquier brecha de seguridad. Es preciso indicar que esta práctica no solo protege los activos críticos y la información sensible, sino que también asegura la confianza de partes interesadas.

La siguiente tabla presenta como la UNAD clasifica sus vulnerabilidades en el proceso de gestión de vulnerabilidades.

Tabla 9

Clasificación de vulnerabilidades

Clasificación de Vulnerabilidad	Descripción	Ejemplos
Vulnerabilidades de Configuración	Configuraciones incorrectas o inseguras en sistemas, redes o aplicaciones que pueden ser explotadas.	Contraseñas por defecto no cambiadas Puertos abiertos innecesariamente Configuración de permisos demasiado permisiva
Vulnerabilidades de Autenticación	Deficiencias en los mecanismos de autenticación que permiten el acceso no autorizado.	Falta de autenticación de dos factores (MFA) Uso de contraseñas débiles Implementación incorrecta de OAuth o SSO
Vulnerabilidades de Autorización	Fallos en la gestión de permisos y privilegios que permiten a usuarios acceder a recursos o realizar acciones no autorizadas.	Elevación de privilegios Control de acceso insuficiente Errores en la implementación de roles y permisos
Vulnerabilidades de Inyección	Problemas que permiten la inyección de comandos o datos maliciosos en una aplicación, alterando su funcionamiento.	Inyección SQL (SQLi) Inyección de comandos en el sistema operativo Inyección de scripts entre sitios (XSS)
Vulnerabilidades de Seguridad en la Red	Vulnerabilidades que afectan la infraestructura de red, facilitando el acceso no autorizado o el tráfico malicioso.	Configuración incorrecta de firewalls o routers Falta de cifrado en el tráfico de red Ataques de hombre en medio (Man-in-the-Middle) Baja seguridad entre VLANs
Vulnerabilidades en Software de Terceros	Vulnerabilidades presentes en software de terceros utilizado dentro de la Universidad.	Uso de librerías con vulnerabilidades conocidas Fallos en plugins o módulos de software Dependencias desactualizadas
Vulnerabilidades de Seguridad Física	Deficiencias en los controles físicos que permiten el acceso no autorizado a instalaciones o equipos.	Falta de control de acceso físico Equipos sensibles dejados sin supervisión Sistemas de vigilancia inadecuados

Vulnerabilidades de Ingeniería Social	Vulnerabilidades que explotan la confianza o el error humano para obtener acceso no autorizado.	Phishing (suplantación de identidad para robar credenciales) Pretexting (uso de una historia falsa para obtener información) Baiting (ofrecimiento de algo tentador para obtener información o acceso)
Vulnerabilidades de Seguridad en la Aplicación	Deficiencias en la seguridad de aplicaciones que permiten la ejecución de acciones no autorizadas.	Fallos en la gestión de sesiones Validación insuficiente de entradas del usuario Exposición de datos sensibles
Vulnerabilidades de Seguridad en el Sistema Operativo	Vulnerabilidades dentro del sistema operativo que permiten la explotación de recursos o la ejecución de código malicioso.	Desbordamiento de búfer Uso de funciones inseguras Errores en la gestión de memoria
Vulnerabilidades de Criptografía	Fallos en la implementación o el uso de mecanismos criptográficos que comprometen la seguridad.	Cifrado débil o inseguro Uso de algoritmos criptográficos obsoletos Mala gestión de claves
Vulnerabilidades de Denegación de Servicio (DoS)	Deficiencias que permiten que un atacante interrumpa la disponibilidad de servicios o sistemas.	Ataques de sobrecarga de red (flooding) Explotación de fallos en la gestión de recursos Vulnerabilidades en protocolos de red

Relación de las Vulnerabilidades con el marco de trabajo Mitre

El marco de trabajo MITRE, a través de su base de datos CVE (Common Vulnerabilities and Exposures) y su matriz ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), juega un papel crucial en la clasificación y comprensión de las vulnerabilidades.

A continuación, se detalla la relación entre la clasificación de vulnerabilidades y estos componentes del marco MITRE:

CVE[7] (Common Vulnerabilities and Exposures): La base de datos CVE es un sistema de referencia estándar que proporciona identificadores únicos para vulnerabilidades conocidas.

[7] https://cve.mitre.org/

Cada CVE incluye información detallada sobre una vulnerabilidad específica, como su descripción, impacto y soluciones recomendadas. La clasificación de vulnerabilidades utiliza CVE como una base fundamental para identificar y catalogar vulnerabilidades específicas

Mitre ATT&CK Framework[8] (Adversarial Tactics, Techniques, and Common Knowledge): Es un marco detallado que categoriza y describe tácticas, técnicas y procedimientos (TTPs) utilizados por atacantes en el mundo real. Está diseñado para ayudar a entender cómo operan los atacantes y a mejorar su capacidad para defenderse. La matriz ATT&CK proporciona un contexto rico sobre cómo las vulnerabilidades pueden ser explotadas en escenarios de ataque reales.

La siguiente tabla presenta algunos ejemplos.

Tabla 10

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

Táctica de MITRE ATT&CK	Ejemplo de Táctica
Reconocimiento	Un atacante recopila información sobre la red objetivo.
Ejecución	Un atacante ejecuta código malicioso en un sistema.
Persistencia	Un atacante mantiene acceso persistente a un sistema.
Escalación de Privilegios	Un atacante aumenta sus privilegios en un sistema.
Defensa y Evasión	Un atacante intenta evadir la detección y el análisis.
Descubrimiento de Información	Un atacante busca información sensible o valiosa.
Movimiento Lateral	Un atacante se mueve lateralmente a través de la red.
Recolección de Información Sensible	Un atacante recopila información confidencial.
Impacto	Un atacante causa daño a los sistemas o datos.

Elaboración propia

Reporte de una vulnerabilidad

El Reporte de una vulnerabilidad de Ciberseguridad de la UNAD es un paso crucial que permite la recopilación y análisis sistemático de la información. Este ayuda a gestionar y mitigar los riesgos asociados de manera eficiente.

A continuación, se detalla que datos son requeridos en el momento de generar un reporte:

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

Información General del Reporte:

- Reporte N°: Número de identificación único asignado al reporte por el CSIRT.
- TLP (Traffic Light Protocol): Nivel de confidencialidad del reporte basado en el protocolo de semáforo (Rojo, Ámbar, Verde), que define cómo se debe manejar y compartir la información.

Fecha de elaboración del reporte: Fecha en la que se genera el reporte.

Detalles de Contacto de quien reporta:

- Nombre de quien reporta: Persona que realiza el reporte.
- Rol: Rol o posición de quien reporta.
- Celular y/o Teléfono: Información de contacto.
- Correo Electrónico: Detalles adicionales para facilitar la comunicación.

Información del Activo Afectado:

- Fecha y hora del descubrimiento: Momento en el que se identificó la vulnerabilidad.
- Unidad: Departamento o unidad afectada por el evento.
- Responsable del activo: Persona encargada del activo de información comprometido.
- Tipo y Nombre del Activo: Clasificación y denominación específica del activo.
- IP y Ubicación: Dirección IP y ubicación física del activo.
- Tipo de activo (Magerit): Clasificación del activo según el esquema Magerit[9].
- Nivel de riesgo: Categoría del activo en la tabla de riesgos máximos.

Descripción del Activo o Servicio:

- Descripción detallada: Información completa sobre el activo o servicio afectado.
- Método de detección: Forma en que se identificó la vulnerabilidad o evento (seleccionable).

Evaluación del Impacto:

- Impacto financiero: Posible impacto financiero del evento.
- Impacto reputacional: Evaluación del daño potencial a la reputación de la universidad.
- Impacto operacional: Posibles efectos en las operaciones de la UNAD.
- Impacto legal: Riesgo de consecuencias legales debido al evento.

Priorización y Tiempo de Respuesta:

---

9 https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

- Clasificación de la Vulnerabilidad: Grado de severidad de la vulnerabilidad.
- Nivel de impacto actual y futuro: Evaluación del impacto presente y potencial.
- Criticidad del sistema: Importancia del sistema afectado.
- Prioridad: Nivel de prioridad para responder al evento.
- Tiempo de respuesta: Tiempo estimado para la respuesta y resolución.

Explotación Potencial:

- Táctica(s) y Técnica(s): Métodos que podrían ser usados para explotar la vulnerabilidad.

Acciones y Seguimiento:

- Acciones realizadas: Medidas tomadas en respuesta al evento o vulnerabilidad.
- Lecciones aprendidas: Conocimientos obtenidos que pueden mejorar futuras respuestas.
- Archivos adjuntos: Evidencias o documentos relacionados con el evento

Plan de Acción para el avance de la sanitización de la vulnerabilidad

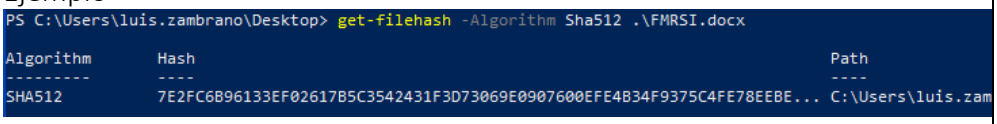
A continuación, se detalla que información aporta en la sanitización de la vulnerabilidad al tener como base un plan de acción para sanitizar o mitigar la vulnerabilidad:

Información Inicial	
Reporte N°	Indica el número de reporte asignado por el CSIRT Académico UNAD en su mesa de ayuda. Este dato lo brinda el CSIRT
TLP (Traffic Light Protocol)[10] :	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[11] 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

[10] https://www.incibe.es/incibe-cert/sobre-incibe-cert/tlp
[11] https://www.first.org/

	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:GREEN : 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
Fecha de elaboración del reporte:	Se debe indicar la fecha y hora en la que se construye el reporte
Propietario responsable del activo de información	Se debe indicar el nombre del responsable del activo de información
Nombre del activo	Se debe indicar el nombre del activo tal como se encuentra relacionado en el inventario de activos de información
Actores que interviene en el proceso de sanitización (interno - externo)	
Nombres	Se debe indicar los nombres de los expertos que intervienen en el proceso de sanitización del incidente
Dependencia	Se debe indicar la dependencia en la que está relacionado el experto. Si esté es personal externo, se debe indicar la empresa
Correo electrónico	Se debe indicar el correo electrónico institucional
Experticia en la solución del evento	Se debe indicar la experticia de cada uno de los expertos que están apoyando el proceso de sanitización del incidente
Actividades	
Etapa	Se debe indicar la etapa correspondiente al informe (1,2, PoC)
Fecha propuesta para iniciar el proceso	Se debe indicar la fecha de inicio programada en el formato de mapa de ruta para la sanitización de la vulnerabilidad de ciberseguridad correspondiente a la actividad

de respuesta	
Fecha real de inicio	Si la actividad presenta diferencia en las fechas planteadas de forma inicial, indique la fecha real en la que se inició la ejecución de está
Fecha propuesta para el cierre de la etapa	Se debe indicar la fecha de cierre programada en el formato de mapa de ruta para la sanitización de la vulnerabilidad de ciberseguridad correspondiente a la actividad
Fecha real del cierre de la etapa	Si la actividad presenta diferencia en las fechas planteadas de para el cierre, indique la fecha real en la que se cerró la ejecución de está
% de proceso de recuperación esperado	Se debe indicar en una escala de 1 a 100 con avances de a 10 el estado de sanitización, según lo planeado en el formato de mapa de ruta para la sanitización de la vulnerabilidad de ciberseguridad
% de recuperación real	Se debe indicar en una escala de 1 a 100 con avances de a 10 el estado de recuperación real para la vulnerabilidad del evento.
	Indique las actividades realizadas
Resultados esperados	Indique los resultados esperados según lo planeado en el formato de mapa de ruta para la sanitización de la vulnerabilidad de ciberseguridad
Resultados obtenidos	Indique los resultados obtenidos reales
Imprevistos, dificultades o éxitos presentadas	Se deben relacionar los imprevistos, dificultades o éxitos presentados en la ejecución de la actividad
Evidencias del proceso de sanitización	
Nombre de la evidencia	Se debe indicar el nombre de la evidencia que se presenta al finalizar cada una de las actividades
Tipo de evidencia	Se debe indicar el tipo de evidencia (Física o Digital)
Ubicación	Si es digital, esta deberá reposar en el sistema indicado por el CSIRT Académico UNAD Si es física, se deberá indicar en que parte locativa de la Universidad se encuentra ubicada.
Hash del archivo	Si es digital indique el Hash de la evidencia.

	Para la generación del HASH puede hacer uso de la librería de Windows GETFileHash a través de PowerShell (tenga presente situarse en la ruta donde se encuentra el archivo) Instrucción: get-filehash -Algorithm Sha512 .\ Ejemplo 
Firma de quien diligencia el formato	El responsable de la actividad post incidente deberá firmar el formato correspondiente

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.

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
inferio	Afecta a los sistemas de la organización
	Interrupción de la prestación de un servicio
	Daños reputacionales puntuales, sin eco mediático

Elaboración propia

Lecciones Aprendidas

La gestión efectiva de una vulnerabilidad de ciberseguridad no solo resuelve el problema inmediato, sino que también ofrece valiosas lecciones que pueden fortalecer la postura de seguridad de una organización a largo plazo. A continuación, se presentan algunas lecciones clave que pueden derivarse de una correcta gestión de vulnerabilidades, especialmente en el contexto de una institución educativa como la Universidad Nacional Abierta y a Distancia:

- Importancia de la Detección Temprana y la Monitorización Continua:
- Eficiencia de los Protocolos de Respuesta
- Valor de la Comunicación Clara y Coordinada
- Necesidad de la Documentación Detallada
- Beneficio de la Evaluación Post-Incidente
- Necesidad de la Capacitación Continua
- Efectividad de las Medidas Preventivas
- Importancia de la Evaluación de Riesgos
- Fomento de una Cultura de Seguridad
- Integración de Mejores Prácticas y Estándares
- Capacidad de Adaptación a Amenazas Emergentes

Referentes Bibliográficos Usados

[1] https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

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

[3] https://csrc.nist.gov/News/2023/nist-releases-cybersecurity-framework-2-0-draft

[4] https://www.icontec.org/eval_conformidad/certificacion-iso-27001-sistemas-de-gestion-de-seguridad-de-la-informacion-2/

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

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

[7] https://cve.mitre.org/
[8] https://attack.mitre.org/
[9] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

[10] https://www.incibe.es/incibe-cert/sobre-incibe-cert/tlp

[11] https://www.first.org/