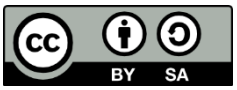
Plan de Comunicaciones del Incidente de Ciberseguridad

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

Modelo de Seguridad
y Privacidad de la Información



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

Grupo de Byte InDesign
Semillero de Investigación Ceros y Unos

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Andrés Ernesto Salinas Duarte
Vicerrector de Innovación y Emprendimiento

Luis Fernando Zambrano Hernández
Líder CSIRT Académico UNAD

Yenny Stella Nuñez Alvarez
Analista 1

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	Plan de Comunicación del Incidente de Ciberseguridad. Universidad Nacional Abierta y a Distancia - UNAD

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".*[1] En este sentido la comunicación de un Incidente en la UNAD puede ser realizado teniendo presente este documento, el cual define lineamientos para la comunicación del incidente basado en lo que debe ser comunicado partes interesadas.

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

[1] https://www.incibe.es/empresas/blog/primeros-pasos-respuesta-incidentes

Glosario de Términos:

Activos de Información: Cualquier componente (humano, tecnológico, software, manuales, documentos físicos y electrónicos, entre otros) que tiene importancia para la organización y signifique riesgo si llega a manos de personas no autorizadas al manejo de esta.

Base de Datos: Conjunto de datos almacenados y organizados en medios físicos o electrónicos con el fin de facilitar su tratamiento, acceso y recuperación.

Ciberseguridad: Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados

Ciberdefensa: Conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición.

Criticidad: importancia o gravedad de una vulnerabilidad, amenaza o incidente en relación con los activos de información de una organización.

CSIRT: Computer Security Incident Response Team (Equipo de respuesta a incidentes de seguridad cibernética).

CSIRT Académico: Computer Security Incident Response Team (Equipo de respuesta a incidentes de seguridad cibernética) que atienden comunidades académicas, universidades, facultades, escuelas o institutos.

Comunicación del incidente: "*Toda violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos física o automatizada administrada por el responsable del tratamiento o por su encargado que genere algún riesgo al titular de la información debe ser reportada a la SIC*"[2].

Copias de respaldo o Backups: Copia que se realiza a la información institucional definida como importante, sensible o vulnerable; con el fin de utilizarla posteriormente para restablecer el original ante de una eventual pérdida de datos, para continuar con las actividades rutinarias y evitar pérdida generalizada de datos.

Dato sensible o vulnerable: También llamado activo sensible, es el nombre que recibe la información personal o institucional de carácter confidencial y particularmente autorizada por su propietario del activo (datos personales, información financiera, contraseñas de correo electrónico, domicilio, datos de investigaciones).

[2] https://www.sic.gov.co/sites/default/files/eventos/memorias/presentaci%C3%B3n%20Incidentes%20Final-Autorizada.pdf

Dato Origen: Elemento inicial para la construcción de información o conocimiento, susceptible de protección y control.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Se clasifican:

Dato personal público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Dato personal privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. Tienen esta naturaleza los gustos o preferencias de las personas.

Dato Semiprivado: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento interesa no sólo a su titular sino a cierto sector o grupo de personas. (Por ejemplo, cuando se trata de los datos financieros o crediticios.)

Dato sensible: Es aquel que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, organizaciones de derechos humanos o que promuevan intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos, entre otros.

Incidente: Hace referencia a cualquier evento o suceso que tenga un impacto negativo en la seguridad de los sistemas informáticos o la información que contienen.

Oficial de Seguridad: Profesional responsable de alinear las iniciativas de seguridad con los objetivos misionales, garantizando que los bienes y las tecnologías de la información estén adecuadamente protegidas.

Propietario: Individuo que se le otorga la propiedad del activo y del riesgo del mismo en cada una de las unidades estratégicas, divisiones organizacionales, gerencias, rectorías o vicerrectorías.

RBAC: mecanismo de control de acceso que define los roles y los privilegios para determinar si a un usuario se le debe dar acceso a un recurso.

Seguridad de la Información: Son todas aquellas medidas proactivas, preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información.

SOC: Security Operations Center. El Centro de Operaciones de Seguridad emplea personas, procesos y tecnología para monitorear y mejorar continuamente la postura de ciberseguridad y ciberdefensa de una organización mientras previene, detecta, identifica, protege, contiene, analiza, responde y se recupera a un incidente de ciberseguridad.

Titulares de la Información: "*La comunicación a los Titulares de la Información brinda la oportunidad para que ellos mismos puedan adoptar las medidas necesarias para protegerse de las consecuencias de un incidente de seguridad, Por ejemplo, cambiar su nombre de usuario y contraseña; monitorear su historial crediticio; cancelar su tarjeta de crédito*" [5]

V-SOC: Virtual Security Operations Center.

Usuarios: Entiéndase por aquel que hace uso de alguno de los sistemas que la universidad provee (Académico, Directivo, Administrativo, Operativo o de Gestión), mediante la asignación de un usuario y una contraseña

Ventana Temporal: Hace referencia a un período de tiempo específico durante el cual un sistema o una red se considera vulnerable o expuesto a una posible explotación. Durante esta ventana temporal, los administradores de seguridad son conscientes de una vulnerabilidad o debilidad en el sistema, pero aún no se ha aplicado una solución o parche para corregirlo.

Objetivo:

Proveer el plan para la comunicación de cualquier incidente que afecte la ciberseguridad, con el fin de informar a partes interesadas y minimizar el impacto legal y reputacional que esté presente.

Alcance:

El plan de comunicaciones del incidente aborda 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).

La definición de los canales de comunicación a utilizar, para transmitir la información relacionada con el incidente. (prensa nacional e internacional, correo electrónico, reuniones informativas, actualizaciones en el sitio web de la Universidad, redes sociales, entre otros).

El establecimiento de los mensajes que deben ser comunicados a partes interesadas, con el fin de garantizar una comprensión precisa del incidente y las medidas tomadas para abordarlo.

La definición de plazos para notificar a las partes interesadas sobre el incidente, estableciendo quién es el responsable de la comunicación, qué información debe proporcionar y en qué momento debe realizar las respectivas actualizaciones.

Contenido

Marco Legal, Normatividad y Estándares

Para la construcción del Plan de Comunicaciones del Incidente de Ciberseguridad 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
CONPES	
CONPES 3854 de 2016	Política Nacional de Seguridad digital
Otros documentos	
Guía 21 MINTIC	Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información

Esquema de Intercambio de Información

Indica el nivel de confidencialidad del reporte o publicación. A continuación, se relaciona el código de colores aprobado actualmente por FIRST[3]

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

Escala definida por la UNAD para la notificación de un incidente de Ciberseguridad

La guía para la Gestión y Clasificación de un evento o incidentes de Cibserguridad UNADSITA presenta el nivel de criticidad del impacto de un incidente y su respectivo nivel de prioridad

Nivel de Criticidad

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

Nivel 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: Guía para la Gestión y Clasificación de un evento o incidente

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

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 2

Tabla 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 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

Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

Nota.* Una tabla de riesgos máximos se presenta como instrumento crucial para la gestión eficaz de incidentes de seguridad. Esta herramienta permite a la Universidad priorizar y clasificar los ciberincidentes según su impacto potencial y probabilidad de ocurrencia. Al identificar claramente los riesgos más significativos, se facilita la toma de decisiones rápidas y adecuadas, garantizando una respuesta oportuna y eficiente ante amenazas críticas, con el fin de focalizar los recursos de manera óptima y elaborar planes de mitigación específicos para los escenarios de mayor riesgo.

Nivel de peligrosidad del incidente

A partir de lo anterior y con base en lo propuesto por la Guía Nacional de Notificaciones y Gestión de Ciber incidentes del Gobierno de España[4], la UNAD establece los criterios para la determinación del nivel de peligrosidad de un incidente así:

Tabla de Nivel de Peligrosidad del Incidente		
Nivel	Clasificación	Tipo de Incidente
Superior	Amenaza Persistente Avanzada	APT[5]
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[6] Criptografía débil
Bajo	Contenido abusivo	Spam
	Obtención de información	Análisis de paquetes - Escaneo de red
	Otros	Otros

Recuperado de: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

4 https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

5 https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats

6 https://www.cloudflare.com/es-es/learning/ddos/dns-amplification-ddos-attack/

Comunicación de Incidente de Ciberseguridad

La UNAD establece su plan de comunicación del incidente de ciberseguridad a partir de: Toda violación de la seguridad o la pérdida, robo y/o acceso no autorizado a la información contenida en una base de datos física o digital que genere algún riesgo al titular de la información. Esta, deberá ser reportada ante el ente de control correspondiente.

Titulares de la información

La UNAD reconoce como titular de la información a toda persona natural o jurídica a quien se refiere la información que reposa en sus bases de datos.

¿Cómo comunicar el incidente?

La UNAD establece los siguientes canales de comunicación para el reporte de un incidente:

- Correo: seguridad.informacion@unad.edu.co
- Línea telefónica: 601 - 3443700 ext. 1687

Una vez reportado el incidente, el oficial de seguridad adscrito al equipo funcional de seguridad de la Universidad informará a:

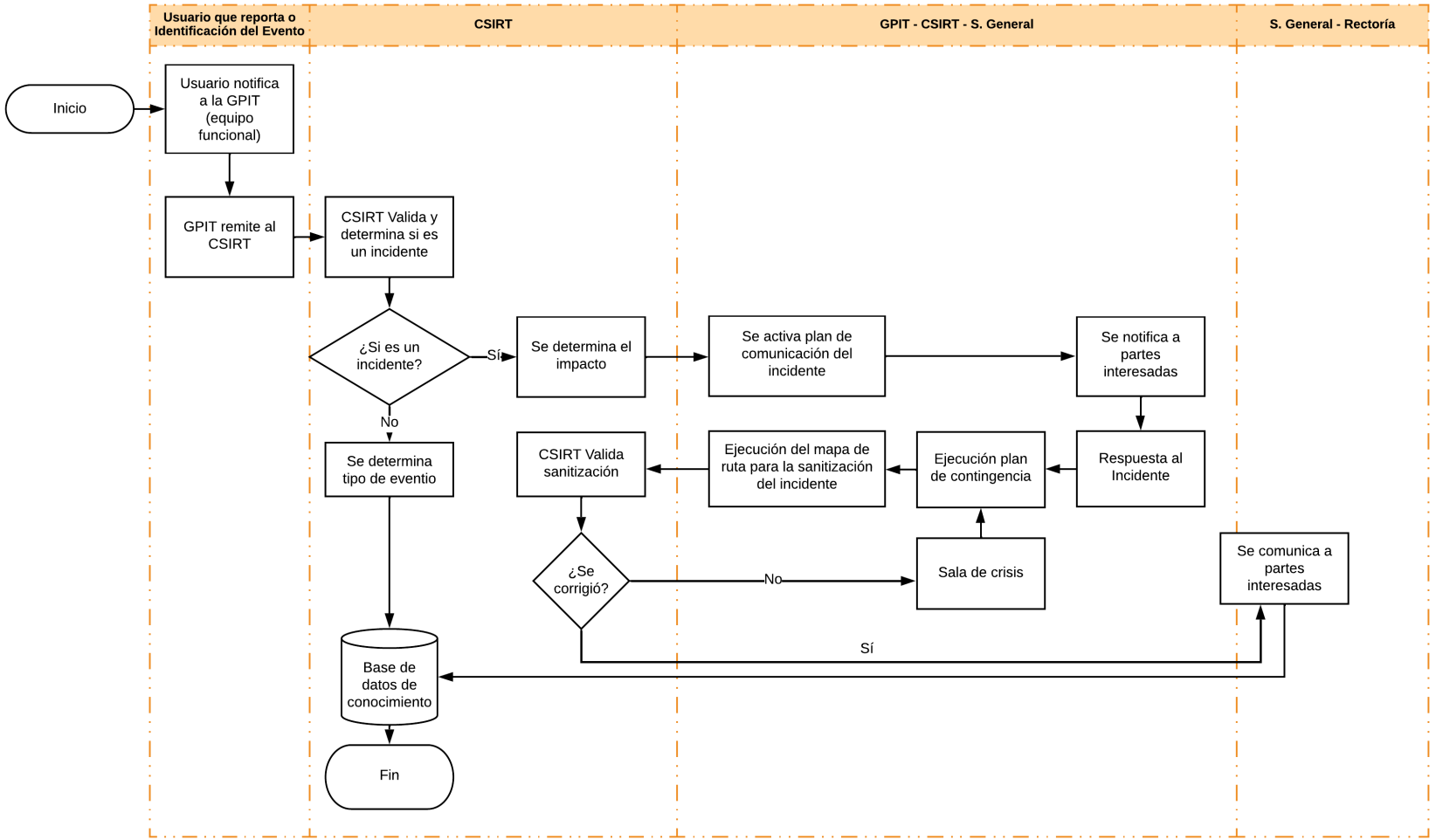
- Secretaria general (Custodio de la Inforamción)
- Gerencia de Plataformas e Infraestructura Tecnológica
- CSIRT Académico UNAD
- Propietario del activo de información

Esto con el fin de dar inicio a la mitigación, respuesta al incidente y el establecimiento de comunicación con partes interesadas.

Si por algún motivo el incidente fue reportado a otra Unidad o funcionario de la Universidad, esté deberá ser reportado a los canales de comunicación oficiales para dar tramité al mismo.

El siguiente diagrama de flujo, presenta la ruta para la activación del plan de comunicación del incidente

Ilustración 1: Plan de comunicación del incidente



Elaboración propia

Canal de comunicación para socializar el estado de avance del incidente

La UNAD establece los siguientes canales de comunicación oficiales para informar a los titulares de la información, como se encuentra el estado de contención y recuperación del incidente. A continuación, se relacionan los medios:

Masivo o General	Personal
https://www.unad.edu.co https://csirt.unad.edu.co Medios de comunicación nacional o internacional	Correo Electrónico institucional Correo electrónico personal reportado y autorizado para ser tratada su información

La información suministrada será compartida con titulares y partes interesadas según sea el caso:

- Reporte de un incidente de ciberseguridad ante la Universidad
- Reporte de un incidente de ciberseguridad ante entes de control Externo
- Comunicación del incidente a titulares de la información
- Comunicación del incidente a medios de comunicación
- Comunicación de una sospecha de actividad de ciberseguridad inusual a medios de comunicación
- Comunicación de una sospecha de actividad de ciberseguridad inusual a titulares de la información
- Socialización de la recuperación y retorno a las operaciones

Para la comunicación del incidente se tiene en cuenta el nivel de criticidad, el riesgo máximo y el nivel de peligrosidad. La siguiente tabla muestra cuando, como, quien y que se debe comunicar respecto al incidente de ciberseguridad.

	Superior	Alto	Medio	Bajo	Inferior
¿Cuándo comunicar?	Entre el primer y tercer día	Entre el primer y octavo día	Entre el primer y el quinceavo día	No requiere comunicación a partes interesadas	No requiere comunicación a partes interesadas
¿Cómo comunicar?	A través de los canales de comunicación establecidos	A través de los canales de comunicación establecidos	A través de los canales de comunicación establecidos	A través del canal de comunicación y notificación establecido por el CSIRT	A través del canal de comunicación y notificación establecido por el CSIRT
¿Quién debe comunicar?	GPIT - Secretaría General – VIEM - Rectoría	GPIT - Secretaría General – VIEM -Rectoría	GPIT - Secretaría General – VIEM - Rectoría	CSIRT Académico UNAD	CSIRT Académico UNAD
¿Qué debe incluirse en la comunicación?	Tipo de incidente Información comprometida Recomendaciones	Tipo de incidente Información comprometida Recomendaciones	Tipo de incidente Información comprometida Recomendaciones	Tipo de incidente Recomendaciones	Tipo de incidente Recomendaciones

*Los tiempos se inicializan a partir de la confirmación del incidente por parte del CSIRT Académico UNAD

Organismos o entes de control externos a los que se deberá o podrá reportar un Incidente

A continuación, se relacionan los entes de control a los que se debe reportar un incidente teniendo en cuenta el ¿Por qué se debe reportar?

Órgano	URL	¿Por qué se debe reportar?
ColCERT	https://www.colcert.gov.co/800/w3-channel.html	Ataques cibernéticos que afecten la continuidad del negocio de la Universidad. Resolución 500 de 2021
SIC[7]	https://www.sic.gov.co/content/reporte-de-incidentes-de-seguridad	Fuga de datos de bases de datos reportadas en RNBD
Policía Nacional	https://www.policia.gov.co/denuncia-virtual/delitos-informaticos	Reporte voluntario

¿Cuándo reportar?: "Hasta 15 días después de confirmado el incidente por el CSIRT Académico UNAD

¿dónde reportar?: A través de los canales de comunicación establecidos por la Universidad o por los entes de control

¿Quién debe reportar?: Rectoría o a quien delegue el Sistema de Alta Dirección de la Universidad

¿Qué debe incluir el reporte?

El reporte debe incluir:

Información Inicial	
Reporte N°	Indica el número de reporte asignado por el CSIRT Académico. Este dato lo brinda el CSIRT
TLP (Traffic Light Protocol)[8]:	Indicar el TLP según el caso
Fecha de elaboración del reporte:	Se debe indicar la fecha y hora en la que se construye el reporte
¿El incidente se había presentado?	Se debe indicar si el incidente se había presentado de forma previa.
Datos de contacto CSIRT Académico UNAD o Persona Quien Reporta el Incidente	
Nombre de quien reporta	Se debe indicar el nombre del analista, funcionario o persona quien está reportando el incidente
Rol:	Se debe indicar el rol que desempeña dentro o fuera de la universidad, quien está realizando el reporte
Celular / teléfono	Se debe indicar el número telefónico de contacto (celular o teléfono)
Correo electrónico	Se debe indicar el correo electrónico institucional
Datos de contacto Unidad que presenta el Incidente	
Fecha y hora del descubrimiento	Se debe indicar la fecha y hora del descubrimiento del incidente

[7] Super Intendencia de Industria y Comercio
[8] https://www.incibe.es/incibe-cert/sobre-incibe-cert/tlp

Unidad	Se debe indicar la unidad responsable del activo de información
Responsable del activo	Se debe indicar el nombre del responsable del activo de información (Quien administra le administra)
Celular / teléfono	Se debe indicar el número telefónico de contacto (celular o teléfono)
Correo electrónico	Se debe indicar el correo electrónico institucional
Activo de Información Afectado	
Nombre del activo	Se debe indicar el nombre del activo tal como se encuentra relacionado en el inventario de activos de información
Dirección IP	Indique la URL o dirección IP donde se encuentra en servicio el activo de información
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
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
Ubicación en la 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
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
Debido al incidente	Se debe indicar con respuesta afirmativa o negativa 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
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
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
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

Técnica	Se debe indicar la técnica asociada con la táctica propuesta por el marco de trabajo de Mitre ATT&CK
Nivel de Prioridad:	
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
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)
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
Prioridad	El nivel de prioridad esta dado por la formula: **Nivel Prioridad = (Impacto actual * 2,5) + (Impacto futuro * 2,5) + (Criticidad del Sistema * 5)**
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
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
Impacto	Luego de la indagación inicial se debe determinar si se presentó impacto de orden: • Financiero • Reputacional • Operacional • Legal
Acciones realizadas	Se debe indicar de forma detallada las acciones realizadas en el momento para la comunicación y respuesta al incidente. Algunas acciones de ejemplo 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 el sistema de alta política. • 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 teniendo presente el **Plan de Comunicación del Incidente**. Esto puede incluir medios de comunicación
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 partes 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.
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.
Archivos adjuntos	Indique los archivos adjuntos. Estos deberán encontrarse en el sitio que determine el CSIRT Académico UNAD para su gestión y consulta

Esté se construye teniendo como base lo planteado por INCIBE[9]

[9] https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

Ventana Temporal del Reporte

Todo incidente que sea obligado a reportar ante una autoridad competente, se debe hacer teniendo en cuenta la siguiente tabla:

	Notificación Inicial (Proceso de Contención)	Notificación Intermedia (Proceso de Erradicación)	Notificación final (Proceso de Recuperación y PoC)
Superior	Entre el primer y tercer día	Según lo establecido	Según lo establecido
Alto	Entre el primer y octavo día	Según lo establecido	Según lo establecido
Medio	Entre el primer y quinceavo día	-	-
Bajo	-	-	-
Inferior	-	-	-