	PROCESO: GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD OPERACIONAL DE LA ORGANIZACIÓN	**CÓDIGO:** P-18-2
		VERSIÓN: 0-16-05-2025
	PROCEDIMIENTO: GESTION DE EVENTOS E INCIDENTES DE CIBERSEGURIDAD	**PÁGINAS:** Página 1 de 8

1) INFORMACIÓN GENERAL DEL PROCEDIMIENTO	
1.1) Unidad Responsable:	VIEM – CSIRT Académico UNAD
1.4) Objetivo:	Gestionar de manera efectiva los eventos e incidentes de ciberseguridad en los activos de información críticos de la Universidad Nacional Abierta y a Distancia - UNAD, a partir de la detección, análisis, respuesta y recuperación oportuna ante amenazas y vulnerabilidades, con el fin de garantizar la Disponibilidad, Integridad y Confidencialidad de la información gestionada.
1.5) Alcance:	Este procedimiento brinda los lineamientos para los eventos e incidentes de ciberseguridad que afecten los activos de información críticos de la Universidad Nacional Abierta y a Distancia, soportados por la infraestructura tecnológica. El alcance contempla la identificación temprana de amenazas, el análisis de vulnerabilidades, la implementación de respuestas efectivas y la ejecución de procesos de recuperación.

2) DEFINICIONES	
2.1) Concepto	**2.2) Definición**
VIEM	Vicerrectoría de Innovación y Emprendimiento
CSIRT Académico UNAD	Centro de Respuestas a Incidentes Informáticos
Análisis de Vulnerabilidades	Proceso de identificación, evaluación y clasificación de las vulnerabilidades presentes en los sistemas críticos para priorizar su mitigación.
Respuesta a Incidentes	Conjunto de acciones y protocolos destinados a contener, erradicar y mitigar los efectos de un incidente de ciberseguridad en los sistemas críticos.
Disponibilidad	Garantía de que los sistemas, servicios y datos estén accesibles y operativos cuando sean requeridos, protegiendo la continuidad de las operaciones
Integridad de la Información	Protección de los datos y sistemas frente a modificaciones no autorizadas, asegurando su precisión y confiabilidad.
Confidencialidad	Salvaguarda de la información sensible para que solo personas o procesos autorizados puedan acceder y gestionar dicha información
Detección de Amenazas	Proceso de monitoreo continuo y análisis para identificar actividades sospechosas o indicios de posibles amenazas de seguridad en los sistemas críticos
Evaluación de Impacto	Análisis que determina el alcance y la gravedad de un incidente de ciberseguridad, así como las posibles consecuencias para los sistemas y la operación de la institución

Recuperación de Incidentes	Acciones orientadas a restaurar los sistemas y servicios afectados a su estado operativo normal, minimizando el tiempo de interrupción y las pérdidas potenciales
Registro de Incidentes	Documentación detallada de cada incidente de ciberseguridad, incluyendo el tipo de amenaza, el impacto, las acciones de respuesta y los aprendizajes para mejorar futuras gestiones
Normativas y Estándares de Seguridad	Conjunto de directrices y requisitos de seguridad que deben cumplirse para proteger la información y los sistemas, alineándose con prácticas reconocidas a nivel nacional e internacional
Sala de crisis	Equipo que coordina acciones frente a un incidente de ciberseguridad, de orden significativo o crítico. Está conformado por: Vicerrector de Innovación y Emprendimiento, Gerente de Plataformas e Infraestructura Tecnológica, Líder del CSIRT Académico UNAD, Oficial de seguridad GPIT, delegado de la Secretaría General o su delegado (Asesor jurídico), delegado de Gerencia de Mercadeo y Comunicaciones, delegado de la unidad afectada

3) CONDICIONES GENERALES

3.1 La Universidad Nacional Abierta y a Distancia gestionará sus vulnerabilidades e incidentes de ciberseguridad, conforme a la Ley 1581 de 2012, y la RESOLUCIÓN No. 007298 DE 10 DE MAYO DE 2023, que establecen las directrices a partir del Marco de Referencia del Sistema de Gestión de Seguridad de la Información – SGSI.

3.2 Todos los eventos o incidentes de ciberseguridad deberán ser reportados al correo electrónico seguridad.informacion@unad.edu.co

3.3 El medio de comunicación oficial para el tratamiento y seguimiento de incidentes de ciberseguridad es el establecido en la aplicación de mesa de ayuda del CSIRT Académico https://ayudacsirt.unad.edu.co/

3.4 Es responsabilidad de proveedores de los servicios tercerizados, apoyar procesos de fortalecimiento de los sistemas de información y de sanitizar los eventos o incidentes de ciberseguridad que se presenten en estos

3.5 Se tiene cómo orientación para la respuesta a incidentes de ciberseguridad la guía denominada “Guía para la Gestión y Clasificación de un Incidentes de Ciberseguridad**”**
https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

4) DESCRIPCIÓN DEL PROCEDIMIENTO

Actividad de Control Operacional

Nº	4.1) Actividad	4.2) Insumos necesarios para la actividad	4.3) Descripción detallada de la actividad	4.4) Registros de Ejecución y de Resultados de la Actividad	4.5) Encargado de la actividad (responsables)
1	Reportar detección de un evento o un incidente de ciberseguridad		Notificar a través de correo electrónico la detección de un evento o incidentes de ciberseguridad por parte de cualquier usuario, indicando la información relevante.	Correo de notificación del incidente de ciberseguridad	Plataforma Humana Unadista, Estudiantes, Egresados, Aspirantes, Proveedores.
2	Validar reporte preliminar para determinar si corresponde a un evento o incidente de seguridad	Correo de notificación del incidente de ciberseguridad	La GPIT remite al CSIRT Académico el reporte preliminar del evento o incidente relacionado con el activo de la información, indicando el posible nivel de criticidad respecto al activo de información, para su análisis, validación y clasificación. Si corresponde a un incidente de ciberseguridad **ir al paso 3**; Si el evento no es clasificado como incidente, se genera clasificación	Clasificación del evento y notificación a partes interesadas	Equipo Funcional de Seguridad – GPIT CSIRT Académico

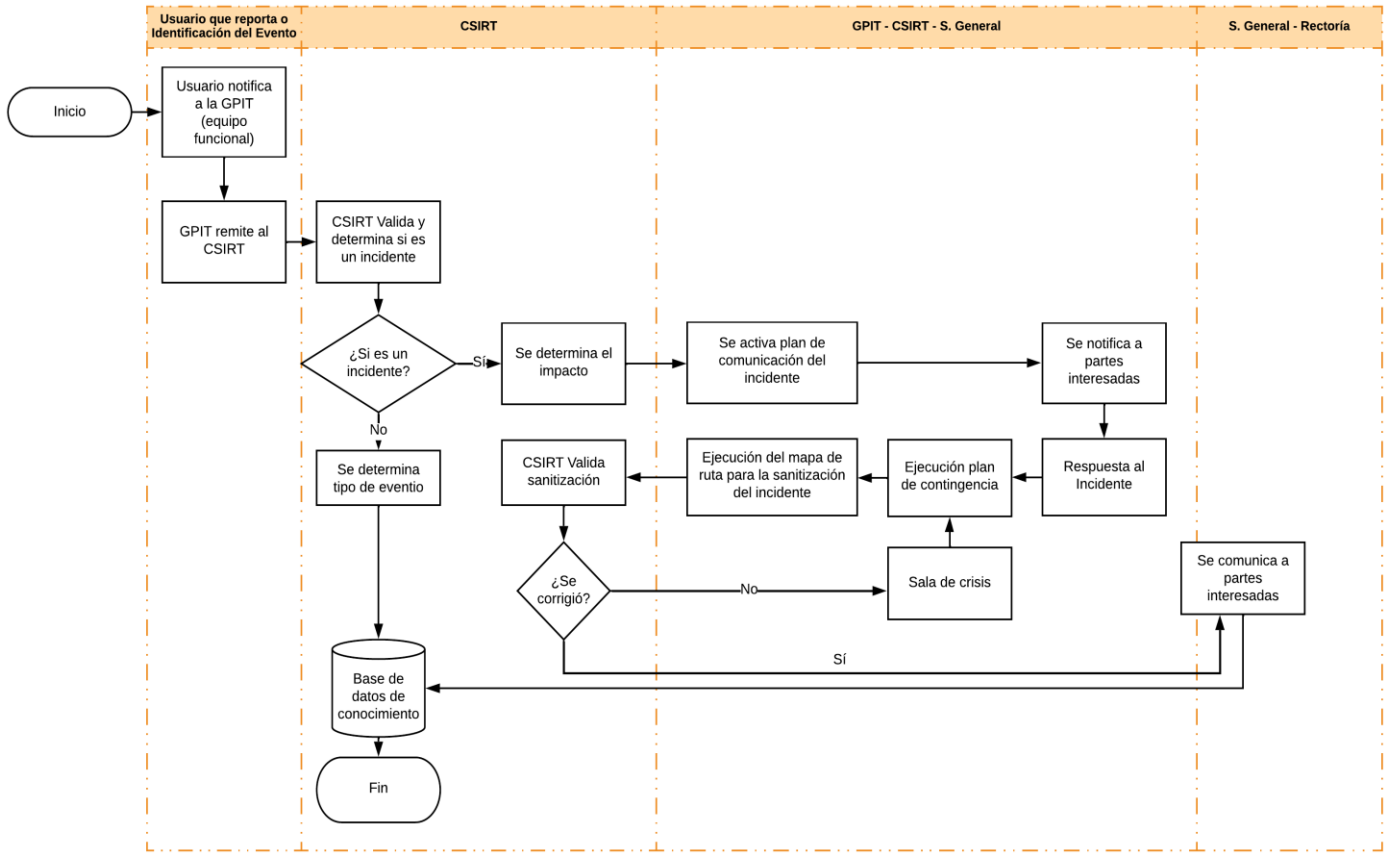
			que describe el tipo de evento y se notifica a partes interesadas.		
3	Generar caso a través de la aplicación de mesa de ayuda del CSIRT	Evaluación y clasificación del evento	Se registra y documenta el incidente de ciberseguridad en la aplicación de mesa de ayuda, incluyendo descripción del impacto preliminar, activos afectados, evidencias recopiladas y clasificación del tipo de incidente según los criterios de la guía para la gestión de incidentes.	Notificación a la GPIT a través de la aplicación de mesa de ayuda, asignando observador y técnico correspondiente para dar atención al caso.	CSIRT Académico UNAD
4	Activar el plan de comunicación del incidente		Según la criticidad del incidente, se notifica a partes afectadas el posible impacto que se puede presentar, con el fin de mitigar superficies de ataques y las acciones de contención. La información se clasifica según el Protocolo de Luz de Tráfico (TLP).	Notificación a partes interesadas.	GCMK - VIEM – GPIT – Rectoría -CSIRT
5	Documentar la respuesta al incidente a través del mapa de ruta para la sanitización del incidente		La unidad afectada debe definir las actividades que se realizarán para contener, erradicar y mitigar el impacto del incidente, definiendo prioridades, actividades específicas y tiempos de respuesta en función de la criticidad.	Mapa de ruta para la sanitización del incidente a través de la mesa de ayuda del CSIRT.	Unidad afectada – GPIT – CSIRT

6	Ejecutar el plan de avance ante la respuesta de un incidente	Mapa de ruta para la sanitización del incidente	Ejecutar las acciones propuestas en el mapa de ruta para asegurar la continuidad operativa y mitigar daños, a partir de las fases de contención, erradicación y recuperación.	Plan de avance ante la respuesta a un incidente de ciberseguridad	Unidad afectada
7	Validar la sanitización	Plan de avance ante la respuesta a un incidente de ciberseguridad	El equipo del CSIRT revisa los resultados de las acciones de contención y erradicación aplicadas, verificando que todas las medidas implementadas han eliminado la amenaza y que no quedan rastros activos del incidente. En este ejercicio, se ejecutan Pruebas de Concepto (PoC) que simulan el comportamiento del sistema en un entorno seguro para evaluar su integridad y asegurar que las vulnerabilidades han sido corregidas y no pueden ser explotadas de nuevo. Si el incidente se corrige, se confirma que todas las amenazas han sido eliminadas y que el sistema está en un estado seguro y	Reporte de Prueba de Concepto	CSIRT – Equipo funcional de seguridad GPIT – Unidad afectada

			funcional se documenta la base de datos del conocimiento, se comunica a partes interesadas y se cierra el caso en mesa de ayuda. En caso contrario, seguir con el paso 8.		
8	Activar sala de crisis	Reporte de Prueba de Concepto	Si el incidente persiste, se remite a la sala de crisis para activar nuevamente el plan de avance y ejecutar acciones adicionales de contención, erradicación y recuperación hasta asegurar la completa eliminación de la amenaza. Ir al paso 6.	Ajustes al plan de avance para la sanitización del incidente.	VIEM – CSIRT- GPIT – Unidad afectada

FIN

5) DIAGRAMA DEL PROCEDIMIENTO



6) NORMATIVIDAD Y DOCUMENTOS DE REFERENCIA	
6.1) Documento de consulta	**6.2 Consulta en**
Matriz de Marco Legal y Normatividad Aplicable	Ver enlace

7) MODIFICACIONES/ACTUALIZACIONES		
7.1) Versión	**7.2) Fecha**	**7.3) Descripción resumida de la modificación/actualización**
0	16-05-2025	Primera versión emitida