1. Objeto: Definir las acciones para analizar, contener, erradicar y responder de manera oportuna ante la ocurrencia de un evento y/o incidente de seguridad de la información.

2. Alcance: Inicia desde la detección de un incidente de seguridad de la información, contención y solución de este, finalizando con la documentación y lecciones aprendidas.

3. Referencias Normativas:

- **Resolución 500 de 2021 de Mintic**, *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".*

3. Definiciones:

- **Activo de Información:** Es todo aquello que representa valor para la Universidad desde software, hardware, información, servicios y personas.
- **Ataque Informático:** Es un intento de exponer, alterar, desestabilizar, destruir, eliminar para obtener acceso sin autorización o utilizar un activo.
- Amenaza: Cualquier situación, acción o evento que ponga en peligro la integridad, confidencialidad o disponibilidad de los activos de información.
- Base de Datos: es un conjunto de datos almacenados sistemáticamente y que son consultados mediante un sistema de información.
- Confidencialidad: Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- Disponibilidad: Es la característica o capacidad de asegurar el acceso oportuno a los datos y recursos que los soportan por parte de los individuos autorizados.
- Incidente de Seguridad de la Información: cualquier evento que se presente y que afecte la confidencialidad, integridad o disponibilidad de los activos de información.
- Integridad: Propiedad de la información que busca preservar su exactitud y completitud.
- Vulnerabilidad: Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

5. Condiciones Generales:

- Todo el personal administrativo debe reportar los incidentes de seguridad de la información que se presenten.
- Se deben reportar aquellos eventos que atenten contra la confidencialidad, disponibilidad e integridad de la información.

6. Contenido:

No.	ACTIVIDAD	RESPONSABLE	PRODUCTO
1.	Reportar el incidente de seguridad de la información a la Oficina de sistemas mediante el formato establecido al correo electrónico sistemas@unillanos.edu.co.	Servidores públicos / Contratistas	**FO-GRT-11** Reporte de incidentes de seguridad de la información Correo electrónico
2.	Validar si el incidente reportado atenta contra la confidencialidad, integridad o disponibilidad de algún activo de información de la Universidad.	Profesional de apoyo Oficina de Sistemas	Análisis del incidente reportado

No.	ACTIVIDAD	RESPONSABLE	PRODUCTO
3.	Analizar e identificar el incidente de seguridad de la información reportado, y registrarlo en el formato definido.	Profesional de apoyo Oficina de Sistemas	**FO-GRT-11** Reporte de incidentes de seguridad de la información *-Numeral 2-*
4.	Contener el incidente de seguridad de la información, mediante la realización de las acciones necesarias para contener el incidente y minimizar su impacto.	Profesional de apoyo Oficina de Sistemas	**FO-GRT-11** Reporte de incidentes de seguridad de la información *-Numeral 2-*
5.	Identificar, recopilar y organizar las evidencias producto de la investigación del incidente de seguridad. Una vez se recolectan las evidencias, se inicia el análisis de las mismas, para determinar el origen y responsables del incidente.	Profesional de apoyo Oficina de Sistemas	
6.	Erradicar el incidente de seguridad de la información, mediante la realización de las tareas necesarias para erradicar la causa raíz detectada y evitar que se vuelva a presentar.	Profesional de apoyo Oficina de Sistemas Profesional de apoyo Oficina de Sistemas	
7.	Documentar las acciones realizadas y lecciones aprendidas del incidente de seguridad.	Profesional de apoyo Oficina de Sistemas	**FO-GRT-11** Reporte de incidentes de seguridad de la información
8.	Comunicar a la persona que reportó, la solución del incidente.	Profesional de apoyo Oficina de Sistemas	-Notificación de la solución

7. Flujograma:

No aplica

8. Anexos

Este documento no cuenta con anexos

9. Historial de Cambios:

Versión	Fecha	Cambios	Elaboró / Modificó	Revisó	Aprobó
01	04/07/2024	Documento Nuevo	Mónica M. Hernández *Profesional de Apoyo*	Adriana Ramos *Prof. de apoyo Oficina de Planeación*	Roiman A. Sastoque *Jefe Oficina de Sistemas*