Centro de Respuestas a Incidentes Informáticos
CIP - CSIRT Académico UNAD

Boletín Informativo

Catorce

# Abril: Roles y Responsabilidades de Ciberseguridad Frente a los Activos de Información UNADISTAS

VIEM Vicerrectoría de Innovación y Emprendimiento

ECBTI Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación Ceros y Unos


Medio de Divulgación del Centro de Respuestas a Incidentes Informáticos: CSIRT Académico UNAD

**E-boletín Informativo CSIRT Académico UNAD**

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Catorce
Abril de 2023

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CSIRT Académico 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 (ECBTI)**
Ing. Sonia Ximena Moreno Molano – Líder Programa de Especialización en Seguridad Informática

**Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign**

**Centro de Respuestas a Incidentes Informáticos**
**CSIRT Académico UNAD**
Ing. Luis Fernando Zambrano Hernández – Director
CSIRT Académico UNAD

**Responsable de la Edición**
Ing. Luis Fernando Zambrano Hernández

Revisó
Ing. Diego Fernando Medina Soto
**Director CCAV Facatativá**

**Estado legal:**
Periodicidad: Quincenal
ISSN: 2806-0164

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


# Tabla de Contenido


Boletín informativo Número 13

Abril 24 de 2023

# Roles y Responsabilidades de Ciberseguridad Frente a los Activos de Información UNADISTAS

Autores:

**Fernando Zambrano Hernández**
CSIRT Académico UNAD
https://orcid.org/0000-0002-4690-3526

**Hernando José Peña Hidalgo**
CSIRT Académico UNAD
https://orcid.org/0000-0002-3477-2645

**John Fredy Quintero Tamayo**
CSIRT Académico UNAD
https://orcid.org/0000-0003-0128-1214

**Néstor Raúl Cárdenas Corral**
CSIRT Académico UNAD
https://orcid.org/0000-0003-3691-0148

## Introducción


La implementación del Modelo de Seguridad y Privacidad de la Información UNADISTA implica la asignación de roles y responsabilidades claras para toda la plataforma humana. Los roles y responsabilidades definidos ayudan a asegurar que cada individuo tenga una comprensión clara de sus tareas y obligaciones específicas en la protección de los activos de información, incluyendo datos y sistemas de información críticos. Además, el establecimiento de roles y responsabilidades claramente definidos también aporta en seguir construyendo una cultura de ciberseguridad sólida, lo que puede mejorar la resiliencia ante una amenaza cibernética y minimizar los riesgos ante un incidente de seguridad de la información.

*Nota.1: [Fotografía] Recuperado de https://www.freepik.es/*


# Desarrollo

## ¿Quiénes salvaguardan la información digital UNADISTA?

Son las unidades del metasistema Unadista, y sus integrantes, los encargados de gestionar y tratar los datos que se encuentran en los sistemas de información y bases de datos físicas y digitales. En este sentido, la Universidad debe establecer las responsabilidades necesarias para llevar a cabo las actividades específicas relacionadas con la seguridad de la información, asignando a las personas apropiadas e idóneas para la realización de esta tarea.

La definición clara de roles para la implementación de un Modelo de Seguridad y Privacidad de la Información - MSPI[1] es crucial para garantizar que cada miembro del equipo comprenda su responsabilidad y tenga tareas claramente definidas.

La Gerencia de Plataformas e Infraestructura Tecnológica - GPIT brinda las estrategias, capacidades y herramientas técnicas y tecnológicas para atender, analizar, clasificar, responder, mitigar e investigar los incidentes de seguridad informática, con fin de ejercer controles sobre los activos tecnológicos y de información de la UNAD. Este trabajo se desarrolla de forma articulada con el Centro de Respuestas a Incidentes Informáticos CSIRT Académico UNAD y los propietarios de los activos de información[2].

## ¿Qué metodología usamos para analizar y evaluar el riesgo de ciberseguridad UNADISTA?

Como apoyo metodológico para el análisis y evaluación del riesgo, se hace uso de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - MAGERIT[3], aplicando la técnica especifica de uso de tablas o matrices para la obtención de resultados. La metodología MAGERIT plantea un trabajo estructurado para el análisis y la gestión de riesgos de los sistemas de información[4], ya que se enfoca en el ciclo de vida completo de un determinado sistema, teniendo presente la planificación el diseño, la operación y el mantenimiento del análisis de riesgos. Esta metodología tiene como objetivo orientar la identificación y evaluación de los riesgos de seguridad asociados con los sistemas de información, con el fin de establecer medidas de seguridad adecuadas que permitan minimizar los riesgos.

En el ejercicio de la aplicación de la metodología, es requerido entre otros aspectos el identificar al propietario del riesgo

## ¿Cuáles son los roles que giran en torno a un activo de información?

Como se mencionó de forma anterior, son las unidades del metasistema Unadista quiénes delegan la responsabilidad de proteger y preservar el activo de información. Para esta tarea se cuenta con tres 3 roles los cuales trabajan en

[1] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/
[2] Persona que protege y preserva la confidencialidad, integridad y disponibilidad del activo de información bajo su responsabilidad.
[3] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
[4] El análisis de riesgos de ciberseguridad es un proceso sistemático y estructurado que tiene como objetivo identificar y evaluar las amenazas y vulnerabilidades que pueden afectar la seguridad de la información y los sistemas informáticos de una organización. Este análisis permite determinar el impacto potencial de los riesgos, así como la probabilidad de que ocurran, para poder tomar medidas preventivas y mitigarlos de manera efectiva

conjunto con GPIT para garantizar la reducción de brechas de ciberseguridad que puedan afectar las dimensiones de la seguridad de la información:

Propietario del activo de información:

- Identifica de forma clara qué información es considerada como activo de información.

- Protege la información contra accesos no autorizados, modificaciones no autorizadas, divulgación no autorizada y destrucción no autorizada.
- Asigna roles y responsabilidades claras a las personas que tienen acceso a la información, teniendo presente que la responsabilidad sigue siendo de este.
- Monitorea y evaluar el uso de la información para garantizar que se utilice de acuerdo con las políticas de seguridad establecidas por la Universidad.
- Actualiza y mantiene la información para garantizar que sea precisa y esté actualizada.
- Informa al Centro de Respuestas a incidentes informáticos – CSIRT Académico UNAD a través de los canales de comunicación establecidos de cualquier evento o incidente de ciberseguridad que pueda afectar a la información

Ejemplo: Oficina de Registro y Control – RCA

Es importante mencionar que es la Unidad quien asigna al un funcionario de está la responsabilidad del activo de información

Responsable del Activo de Información:

- Protege y preserva la confidencialidad, integridad y disponibilidad del activo de información bajo su responsabilidad.
- Identifica los posibles riesgos y vulnerabilidades asociados con dicho activo. Esto implica realizar evaluaciones de riesgos periódicas y utilizar herramientas y técnicas adecuadas para identificar y comprender las posibles amenazas.
- Implementa y mantiene las medidas de seguridad necesarias para proteger el activo de información.
- Se asegura de que las políticas y procedimientos de seguridad de la Universidad se cumplan en relación con el activo de información bajo su responsabilidad.

- Actúa de manera oportuna y eficaz para contener, mitigar y resolver un evento que pueda poner en riesgo la integridad, disponibilidad y confidencialidad de la información.

- Se mantiene informado sobre las últimas tendencias, tecnologías y mejores prácticas en materia de seguridad de la información que impacte al activo del cual es responsable.
- Informa al Centro de Respuestas a incidentes informáticos – CSIRT Académico UNAD a través de los canales de comunicación establecidos de cualquier evento o incidente de ciberseguridad que pueda afectar a la información.

Ejemplo: jefe de la oficina de registro y control o a quien delegue.

En el ejercicio de salvaguardar la información, es el Custodio de la información quien gestiona los controles de seguridad de la organización, como firewalls, sistemas de detección de intrusiones, políticas de acceso, encriptación, entre otros, con el fin de reducir la exposición al riesgo del activo de información. Así mismo tiene como función:

Custodio de la información

- Salvaguarda la información que le ha sido confiada y la protege contra cualquier acceso no autorizado, modificaciones no autorizadas, divulgación no autorizada y destrucción no autorizada.
- Implementa en conjunto con la GPIT, las medidas de seguridad necesarias para proteger el activo de información de acuerdo con las políticas y estándares de seguridad de la Universidad.
- Monitorea el acceso a la información y garantizar que se utilice de acuerdo con las políticas y estándares de seguridad establecidos.
- Informa al Centro de Respuestas a Incidentes Informáticos – CSIRT Académico UNAD a través de los canales de comunicación establecidos de cualquier evento o incidente de ciberseguridad que pueda afectar la información.
- Mantiene registros precisos y actualizados del acceso y uso del activo de información.
- Capacita a los usuarios sobre las políticas y estándares de seguridad de la organización para garantizar que se utilice el activo de información de manera segura y responsable.
- Proporciona informes regulares sobre la seguridad del activo de información a la GPIT y otros interesados pertinentes.
- Asigna los accesos y privilegios de uso al activo de información.
- Realiza copia de información del activo de información.
- Modifica o aplicar controles de seguridad al activo de información.

Ejemplo: En cabeza de la Secretaría General con apoyo de la Gerencia de Plataformas e Infraestructura – GPIT

## ¿Cómo identificar un activo de información?

El boletín N° 13 del mes de marzo de 2023 “”, presenta la forma de catalogar un activo de información, a partir de esto, puede tener presente los siguientes aspectos para identificar de forma clara el activo:

| | |
|---|---|
| Nombre del activo de información | Indica el nombre del activo de información |
| Descripción | Indica de forma clara cuál es el objetivo del activo de información |
| Tipo de activo de información | Indica el tipo de activo de información (Ver boletín 13) |
| Proceso al que pertenece | Indica a que proceso del SIG pertenece el activo de información |
| Propietario del activo de información | Indica la Unidad a la cual tiene como responsabilidad la gestiona el activo de información |
| Responsable del activo de información | Indica el nombre completo del funcionario o externo el cual es responsable del activo de información |
| Custodio del activo de información | Indica Unidad responsable de la custodia del activo de información |
| Dueño del dato | Indica quien es el dueño del dato el cual es tratado en el activo de información (Aspirante, estudiante, egresado, funcionario, otro) |
| Tipo de información que gestiona | Indica si la información es publica o reservada[5] (ley 1712 de 2014) |
| Tipo de datos que contiene | Indica si el activo de información contiene datos públicos, privados, semiprivados o sensibles o datos personales o no personales[6] (ley 1581 de 2012) |
| Ubicación | Indicar la ubicación del activo de información determinando si es Física o Digital |

[5] https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882
[6] https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981


## Canales de comunicación

El CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:

Correo: csirt@unad.edu.co

Twitter: @csirtunad

Página web: https://csirt.unad.edu.co