Universidad Nacional Abierta y a Distancia
ACREDITADA EN ALTA CALIDAD

Centro de Respuestas a Incidentes Informáticos
CIP - CSIRT Académico UNAD

Boletín Informativo
Número **Uno**

ECBπ
Escuela de Ciencias Básicas, Tecnología e Ingeniería

VIEM
Vicerrectoría de Innovación y Emprendimiento

Semillero de Investigación
Ceros y Unos

E-boletín Informativo CIP- 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 Uno
Febrero de 2022

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CIP – 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
CIP – CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Director CIP CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernández

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

Licencia Atribución – Compartir igual

Tabla de Contenido

Boletín informativo Número 1

Febrero 22 de 2022

Conoce un poco de nuestro Centro de Innovación y Productividad Centro de Respuestas a Incidentes Informáticos CIP CSIRT Académico UNAD

Autor: Luis Fernando Zambrano Hernández
ORCID: https://orcid.org/0000-0002-4690-3526

Introducción

Con el uso creciente de internet como medio para extender los servicios de una organización hacia sus clientes, la exposición de sus servicios y de su información de la misma forma se incrementan. Reporte reciente de la Cámara Colombiana de Informática y Telecomunicaciones, indica que el crecimiento de ataques informáticos que se reportaron ante el CTI y la Policía Nacional crecieron en el año 2021 un **21%** respecto al año 2020. [1]

https://www.freepik.es/fotos/tecnologia
Foto de Tecnología creado por rawpixel.com

Esto sin duda alguna evidencia la necesidad de contar con personal experto que contribuya en la reducción de eventos a ataques informáticos que pongan en riesgo la información de las organizaciones y la de su talento humano[2].

[1] Tendencias del Cibercrimen 2021 – 2022 [en línea]. Cámara Colombiana de Informática y Telecomunicaciones [fecha de consulta: 21/02/2022] Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf
[2] Primera respuesta: antes de que llegue la policía [en línea]. Organización de los Estados Americanos. [fecha de consulta: 21/02/2022] Disponible en: https://www.oas.org/juridico/spanish/cyber/cyb46_csirts_sp.pdf

Desarrollo

Un Centro de Respuestas a Incidentes Informáticos o como se conoce por su sigla en inglés, un **CSIRT**, *"es una organización que es responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad."* [3] y una de sus características es la de apoyar a partir de un ámbito de actuación sus necesidades.

En este sentido y dando respuesta al **Proyecto 23** del plan de desarrollo de 2019-2023 de la UNAD[4], en el cual uno de sus objetivos es el de *"Desarrollar proyectos y estrategias de carácter científico, tecnológico y de innovación, que fortalezcan los sectores productivos y de educación en Colombia",* se crea el Centro de Innovación y Productividad: Centro de Respuestas a Incidentes Informáticos – CIP CSIRT Académico UNAD, que alineado a su código de ética y sus políticas de funcionamiento, tiene como objetivos:

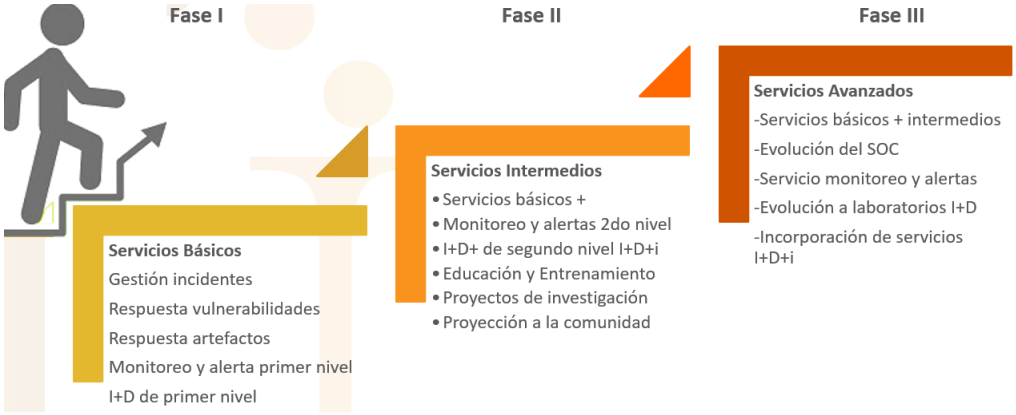
- **Proponer** lineamientos para la gestión de la seguridad de la información que aporten al fortalecimiento de las partes interesadas a partir de programas de educación y cultura enfocados en Ciberseguridad.
- **Gestionar** la arquitectura de Operaciones de Seguridad SOC[5], con el fin de dar respuesta a eventos de Ciberseguridad presentados en los procesos institucionales y de las partes interesadas a partir de su detección, identificación, respuesta, protección y recuperación.
- **Propiciar** alianzas con instituciones de educación, PyMES y entidades territoriales, nacionales internaciones que permitan el despliegue de los servicios del dispositivo contribuyendo en la generación y divulgación de conocimiento de temas de interés asociados con Ciberseguridad.
- **Liderar** espacios que permitan generar Investigación, Desarrollo Tecnológico e Innovación I+D+i para la comunidad académica y las partes interesadas con el fin de divulgar nuevo conocimiento y contribuir en la mejora de entonos digitales seguros.
- **Fortalecer** los procesos académicos de las escuelas que impacte el Centro de Innovación y Productividad CSIRT Académico UNAD, a través de la generación de espacios que permita a los estudiantes, egresados y partes interesadas vincularse en procesos de Investigación, Desarrollo Tecnológico e Innovación I+D+i.

Es así como el Centro de Respuestas a Incidentes Informáticos CIP - CSIRT Académico UNAD se constituye como un dispositivo organizacional enunciado en la Política de Innovación y Emprendimiento de la UNAD, que articula a la Vicerrectoría de Innovación y Emprendimiento VIEM con la Gerencia de Plataformas e Infraestructura Tecnológica GPIT, El programa de Especialización en Seguridad Informática, las Escuelas Académicas, Nodos Zonales y demás dispositivos organizacionales, que permitan generar espacios para la gestión del

[3] Propuesta para la Creación y Consolidación del Centro de Respuesta a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia CSIRT-UNAD [en línea]. Universidad Nacional Abierta y a Distancia. [fecha de consulta: 21/02/2022] Disponible en: https://repository.unad.edu.co/handle/10596/37053
[4] Plan de Desarrollo 2019 – 2023 [en línea]. Universidad Nacional Abierta y a Distancia. [fecha de consulta: 21/02/2022] Disponible en: https://informacion.unad.edu.co/images/planeacion/2020/PLAN_DESARROLLO_2019_-_2023_-_V2_F_compressed.pdf
[5] SOC – Centro de Operaciones de Seguridad

conocimiento y transformación tecnológica e innovación, derivadas de un modelo de operación definido internamente y direccionado por un equipo humano experto. A continuación, se presenta el modelo de madurez de capacidades que el dispositivo está desarrollando con el propósito de dar cumplimiento a sus objetivos

Figura 1. Modelo de Madurez de Capacidades CIP CSIRT Académico UNAD



Fuente. El autor

La Figura 1, presenta como el dispositivo despliega sus capacidades a partir de tres fases definidas que se ejecutan en un lapso de 3 años. En esta se puede notar como los servicios de gestión, monitoreo y respuesta a incidentes marcan la trazabilidad que permite a través de proceso de educación y la ejecución de proyectos de I+D+i, la divulgación de información que contribuya en mejorar la ciberseguridad al interior de la Universidad y en propender por el desarrollo regional en los territorios donde se hace presencia, desarrollando oportunidades para las PyMES y entes territoriales de la región como un aliado estratégico, que desde la gestión de su portafolio de servicios aporte a estos actores con procesos de consultoría, capacitación, auditoria, entrenamiento, educación y auditorias técnicas que den como resultado una buena gestión de la información y procesos de educación y cultura en Ciberseguridad.

Canales de comunicación

El CIP 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

Recursos Bibliográficos Consultados

[1] Tendencias del Cibercrimen 2021 – 2022 [en línea]. Cámara Colombiana de Informática y Telecomunicaciones [fecha de consulta: 21/02/2022] Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-safe-tendencias-del-cibercrimen-2021-2022.pdf

[2] Primera respuesta: antes de que llegue la policía [en línea]. Organización de los Estados Americanos. [fecha de consulta: 21/02/2022] Disponible en: https://www.oas.org/juridico/spanish/cyber/cyb46_csirts_sp.pdf

[3] Propuesta para la Creación y Consolidación del Centro de Respuesta a Incidentes Informáticos de la Universidad Nacional Abierta y a Distancia CSIRT-UNAD [en línea]. Universidad Nacional Abierta y a Distancia. [fecha de consulta: 21/02/2022] Disponible en: https://repository.unad.edu.co/handle/10596/37053

[4] Plan de Desarrollo 2019 – 2023 [en línea]. Universidad Nacional Abierta y a Distancia. [fecha de consulta: 21/02/2022] Disponible en: https://informacion.unad.edu.co/images/planeacion/2020/PLAN_DESARROLLO_2019_-_2023_-_V2_F_compressed.pdf