CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS “CSIRT ACADÉMICO CYBER PHANTOMS ETITC

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En 2025, Colombia enfrenta un panorama desafiante en ciberseguridad, con un aumento significativo en las amenazas cibernéticas impulsadas por tecnologías emergentes como la inteligencia artificial (IA) y la computación cuántica. Los ciberdelincuentes están utilizando herramientas avanzadas, como deepfakes y phishing automatizado, para realizar ataques más complejos y dirigidos.

Además, la creciente adopción de la nube y la distribución de datos en múltiples entornos han ampliado las superficies de ataque, aumentando el riesgo de violaciones de datos. Es así como, para mitigar estos riesgos, se recomienda implementar estrategias como la autenticación multifactor, la educación continua sobre ciberseguridad y el monitoreo en tiempo real.

Estas medidas son esenciales para proteger nuestros activos de información en un entorno digital cada vez más complejo; por está razón se crea el **CSIRT Académico Cyber Phantoms ETITC** “Centro de Respuestas a Incidentes Informáticos “, que es responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad.” y una de sus características es la de apoyar a partir de un ámbito de actuación sus necesidades.

El CSIRT Académico brinda apoyo a la comunidad educativa de la ETITC y, con frecuencia, colabora con otros CSIRT Educativos y de Nación para desarrollar actividades de investigación conjunta. En este sentido y dando respuesta al Plan de Desarrollo Institucional PDI 2025 – 2032 en su eje estratégico No. 2 Investigación y Producción Técnico – Científica, en su línea de acción Capacidades de Investigación e Innovación con su objetivo estratégico: Contar con una sólida capacidad de investigación y su meta estratégica Contar con un (1) grupo de investigación en clasificación A (en MinCiencias), dando cumplimiento a la normativa de Ministerio de Tecnologías de la Información y Comunicaciones de Colombia (MinTIC).

2. OBJETIVO GENERAL

Brindar soporte y respuesta oportuna a los incidentes de ciberseguridad que afecten a la comunidad educativa de la ETITC, promoviendo la protección de la infraestructura tecnológica, la integridad de los datos y la continuidad de los procesos académicos, a través de la implementación de medidas preventivas, la gestión efectiva de incidentes y la colaboración con otros CSIRT para la investigación y el desarrollo de soluciones innovadoras en el ámbito de la ciberseguridad.

2.1. OBJETIVOS ESPECIFICOS

- Gestionar y responder de manera eficiente los incidentes de ciberseguridad que afecten a la comunidad educativa, incluyendo estudiantes, docentes y personal administrativo.

- Implementar medidas proactivas para prevenir ataques cibernéticos, como el despliegue de herramientas de monitoreo y análisis de seguridad, incluyendo auditorías periódicas para la identificación de vulnerabilidades.

- Establecer alianzas y canales de comunicación con otros CSIRT académicos, instituciones de seguridad cibernética y organismos gubernamentales para compartir información sobre amenazas y mejores prácticas que promuevan la investigación para contribuir al desarrollo de soluciones innovadoras en ciberseguridad.

- Mantener actualizado el plan de continuidad del servicio y la recuperación ante desastres (DRP) enfocados en la seguridad cibernética para validar su efectividad de los planes de recuperación y garantizar que la infraestructura crítica de la ETITC pueda restablecerse rápidamente en caso de un ataque.

- Desarrollar y ejecutar investigaciones forenses para determinar el origen y alcance de los incidentes cibernéticos, y recuperar evidencia para posibles acciones legales o disciplinarias. A través de un análisis detallado de los incidentes después de su resolución, con el fin de identificar lecciones aprendidas y aplicar mejoras en los procesos de seguridad.

3. COMPONENTES DEL CSIRT ACADÉMICO CYBER PHANTOMS ETITC

La ETITC cuenta actualmente con un Sistema de Gestión de Seguridad de la Información fuerte, el cuál cumple con los requisitos de la NTC ISO/IEC 27001:2022 y que a su vez cuenta con la Gestión de Proyectos cumpliendo con las estrategias del plan de acción institucional en materia de Ciberseguridad, estos son aplicados a los procesos estratégicos, misionales, de apoyo y de evaluación, por tal motivo, el CSIRT ACADÉMICO CYBER PHANTOMS ETITC, debe apoyar a todos los servidores públicos, proveedores, contratistas y demás partes interesadas en la respuesta inmediata sobre las actividades cibernéticas enmarcados en los componentes para la protección de la infraestructura tecnológica, que debe ser capaz de detectar, responder y mitigar incidentes de seguridad de manera eficiente, brindando apoyo tanto preventivo como reactivo a la comunidad educativa.

Además, la colaboración externa y la educación continua son clave para mantener un entorno seguro y resiliente frente a las amenazas cibernéticas emergentes. Es así que el CSIRT Académico adicionalmente apoyará internamente a la Vicerrectoría Académica y Vicerrectoría de Investigación y a su semillero de investigación en seguridad informática "SAPIENTIAM", donde se incluyan actividades de fortalecimiento de conocimientos de Ciberseguridad, Políticas de Seguridad de la Información y Gestión Administrativa a los estudiantes del semillero para que realicen proyecto de grado de nuestras programas académicos fomentando las líneas institucionales de investigación como la:

1. Pedagogía y Didáctica, Arte, Humanismo y Tecnociencias

2. Energía: asequible, eficiente y sostenible

3. Ambiente y Bioeconomía sustentable

4. Equidad, Desarrollo Social y Posdesarrollo

5. Materiales, Diseño y Procesos de las ingenierías

6. Industrias, Empresas y Emprendimientos

7. Tecnologías Convergentes NBIC (Nanotecnología, Biotecnología, informática (Big Data, internet de las cosas). Cognitivismo (inteligencia artificial y Robótica).

3.1 Estructura Organizacional del CSIRT Académico "Cyber Phantoms ETITC"

La estructura organizacional del CSIRT Académico estará compuesta por:

Director del CSIRT Académico: Quién será el líder del Sistema de Gestión de Seguridad de la Información y a su vez es el responsable de la gestión estratégica y supervisión general del CSIRT.

Equipo de Respuesta a Incidentes: Compuesto por el profesional de ciberseguridad, profesional de continuidad del servicios y protección de datos personales, líder del semillero de investigación SAPIENTIAM y expertos forenses digitales, que se encargan de gestionar y mitigar los incidentes, así como la de coordinar la comunicación tanto interna (con la comunidad educativa) como externa (con otros CSIRT académicos y de gobierno).

Equipo de apoyo en Investigación y Desarrollo: Estudiantes que se encuentren activos en el semillero de investigación SAPIENTIAM durante los últimos tres (3) años de manera consecutiva, y quiénes tendrán la responsabilidad de innovar y mejorar las herramientas y procesos de seguridad, incluyendo las recomendaciones de nuevas soluciones tecnológicas adaptadas a las necesidades de la ETITC, así como la de desarrollar

programas educativos y de sensibilización en ciberseguridad para los miembros de la comunidad académica.

3.2 Infraestructura Tecnológica del CSIRT Académico

- **Plataforma de Gestión de Incidentes:** Se cuenta con el aplicativo GLPI (Herramienta centralizada para recibir, gestionar y hacer seguimiento a los incidentes de seguridad). Esta plataforma debe permitir el registro de informes, clasificación de incidentes, y asignación de tareas al equipo de respuesta.

- **Procedimientos para la Gestión de Incidentes:** Actualmente el SGSI, cuenta con los siguientes procedimientos y formatos:

  - ✓ GSI-SI -PC-01 Identificación, Recolección, Adquisición y Preservación de Evidencias
  - ✓ GSI-SI -PC-05 Gestión de Incidentes de la Seguridad de la Información
  - ✓ GSI-SI -PC-06 Contacto con las autoridades
  - ✓ GSI-SI-FO-01 Compromiso de Confidencialidad en cuanto al uso y divulgación de información de la ETITC
  - ✓ GSI-SI-FO-06 Reporte de eventos e incidentes de seguridad de la información
  - ✓ GSI-SI-FO-07 Lecciones aprendidas
  - ✓ GSI-SI -FO-08 Inspección técnica de seguridad de la información
  - ✓ GSI-SI -FO-09 Informe de pruebas de auditoría técnica

- **Sistemas de Monitoreo:** Soluciones como SEM (Security Event Management) que permiten el correlacionamiento de eventos de seguridad cibernéticos en la infraestructura de la ETITC.

- **Sistemas de Inteligencia de Amenazas:** Tecnología que permite la automatización e investigación forense, así como la visualización de activos comprometidos y de accesos no autorizados.

- **Sistemas de Cifrado y Protección de Datos:** Implementación de cifrado de extremo a extremo para la protección de los datos sensibles de estudiantes, docentes y personal administrativo.

3.3 Funcionamiento del CSIRT Académico

Recepción de Informes: Establecimiento de canales seguros y accesibles (como una página web, correo electrónico y línea telefónica) para recibir reportes de incidentes desde cualquier miembro de la comunidad educativa.

Clasificación y Priorización: Cada incidente debe ser clasificado según su naturaleza (phishing, malware, acceso no autorizado, etc.) y priorizado a través de su impacto potencial en la infraestructura tecnológica de la ETITC.

Análisis y Respuesta: El equipo de respuesta realiza un análisis forense preliminar, identifica la causa raíz y, en función del tipo de incidente, toma medidas correctivas (desinfectar equipos, actualizar parches, etc.).

Escalamiento: En caso de incidentes graves o complejos, se debe contar con un protocolo de escalamiento que involucre a expertos externos o autoridades si es necesario (por ejemplo, un ataque DDoS masivo o fuga de datos).

Informe y Seguimiento: Después de resolver el incidente, se elabora un informe detallado para documentar el proceso de respuesta, las lecciones aprendidas y las medidas preventivas a implementar.

3.4 Servicios de Apoyo a la Comunidad Educativa del CSIRT Académico

Educación y Capacitación Continua: Organizar talleres, seminarios y cursos para estudiantes, profesores y personal administrativo sobre las mejores prácticas en ciberseguridad, protección de datos y cómo detectar amenazas comunes (como el phishing).

Asesoramiento Técnico: Brindar asesoría personalizada a facultades, departamentos y proyectos educativos en temas de seguridad cibernética, como la protección de plataformas de gestión académica, correos electrónicos y redes de comunicación interna.

Alertas y Notificaciones: Enviar comunicaciones regulares a la comunidad académica sobre nuevas amenazas cibernéticas, vulnerabilidades críticas, y parches de seguridad disponibles.

Recursos y Herramientas: Ofrecer herramientas de seguridad, como antivirus, firewalls, y gestores de contraseñas, y asegurar que todos los miembros de la comunidad tengan acceso a ellos.

3.5 Colaboración con Otros CSIRT y Entidades Externas

Alianzas con otros CSIRT: Crear vínculos con otros CSIRT académicos, sectoriales, de gobierno y de organizaciones externas para compartir inteligencia sobre amenazas emergentes y mejores prácticas en ciberseguridad.

Colaboración con Autoridades: En casos de incidentes graves, como el acceso no autorizado a información personal sensible, colaborar con las autoridades correspondientes (CSIRT policía, CSIRT defensa, entre otros) para garantizar que se tomen las acciones legales apropiadas.

3.6 Evaluación y Mejora Continua

Simulacros de Seguridad: Realizar simulacros de ciberseguridad regulares, como simulaciones de ataques cibernéticos o de fuga de datos, para poner a prueba la capacidad de respuesta del CSIRT y la comunidad educativa.

Análisis Post-Incidente: Después de cada incidente, realizar un análisis exhaustivo para identificar fortalezas y áreas de mejora en los procedimientos de respuesta, así como en las herramientas y políticas de seguridad, ciberseguridad y protección de la privacidad.

3.7 Recursos Humanos y Formación del Equipo

Capacitación del Personal del CSIRT: Asegurar que el equipo del CSIRT esté capacitado en las últimas tendencias en ciberseguridad, como amenazas avanzadas, análisis forense y respuesta ante incidentes.

Reclutamiento de Especialistas: En el caso de incidentes complejos, contar con un grupo de especialistas que puedan ser reclutados para apoyar al CSIRT en la resolución de casos más avanzados.

4. HISTORICOS DEL PROYECTO

La iniciativa del CSIRT Académico Cyber Phantoms ETITC, proyectada en marzo del 2025, por la ingeniera Sandra J. Guerrero G., especialista en seguridad de la información y líder de este proyecto, representa un paso fundamental hacia la consolidación de un entorno

académico seguro en la ETITC. Con una sólida visión estratégica, la ingeniera Guerrero ha logrado estructurar un equipo capaz de enfrentar los desafíos cibernéticos que impactan directamente en la comunidad educativa, brindando un enfoque preventivo, reactivo y formativo.

A través de la creación de este CSIRT, se refuerza la importancia de la protección de la infraestructura tecnológica, la sensibilización constante en ciberseguridad y la colaboración interinstitucional con otros actores clave del ecosistema de seguridad. En última instancia, Cyber Phantoms ETITC no solo busca proteger la integridad de los datos y sistemas académicos, sino también promover una cultura de seguridad cibernética en toda la comunidad educativa, asegurando un futuro más seguro y resiliente frente a las crecientes amenazas cibernéticas.

5. CONCLUSIONES

El CSIRT Académico Cyber Phantoms ETITC desempeña un rol crucial en la protección de la infraestructura tecnológica de la ETITC y en la seguridad de la comunidad educativa. Al establecer un enfoque integral que combine la prevención, respuesta rápida y formación continua, este equipo se convierte en una pieza fundamental para mitigar los riesgos cibernéticos que puedan afectar a estudiantes, docentes y personal administrativo. Su capacidad para gestionar incidentes, ofrecer apoyo proactivo y colaborar con otros CSIRT y entidades externas permite crear un entorno académico más seguro y resiliente. Así, el CSIRT no solo actúa como un centro de respuesta, sino también como un motor de innovación y sensibilización, asegurando que la ETITC se mantenga a la vanguardia en términos de ciberseguridad y proteja su valiosa información en un contexto digital cada vez más complejo.

6. CONTROL DE CAMBIOS

FECHA	VERSIÓN	CAMBIOS
2025-03-19	1	Se adopta el documento

ELABORÓ	REVISÓ	APROBÓ
Esp. SANDRA J. GUERRERO G. Líder de Seguridad de la Información	**ANAY PINTO VALENCIA** Administrador de la Documentación	**Dr. JORGE HERRERA ORTIZ** Jefe de oficina de planeación Institucional