Evidencia congreso de isecurity Summit colombia

Jaider Alejandro Rodriguez Avendaño

Universidad ECCI

Ingeniería de Sistemas

Seguridad Informática

Alexander Sabogal

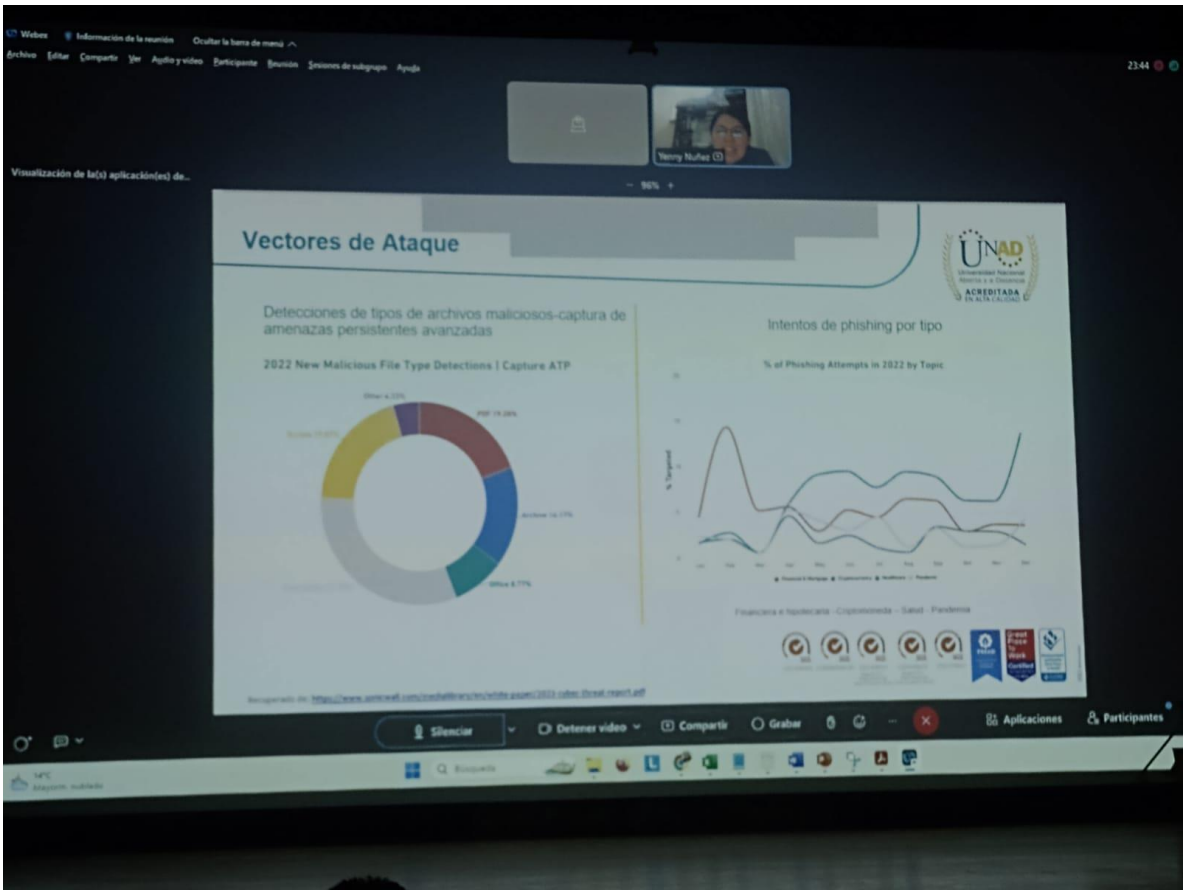
Bogotá

2023

El congreso de Ciberseguridad tuvo lugar los días viernes 13 y sábado 14 de octubre en el teatro de la Universidad ECCI. Durante el evento, se abordaron diversos temas cruciales, como la relevancia de una implementación efectiva de ciberseguridad en las empresas, la seguridad en la infraestructura y el papel fundamental de las mujeres en el ámbito de la ciberseguridad en la actualidad.

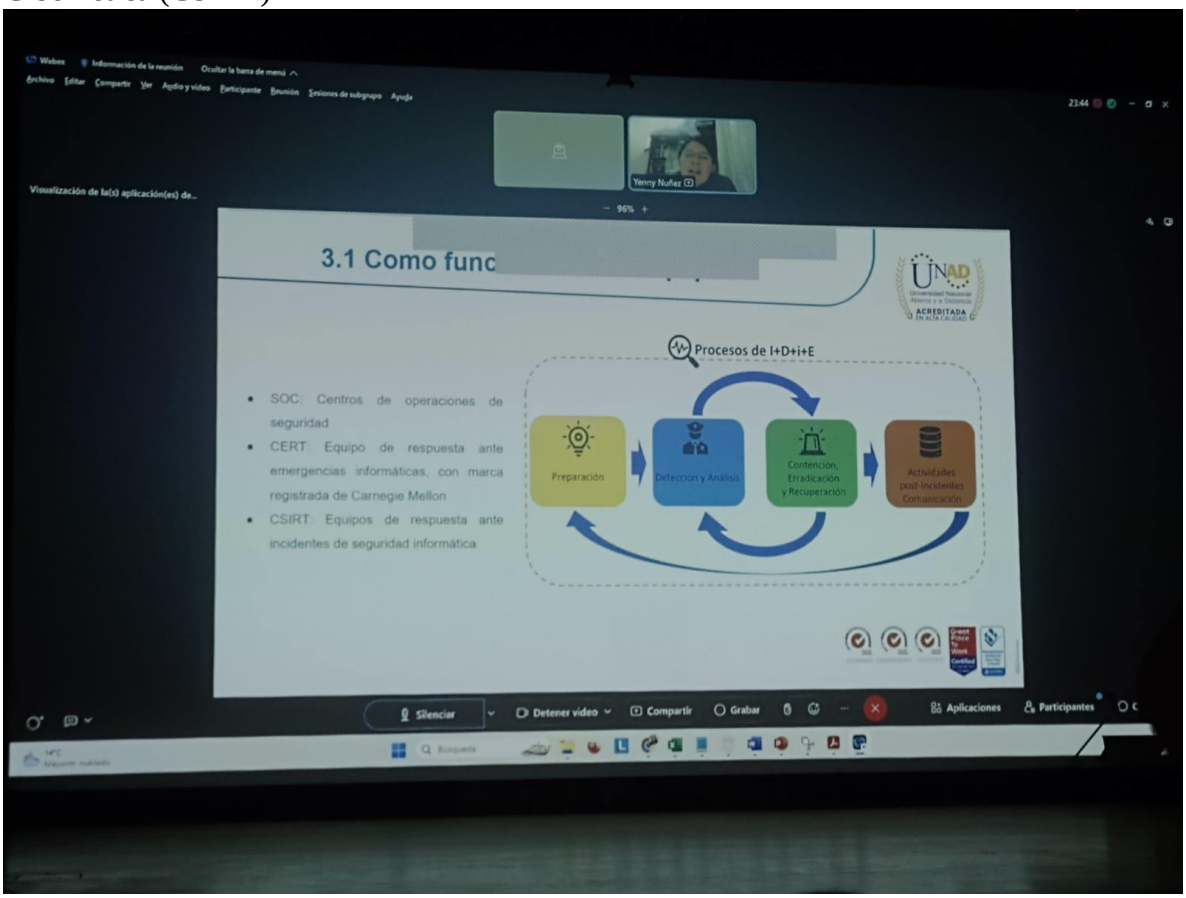
En este documento, nos centraremos en un tema específico: la importancia y responsabilidad que conlleva el equipo de ciberseguridad dentro de una empresa.

La ingeniera Yenny Muñoz proporciona insights valiosos sobre la responsabilidad que asume un equipo de ciberseguridad en las empresas. Esto comienza con el análisis de datos relacionados con ataques a empresas, como la presencia de archivos maliciosos y los intentos de phishing.



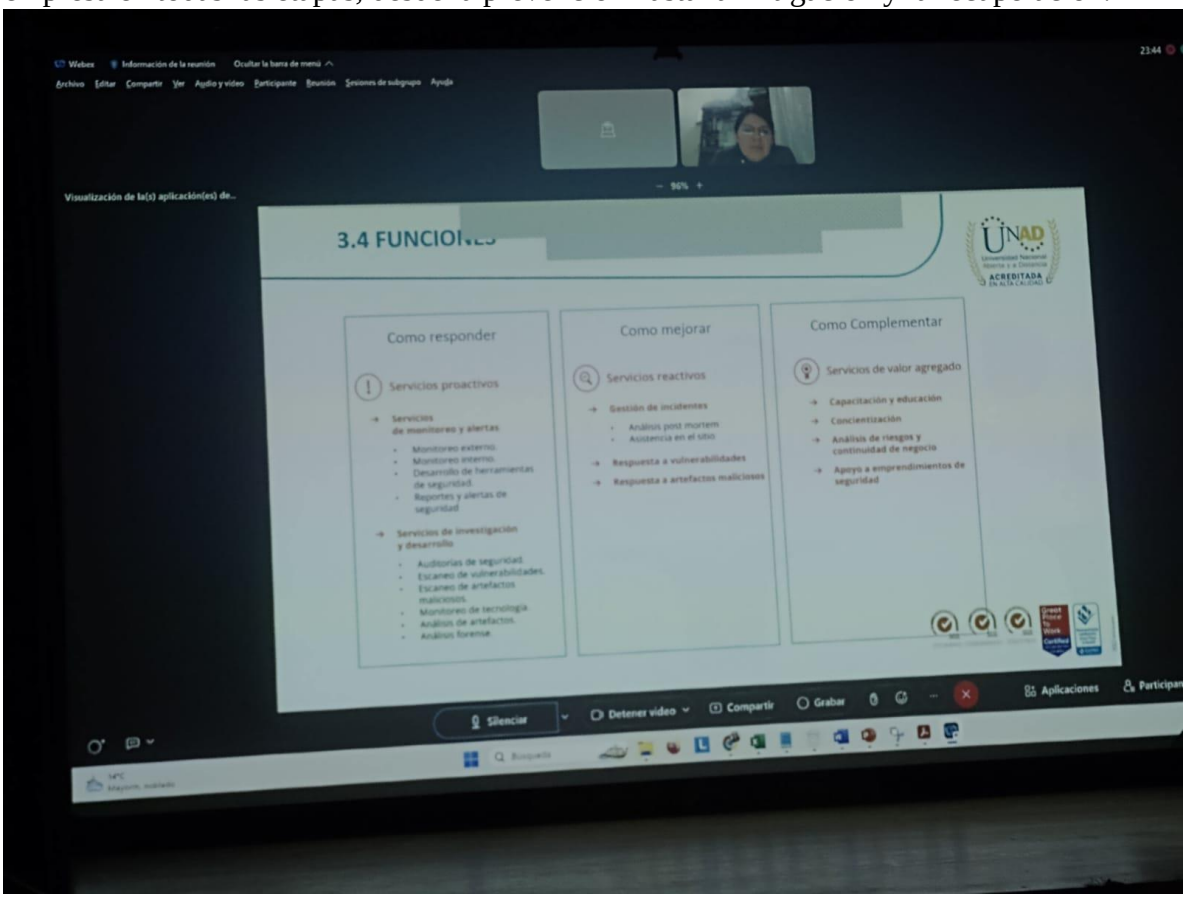
A continuación, la ingeniera Yenny Muñoz detalló los equipos que están operativos en diferentes fases: antes, durante y después de enfrentar un ataque cibernético. Estos equipos son el Centro de Operaciones de Seguridad (SOC), el Equipo de Respuesta a Incidentes de Seguridad Informática (CERT) y el Equipo de Respuesta a Incidentes de Seguridad

Cibernética (CSIRT)



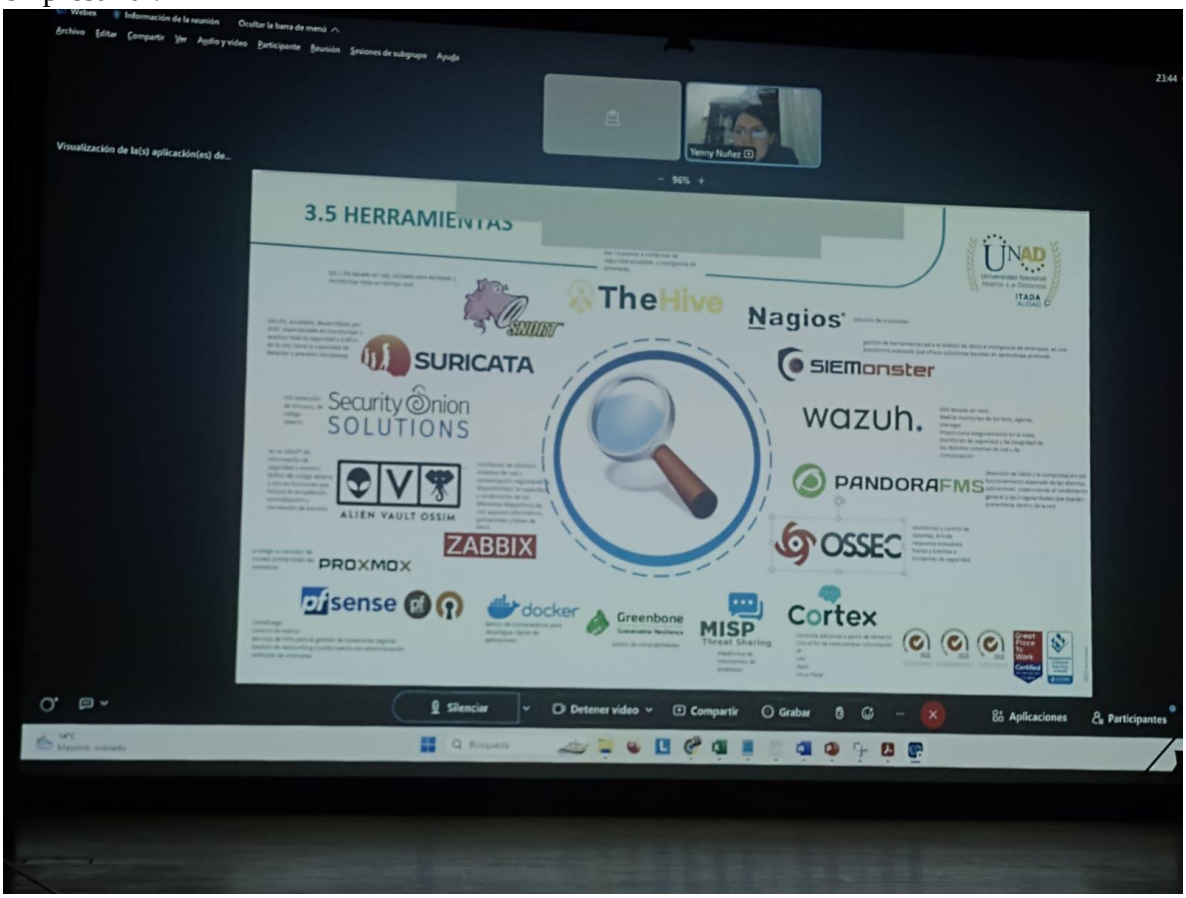
La ingeniera Yenny Muñoz destacó las diversas funciones desempeñadas por estos equipos de ciberseguridad, que abarcan desde el monitoreo y la alerta ante amenazas hasta servicios cruciales de investigación y desarrollo, así como la gestión integral de incidentes. Entre las responsabilidades específicas se incluyen la detección proactiva de amenazas, la investigación de incidentes, el desarrollo de estrategias para contrarrestar vulnerabilidades, la respuesta ante artefactos maliciosos y la coordinación eficiente durante situaciones de emergencia. Estas funciones se combinan para fortalecer la postura de seguridad de la

empresa en todas las etapas, desde la prevención hasta la mitigación y la recuperación.



Posteriormente, la ingeniera Yenny Muñoz expuso diversas herramientas que se pueden emplear para la gestión de la seguridad y la toma de acciones frente a riesgos cibernéticos. Entre estas herramientas se incluyen soluciones de monitoreo avanzado, sistemas de detección de intrusiones, plataformas de análisis de amenazas, y software especializado para la identificación y neutralización de malware. Estas herramientas desempeñan un papel esencial en la optimización de la capacidad de respuesta y la efectividad de los equipos de ciberseguridad ante las crecientes y sofisticadas amenazas en el entorno digital

empresarial.



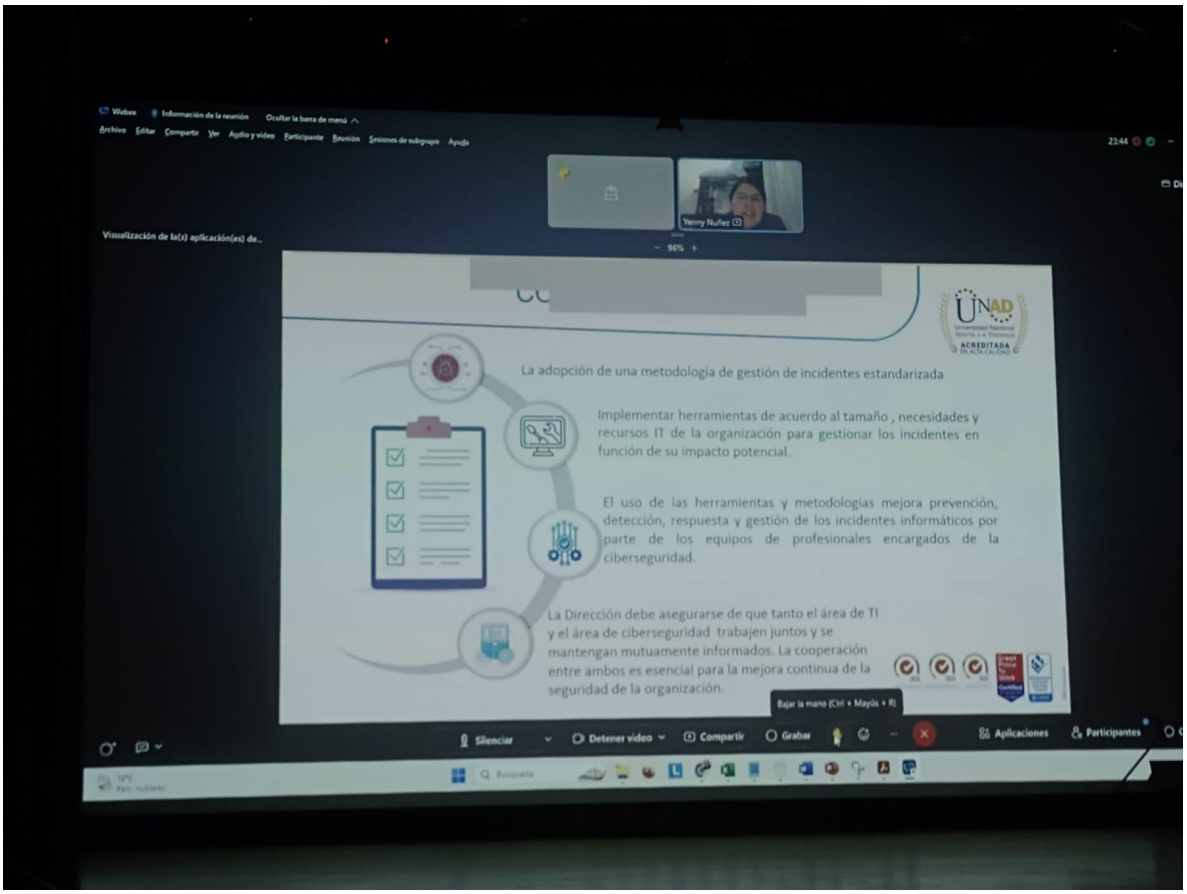
Finalmente, la ingeniera Yenny Muñoz proporcionó una lista de tareas fundamentales que deben considerarse para garantizar una sólida seguridad cibernética:

Implementar una metodología efectiva de gestión de incidentes.

Adquirir y aplicar herramientas que se ajusten a las necesidades específicas y recursos tecnológicos de la empresa.

Fomentar una colaboración estrecha entre el área de Tecnologías de la Información (TI) y el equipo de ciberseguridad para lograr los mejores resultados en términos de protección y respuesta ante amenazas.

Estas acciones son esenciales para establecer y mantener un entorno digital empresarial seguro y resiliente frente a las constantes evoluciones en el panorama de la ciberseguridad.


Webex
Información de la reunión
Ocultar la barra de menú
Archivo Editar Compartir Ver Audio y video Participante Reunión Sesiones de subgrupo Ayuda
23:44
Yenny Nuñez
Visualización de la(s) aplicación(es) de...
96%
UNAD
ACREDITADA EN ALTA CALIDAD
La adopción de una metodología de gestión de incidentes estandarizada
Implementar herramientas de acuerdo al tamaño , necesidades y recursos IT de la organización para gestionar los incidentes en función de su impacto potencial.
El uso de las herramientas y metodologías mejora prevención, detección, respuesta y gestión de los incidentes informáticos por parte de los equipos de profesionales encargados de la ciberseguridad.
La Dirección debe asegurarse de que tanto el área de TI y el área de ciberseguridad trabajen juntos y se mantengan mutuamente informados. La cooperación entre ambos es esencial para la mejora continua de la seguridad de la organización.
Bajar la mano (Ctrl + Mayús + R)
Silenciar
Detener video
Compartir
Grabar
Aplicaciones
Participantes


iSecurity
Summit Colombia
13 y 14 de octubre de 2023
$WHOAMI
Jaider
Rodriguez.
CIBER-TEC
Security and Defense Solutions
bidaidea
GIZEM
UNIVERSIDAD ECCI
Xylextech
colocon
TECNEO
NetSat
certJOIN