Centro de Respuestas a Incidentes Informáticos
CIP - CSIRT Académico UNAD

Boletín Informativo

Número **Siete** – Edición Especial

Primer Encuentro Internacional

CYBERTECH WOMEN UNAD 2022

ECBπ
Escuela de Ciencias Básicas, Tecnología e Ingeniería

VIEM
Vicerrectoría de Innovación y Emprendimiento

Semillero de Investigación
Ceros y Unos

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

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 Siete
Julio 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

Tabla de Contenido

Boletín informativo Número 7

Julio 4 de 2022

CYBERTECH WOMEN UNAD

Autores:

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

Yenny Stella Nuñez Álvarez
ORCID: https://orcid.org/0000-0003-0128-1214

Ana Milena Corregidor Castro
ORCID: https://orcid.org/0000-0003-3949-9454

Introducción

La universidad Nacional Abierta y a Distancia Unad, la Escuela de Ciencias Básicas Tecnología e Ingeniería - ECBTI y sus programas de Especialización en Seguridad Informática e Ingeniería de Sistemas, se han unido para crear CYBERTECH WOMEN UNAD 2022, un espacio virtual académico e investigativo, que busca abordar la ciberseguridad y la tecnología a partir de la experticia de mujeres del sector quienes con sus experiencias, investigación y conocimiento, contribuyen a la apropiación de estas temáticas.

Recuperado de: https://www.freepik.es/

Desarrollo

En que nos inspiramos:

CYBERTECH WOMEN UNAD 2022, busca abordar la ciberseguridad y la tecnología a partir de la experticia, conocimiento y profesionalismo de mujeres profesionales en esta disciplina con un reconocimiento nacional e internacional, que le ha permitido destacarse en el sector, inspirando a otras mujeres con carreras STEM[1] a profundizar en nuevas tendencias, avances, herramientas, técnicas, métodos, estándares, perspectivas y enfoques en las áreas asociadas.

Asimismo, el evento tuvo como propósito recopilar ponencias y póster de las diferentes instituciones educativas, semilleros de investigación y organizaciones públicas y privadas de orden regional, nacional e internacional, permitiendo así, la transferencia y socialización de nuevo conocimiento.

Objetivos planteados en CYBERTECH WOMEN UNAD2022

- ✓ Promover espacios virtuales académicos que permitan el intercambio de experiencias, perspectivas y conocimientos de mujeres en las áreas de ciberseguridad y la tecnología.
- ✓ Estimular la generación de productos de nuevo conocimiento y el desarrollo de nuevas habilidades y capacidades en las líneas temáticas propuestas.
- ✓ Resaltar proyectos académicos y de investigación innovadores realizados por mujeres en distintas temáticas relacionadas con ciberseguridad y tecnología.
- ✓ Valorar el rol de la mujer en el ámbito académico, profesional y productivo desde su desempeño y empoderamiento en las áreas de las TI y la ciberseguridad a través de espacios de reflexión y transferencia de conocimiento.

Recuperado de: https://www.freepik.es/

[1] ¿Qué es STEM? | Ruta STEM (colombiaaprende.edu.co)

Líneas Temáticas Abordadas:

CYBERTECH WOMEN UNAD 2022, desarrollo dos líneas temáticas. Una, enfocada en las disciplinas de la Tecnología y Ciberseguridad, abordando temas relacionados con:

- Multi Cloud Computing y Seguridad en la Nube
- Estándares, Normatividad y Regulación de la Ciberseguridad
- Desarrollo de software seguro
- Ciber inteligencia Integral
- Gestión de Malware
- Análisis Forense
- Criptografía
- Gestión de Riesgos y Vulnerabilidades
- Ciberseguridad industrial
- Ethical hacking
- Resiliencia Cibernética y Continuidad en el Negocio
- Gestión y Respuesta a Incidentes Informáticos.
- Ciberataque y ciberdefensa
-

Y otra, relacionada con Tecnologia, abordando temas, tales como:

- Visión por computadora y aprendizaje automático/autónomo
- Realidad Virtual, Realidad Aumentada y Realidad Mixta
- IoT
- Transferencia de tecnología: Emprendimiento académico y sistemas de innovación
- Ciencias de Datos y Minería de Datos
- Blockchain.
- Gestión de sistemas y bases de datos.
- Big Data
- Inteligencia artificial
- Robótica y Drones.
- Dinámica de sistemas Ingeniería de software
- Redes e infraestructuras tecnológicas.
- Industria 4.0. Sistemas Inteligentes
- Integración de tecnologías convergentes para el mejoramiento de la calidad de vida.
- Diseño de nuevos procesos o productos a partir de la aplicaciones de tecnologias convergentes

Nuestras Ponentes Magistrales:

El encuentro internacional CYBERTECH WOMEN UNAD 2022, permitió compartir, motivar y propiciar una transformación social que favorece el posicionamiento de las mujeres en las áreas de ciberseguridad y la tecnología, a partir de las conferencias magistrales de:

Elizabeth León Guzmán; PhD en Ingeniería y Ciencias de la Computación Ingeniera de Sistemas de la Universidad Nacional , en su conferencia "*Hacia el tratamiento y análisis de datos que contribuya a la transformación digital*" manifiesta que se estima que para el 2025 un crecimiento exponencial de 175 zettabytes de información en el mundo, producto del uso de miles de dispositivos que están generando constantemente transporte cada vez más digital , efectuando muchas tareas automáticas y produciendo muchísimos datos a velocidades muy rápidas. Basado en esta premisa, deja ver su experiencia en la investigación sobre la transformación digital e integración de tecnología digital a procesos, productos, activos para mejorar la eficiencia, descubrir nuevas oportunidades y brindar valor a la organización. Asimismo, destaca la tendencia para tratamiento y análisis de los datos, a partir del uso de la inteligencia artificial por medio de algoritmos avanzados que facilitan estadísticas y capacidades computacionales aplicables en diversas áreas del conocimiento relacionadas a la IoT, Ciberseguridad, Aprendizaje maquinal, E-commerce, entre otros.

Elizabeth León Guzmán
PhD en Ingeniería y Ciencias de la Computación
Ingeniera de Sistemas de la Universidad Nacional
Colombia

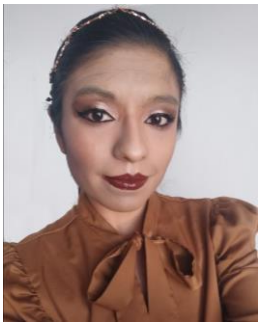
Katherina Canales Madrid; Top Women in Cybersecurity en Latinoamérica, Ex Directora operacional del CSIRT de gobierno, líder en la implementación de programas de concientización sobre seguridad cibernética, experta en estrategias de ciberseguridad, quien nos presenta en su conferencia "*Equipos de respuesta y gestión de incidentes de seguridad informática*", la importancia de la higiene digital, de humanizar la ciberseguridad, de cómo se pueden prevenir incidentes y establecer planes de mitigación con equipos de trabajo integrados por profesionales de perfiles multidisciplinarios, y de cómo fomentar la generación de protocolos de respuesta frente a eventos o incidentes de ciberseguridad. Resaltó la importancia de contar con grupos de respuesta – CSIRT, como estos contribuyen en la generación de métricas y en establecer alianzas entre equipos de respuesta, que contribuyan en mejorar la ciberseguridad de nuestros entornos digitales.

Katherina Canales Madrid
Administradora Publica, licenciada en CS Jurídicas, Co fundadora y COO de la consultora internacional GlobalCyber.
Chile

Berenice Guerra Martinez; Ingeniera en Electrónica. Especialista en Ciberseguridad se ha desempeñado en áreas como soporte técnico en la tecnología de Firewall con experiencia en productos de seguridad Cisco como Firepower y SecureX. Cuenta con experiencia en: Linux, análisis de vulnerabilidades e integración de diferentes soluciones de Seguridad. En su conferencia *"Ciberseguridad en la industria del IoT"* nos lleva a reconocer esa necesidad de integrar IoT[2] con la Ciberseguridad, describe brevemente los ataques destacados a la IoT como Stuxnet 2010, el evento de la planta de energía en Ucrania en 2015 y Mirai Botnet 2016, con el fin demostrar el efecto de las malas prácticas, brechas de seguridad industrial, la falta de actualización de los sistemas operativos y ausencia de parches de seguridad en las Tecnologías de Información y Tecnologías de Operación. Afirmando: "No puedes asegurar lo que no puedes ver", es decir, se debe conocer todo lo que se tiene conectado en la red para determinar lo que se va a proteger, esto con el fin de definir las capas de seguridad requeridas en las infraestructuras TI y TO dentro los procesos industriales y sistemas de información.

Berenice Guerra Martinez
Ingeniera en Electrónica. Especialista en Ciberseguridad
México

Fátima Rodríguez Giles; MSc. en Ingeniería en Seguridad y Tecnologías de la Información y Especialista en criptografía y hacking ético. Ingeniera en Telecomunicaciones. En su conferencia *"Cloud security: ¡hackea la nube!"* realiza un interesante ejercicio práctico sobre cómo se puede configurar la seguridad en servicios alojados en la nube con herramientas de Amazon, exponiendo la versatilidad para el despliegue de servicios y aplicaciones seguras. Además, resalta la ventaja de tener los servicios en la nube para los cuales no se requiere de instalaciones físicas debido a que la compra se realiza únicamente para el procesamiento de módulos específicos que se pueden ejecutar; otras de las ventajas presentadas es la posibilidad de contratar de forma conjunta, con otras personas, entornos de virtualización que son administrados mediante balanzas de carga, estos corresponden a modelos de despliegue que pueden ser públicos, privados o híbridos, según las necesidades particulares de las organizaciones, así es que debido a la importancia de la información, la seguridad de la nube requiere de roles y responsabilidades, resaltando que la seguridad es una responsabilidad compartida, tanto del proveedor como de quien contrata el servicio.



Fátima Rodríguez Giles
MSc. en Ingeniería en Seguridad y Tecnologías de la Información y Especialista en criptografía y hacking ético.
México

[2] ¿Qué es el Internet de las cosas (IoT)? | Oracle Colombia

Posters y Ponencias, Enriquecimiento de la Experiencia:

Carolina Castro Rodríguez y Rafael Alonso Gómez Melo de la Universidad Pedagógica y Tecnológica de Colombia UPTC, en la ponencia "*Delitos informáticos y buenas prácticas de internet en la universidad pedagógica y tecnológica de Colombia sede seccional Sogamoso"* presentan la legislación que permite sancionar los delitos informáticos, y como podemos infringir fácilmente las leyes por falta de conocimiento, "Existen las normas, pero no se conocen", y como en el campus universitario de la UPTC aún está en proceso por establecer políticas internas para una cultura digital en la comunidad estudiantil. Al acceder de manera libre a internet y a las redes sociales en el campus de la Universidad Pedagógica y Tecnológica de Colombia Facultad Seccional Sogamoso, los estudiantes no tienen en cuenta las buenas prácticas de uso, llegando incluso a utilizar la red informática de la Universidad para fines y propósitos incorrectos que podrían ubicarse en el rango de conductas tipificadas en nuestra legislación penal, como delitos informáticos. El desconocimiento jurídico en el uso de internet y las redes sociales, conllevan a que los estudiantes en su gran mayoría incurran en prácticas que de alguna manera estarían transgrediendo bienes jurídicos tutelados por las Leyes Colombianas. Al hacer un análisis del contexto en el que se desarrolla este articulo determinaremos si efectivamente los estudiantes de la U.P.T.C Facultad Seccional Sogamoso, recurren a prácticas que denotan una falta de "cultura informática", y si se hace necesaria la implementación de políticas internas en la Universidad que contemplen acciones encaminadas a la adopción de cultura digital en la comunidad estudiantil.

Yuly Paola Morales Álvarez de la *Universidad Pedagógica y Tecnológica de Colombia UPTC*, en la ponencia *"Fomentando una cultura de paz en la enseñanza del inglés a través de un proyecto basado en el buen uso de las redes sociales "* resalta la importancia de interesarnos en lo que los estudiantes les preocupa; tomando como base el argumento de que en Colombia somos uno de los países de mayor ingreso a redes sociales, y esto tiene efectos de ansiedad sueño, crisis de pánico, depresión e incluso suicidio; por consiguiente, en su proyecto decide incorporar las TIC para aprovechas esa afición por las redes sociales en los procesos de aprendizaje de una segunda lengua. La investigación empleó actividades didácticas y herramientas tecnológicas como Padlet y otras aplicaciones, útiles en la enseñanza del inglés para potenciar un uso responsable de las Redes Sociales como herramienta para promover la Paz a nivel individual y mundial. La razón surge porque las redes sociales y el Internet han ganado mucha aceptación, para unir comunidades diversas en todo el mundo, especialmente jóvenes universitarios. Adicionalmente, con esta investigación asumí una posición colaborativa como docente que realmente se preocupa por las nuevas generaciones que llegan a la universidad en busca de un futuro mejor y un mundo en paz. La necesidad de una educación para la paz está articulada en la Declaración de la UNESCO y el Marco de Acción Integrado sobre Educación para la Paz, los Derechos Humanos y la Democracia y debe articularse con las escuelas y universidades para lograr una mejora en la promoción de las habilidades y actitudes necesarias para una cultura de paz: empatía, tolerancia y respeto por la diversidad y por las diferencias. La Investigación se basó en Cultura de Paz, enseñanza del inglés y el buen uso de las redes sociales haciendo conscientes a los estudiantes acerca de las ventajas y desventajas de ellas.

Juliana Castillo Araujo de la Universidad de Cundinamarca y hace parte del Semillero CREINNG (Creatividad Innovación e Ingeniería), en la ponencia "La seguridad de la información en un mundo moderno" se presenta la importancia de la seguridad informática en base a la información personal, siendo esta una parte fundamental en la privacidad de los datos de cliente-usuario en el flujo monetario de acceso directo para empresas nacionales e internacionales que se dedican desde finales de web 1.0 y comienzos de la web 2.0 a brindar protección de información ingresada en la red gracias al uso de tecnologías de gestión de información en Cloud Computing. A su vez se detalla el auge crecimiento de los tres servicios más usados en la nube en sectores de Infraestructura (Las), Plataforma (PaaS) y Software (SaaS) en donde cada una de estas subscripciones van enfocadas hacia los diferentes tipos de usuarios o empresas lideres en la industria tecnológica como lo son Google, Amazon, Microsoft que durante la reciente pandemia COVID-19 tuvieron que reforzar las áreas STEM (Science, Technology, Engineering and Mathematics) en pro de la información digital a nivel global revolucionando la ciberseguridad informática que se tenía a principios de la primera década del siglo XXI.

Amarilis Almengor de la Universidad Tecnológica de Panamá, en la ponencia *"Desafíos de la seguridad en Multicloud",* expone como el surgimiento de nuevas tecnologías van de la mano nuevos retos, vulnerabilidades y errores por corregir que pueden ser aprovechados por personas con fines maliciosos y poner en riesgo nuestra información y reputación. Las nubes son una nueva forma de infraestructura más flexible, escalable y con un costo más bajo, que se adaptan a las necesidades de las organizaciones. Hoy en día muchas empresas están utilizando más de una nube de distintos proveedores en sus infraestructuras y es importante recalcar que a mayor número de entornos cloud significa una mayor superficie de ataque, y un solo descuido en las configuraciones de seguridad de la nube puede tener efectos negativos con un gran impacto. Por ello se debe encontrar una forma para asegurar los entornos Multi Cloud de manera centralizada con un enfoque único que entrelace las funciones de seguridad y de red. En este sentido es muy importante tener en cuenta que la seguridad en la nube es una responsabilidad compartida del proveedor.

Angela Esperanza Saavedra y Santiago Hernando de la Fundación Universitaria Juan de Castellanos y hacen parte del Semillero TECSI , en la ponencia "*Realidad aumentada como recurso tecnológico en el proceso enseñanza-aprendizaje, área de ciencias naturales grados 3°, 4° y 5° en la Institución Educativa Luis Antonio Escobar del Municipio de Villapinzón*" presentan un interesante trabajo con la realidad aumentada como recurso tecnológico en el proceso enseñanza-aprendizaje, para los niños, empleando un diagrama de necesidades, a fin de dinamizar la forma de transmitir las temáticas para que logren una mayor comprensión. Asimismo, buscando mejorar el desarrollo de su aprendizaje en especial en el área de las ciencias naturales de forma más interactiva.

Sarai Pérez de la Universidad Tecnológica de Tula Tepeji (México) y Galoget Latorre Hackem Cybersecurity Research Group (Ecuador) , en la ponencia *"Técnicas de ataque a contraseñas en una era post-pandemia",* exponen como el cracking de contraseñas como un problema de seguridad en las empresas y también para individuos. Las técnicas utilizadas por cibercriminales en una era post-pandemia, ¿qué ha cambiado?, ¿qué se ha mantenido?, donde se ve de primera mano varias técnicas que se usan para obtener o recuperar contraseñas en texto claro, para realizar este proceso hacen uso de diferentes herramientas, desde identificar el tipo de algoritmo hash que se aplicó y de esta manera sea más fácil el descifrar la contraseña, por otra explican las herramientas que permiten atacar a un determinado servicio y poder obtener el texto plano, donde nombran algunas de las técnicas más comunes como: ataques de fuerza bruta y ataque de diccionario. De esta manera los ciber - atacantes pueden tener rápidamente acceso no autorizado al sistema o cuentas de la víctima.

Azul Garcia de la Universidad Tecnológica de Tula Tepeji (México) y Galoget Latorre Hackem Cybersecurity Research Group (Ecuador), en la ponencia "Creación de entornos honeypot como *estrategia de defensa en redes corporativas"* donde hablan desde el lado del defensor con creación de entornos Honypot, un complemento de como capturar evidencia de como los cibercriminales buscan atacarnos, y es importante desviarlos. Un Honeypot, también conocido como "trap system" o "señuelo", reside dentro de una red o sistema informático, y por tanto su finalidad es evitar posibles ataques que se produzcan en las redes de una organización. La función principal de esta herramienta es detectar y obtener información sobre ataques informáticos, especialmente sobre el origen de los ataques, técnicas utilizadas y herramientas, para que posteriormente se puedan tomar las medidas de seguridad necesarias. Los Honeypots actuales son realmente potentes y nos permiten "simular" el comportamiento real del sistema, convenciendo al ciberdelincuente de que se ha infiltrado en un sistema real y que puede tomar el control fácilmente. Sin embargo, estarán en un sistema aislado y podremos ver exactamente qué están haciendo y qué vulnerabilidades están tratando de explotar. Podemos configurar diferentes escenarios con Honeypots para que actúen como medidas de seguridad de diferentes formas. Gracias a las herramientas Honeypot, es posible detectar formas de ataque previamente desconocidas y detectar vulnerabilidades específicas de nuestra red, de manera que se puedan desarrollar estrategias de seguridad y soluciones de protección más efectivas.

POSTERS

El evento se enriqueció con la presentación de los video-posters en donde se presentaron interesantes trabajos de investigación sobre diferentes temáticas relacionadas con tecnología y ciberseguridad y que se resaltan a continuación.

Tabla 1. *POSTERS PRESENTADOS EN CYBERTECH WOMEN UNAD 2022*

Título Póster	Autores
• Análisis del estado de emergencia sanitaria- covid 19 y la implementación de medidas de seguridad informática en el uso de canales electrónicos y la gestión de documentos electrónicos en ambientes de trabajo en casa	Clara Inés Muñoz Universidad Nacional abierta y a distancia UNAD.
• Análisis de efectividad de la autenticación y control de acceso IMS-AKA como mecanismo de protección de integridad y confidencialidad de la información en los servicios basados en IP	Andrea Tatiana Romero Universidad Nacional abierta y a distancia UNAD.
• Análisis de la seguridad del protocolo de transporte MQTT en dispositivos para internet de las cosas	Paulita Flor Salazar Universidad Nacional abierta y a distancia UNAD.
• Construyendo entidades ciberseguras y resilientes	Shary Llanos - Adriana Jaramillo Universidad Nacional UNAL- Del Laboratorio al Campo - DLC
• Análisis de los protocolos de seguridad inalámbrica implementadas en las redes wifi en la ciudad de Bogotá	Jeimy Tatiana Pérez Universidad Nacional abierta y a distancia UNAD.
• Desafíos de seguridad en Multi Cloud	Amarilis Almengor Universidad Tecnológica de Panamá

Elaboración propia

TRABAJOS DE INVESTIGACIÓN DESTACADOS Y QUE FUERON GANADORES EN CYBERTECH WOMEN

TABLA 2 TRABAJOS CON MENCIÓN DE HONOR CYBERTECH WOMEN

TITULO	AUTORES	PUESTO
• Desafíos de seguridad en MULTI CLOUD	Amarilis Almengor Universidad Tecnológica de Panamá	PRIMER LUGAR PONENCIA
• Creación de entornos HONEYPOT como estrategia de defensa en redes corporativas	Azul García Universidad Tecnológica de Tula Tepeji (México) Galoget Latorre Hackem Cybersecurity Research Group (Ecuador)	SEGUNDO LUGAR PONENCIA
• Fomentando una cultura de paz en la enseñanza del inglés a través de un proyecto basado en el buen uso de las redes sociales	Yuly Paola Morales Álvarez Universidad Pedagógica y Tecnológica de Colombia UPTC	TERCER LUGAR PONENCIA
• Desafíos de seguridad en MULTI CLOUD	Amarilis Almengor Universidad Tecnológica de Panamá	PRIMER LUGAR EN POSTER
• Análisis de la seguridad del protocolo de transporte MQTT en dispositivos para internet de las cosas	Paulita Flor Salazar Universidad Nacional abierta y a distancia UNAD.	SEGUNDO LUGAR EN POSTER
• Construyendo entidades ciberseguras y resilientes	Shary Llanos Antonio Universidad Nacional UNAL- Del Laboratorio al Campo - DLC	TERCER LUGAR POSTER
• Construyendo entidades ciberseguras y resilientes	Adriana Jaramillo Universidad Nacional UNAL- Del Laboratorio al Campo - DLC	

Elaboración propia

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] Ruta STEAM [en línea]. Colombia Aprende [fecha de consulta: 30/06/2022] Disponible en: https://especiales.colombiaaprende.edu.co/rutastem/definicion.html#:~:text=El%20t%C3%A9rmino%20STEM%20apareci%C3%B3%20por,%C3%A1reas%20(Bybee%2C%202013).

[2] ¿Qué es el IoT? [en línea]. Oracle [fecha de consulta: 30/06/2022] Disponible en: https://www.oracle.com/co/internet-of-things/what-is-iot/