UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

PROTOCOLO PARA WEBINAR: TECNOLOGÍAS PARA MITIGAR VULNERABILIDADES Y COMBATIR LA DESINFORMACIÓN

Código documento:	*DCCO-V1-2024- 063*
Versión:	V2.0
Fecha de la versión del documento:	2024-12-10
Nivel de confidencialidad:	Interno

ÍNDICE

A. INTRODUCCIÓN

En un mundo digitalizado donde la información es un activo crítico, la seguridad informática y la veracidad de los datos han adquirido un rol estratégico en la construcción de confianza y en la protección de los sistemas digitales. La proliferación de ciber amenazas, la creciente dependencia de los servicios en línea y la necesidad de verificar la autenticidad de la información han llevado a organizaciones y profesionales a priorizar estrategias tecnológicas que fortalezcan la seguridad y la transparencia en el entorno digital como medios de información.

Este webinar, titulado "Tecnologías para Mitigar Vulnerabilidades y Combatir la Desinformación", se organiza como una respuesta oportuna a estas demandas actuales. Está dirigido especialmente a estudiantes de últimos semestres, graduados, docentes y personal técnico o profesional interesados en adquirir conocimientos actualizados y herramientas prácticas en ciberseguridad y verificación digital.

La Universidad de las Fuerzas Armadas-ESPE, a través del Departamento de Ciencias de la Computación, reafirma su compromiso con la formación continua y la transferencia de conocimiento al ofrecer este espacio académico. Las ponencias estarán a cargo de expertos reconocidos en los campos de la ciberseguridad y la tecnología de validación de datos, quienes compartirán su experiencia y perspectivas sobre los desafíos y oportunidades en este ámbito.

Con esta iniciativa, se busca no solo fortalecer las capacidades técnicas de los participantes, sino también fomentar una comunidad académica y profesional comprometida con el desarrollo de soluciones innovadoras que promuevan la seguridad, integridad y veracidad en el entorno digital. Este evento representa una oportunidad única para explorar tendencias emergentes, interactuar con líderes del sector y aplicar los conocimientos adquiridos en contextos reales y profesionales.

B. OBJETIVO GENERAL

Promover el fortalecimiento de las competencias técnicas y académicas de estudiantes de últimos semestres, graduados, docentes y profesionales interesados en ciberseguridad y verificación digital, este evento tiene como propósito principal proporcionar un espacio de aprendizaje y análisis donde los participantes puedan explorar estrategias tecnológicas innovadoras, comprender los desafíos actuales en la seguridad de la información y la veracidad de la información en medios digitales, e identificar herramientas prácticas aplicables en sus contextos académicos y profesionales.

C. OBJETIVO ESPECÍFICOS

- Presentar los avances en estrategias tecnológicas para la ciberseguridad y la verificación de información de medios digitales, destacando casos prácticos y experimentales que faciliten la comprensión de su aplicación en entornos profesionales y académicos.

- Fomentar el intercambio de conocimientos entre estudiantes, graduados, docentes y profesionales, promoviendo la construcción de redes colaborativas enfocadas en la investigación y desarrollo de soluciones para fortalecer la seguridad y veracidad digital.

D. ALCANCE

El webinar se realizará en modalidad híbrida, permitiendo la participación tanto virtual como presencial para mayor accesibilidad. Está dirigido principalmente a estudiantes de los últimos semestres y egresados de carreras tecnológicas, con especial énfasis en aquellos de la carrera de Tecnología Superior en Redes y Telecomunicaciones. Este evento busca ofrecer conocimientos prácticos y aplicables a los futuros profesionales de carreras tecnológicas en temas relacionados con la ciberseguridad y la inteligencia artificial. Asimismo, se extiende la invitación a participantes de todas las carreras de la Universidad de las Fuerzas Armadas ESPE, fomentando el aprendizaje integral y actualizado.

E. GLOSARIO DE TÉRMINOS

Ciberseguridad: Conjunto de prácticas, tecnologías y políticas diseñadas para proteger sistemas, redes y datos contra ciberataques y accesos no autorizados.

Desinformación: Información falsa o engañosa que se difunde deliberadamente con la intención de manipular, confundir o influir en la percepción pública.

Modalidad Híbrida: Forma de realizar eventos que combina la participación presencial y virtual, permitiendo flexibilidad y accesibilidad a los asistentes.

Verificación Digital: Proceso de validación de la autenticidad y exactitud de la información disponible en medios digitales, mediante herramientas tecnológicas y análisis de datos.

Certificados TLS (Transport Layer Security): Protocolos criptográficos que aseguran las comunicaciones a través de redes, proporcionando confidencialidad y protección contra accesos no autorizados.

Machine Learning (Aprendizaje Automático): Rama de la inteligencia artificial que permite a los sistemas aprender y mejorar automáticamente a partir de datos sin ser programados explícitamente.

Vulnerabilidades Digitales: Fallos o debilidades en un sistema informático o red que pueden ser explotados por atacantes para comprometer su seguridad.

F. DISPOSICIONES GENERALES

- Coordinar la participación de los expositores, asegurando su disponibilidad y la provisión de los recursos tecnológicos requeridos para el adecuado desarrollo del evento.
- Promover la difusión del evento mediante los canales institucionales, incluyendo correo electrónico, redes sociales y el micrositio oficial de la carrera, garantizando su alcance a la audiencia objetivo.
- Asegurar la correcta inscripción y registro de los participantes, facilitando su acceso a la plataforma de reuniones virtuales y brindando soporte técnico cuando sea necesario.
- Diseñar y emitir certificados digitales para los expositores, gestionando su entrega posterior a la culminación del evento.
- Llevar a cabo pruebas técnicas de conexión con los expositores antes del evento, y supervisar la operatividad de las herramientas tecnológicas durante el desarrollo del webinar.
- Designar personal capacitado para moderar el evento, gestionar los tiempos de intervención de los ponentes y coordinar la interacción con los asistentes.
- Supervisar el cumplimiento del cronograma establecido, garantizando que las actividades planificadas se desarrollen según lo previsto y resolviendo de manera eficiente cualquier eventualidad que pudiera surgir.
- Presentar a las autoridades competentes un informe detallado sobre el desarrollo y resultados del evento, incluyendo evidencias documentales y análisis de los logros alcanzados.

G. DISPOSICIONES ESPECÍFICAS

Organización:

- Coordinar la agenda con los ponentes y confirmar los temas a tratar, alineándolos con los objetivos del webinar.
- Realizar pruebas técnicas de conexión y calidad de audio/video para garantizar la operatividad de la plataforma y los equipos presenciales.
- Preparar los recursos audiovisuales y logísticos necesarios para la modalidad presencial, incluyendo espacios adecuados y materiales de apoyo.

Promoción:

- Difundir las invitaciones a través de redes sociales, correos electrónicos institucionales y carteleras digitales para maximizar la participación.
- Diseñar y publicar un afiche publicitario digital que incluya información clave sobre el webinar, los ponentes y los horarios.
- Coordinar con las unidades académicas para garantizar la promoción en todas las sedes y extender la invitación a egresados.

Ejecución:

- Garantizar el soporte técnico continuo durante el evento, resolviendo cualquier inconveniente que surja en las modalidades virtual o presencial.
- Designar un moderador para coordinar las intervenciones, gestionar las preguntas de los asistentes y asegurar un flujo adecuado en las sesiones.
- Registrar las sesiones virtuales y presenciales para su posterior análisis y difusión entre los asistentes registrados.

Seguimiento:

- Elaborar un informe final que detalle las actividades realizadas, los resultados obtenidos y las recomendaciones para mejorar futuros eventos.
- Compartir las grabaciones y materiales del webinar con los participantes registrados, fomentando un aprendizaje continuo.

H. ANEXOS :

1. Cronograma de actividades

EVENTO	**WEBINAR: SEGURIDAD Y TECNOLOGÍA EN ECUADOR**
FECHA	13 de diciembre de 2024
HORARIO	10H30 – 11H30 10H35: Implementación de certificados TLS gratuitos para servicios virtuales: Un enfoque experimental en Proxmox VE. Ing. Raúl Gallegos Herrera. 11H05: Comparación de algoritmos de aprendizaje automático en la detección de noticias falsas contrastando información de medios digitales. Ing. Milton Escobar Sánchez.
DURACIÓN	1 hora
LUGAR	Auditorio B del Campus de Belisario Quevedo Modalidad Virtual y Presencial
PARTICIPANTES	Graduados de la Carrera de Tecnología Superior en Redes y Telecomunicaciones Estudiantes de 3 y 4 semestre de carreras de Tecnología.
ORGANIZADOR Y DIRECCIÓN DEL EVENTO	Ing. Verónica Tintín Ing. Alvaro Uyaguari
DOCENTES COLABORADORES DEL EVENTO	Ing. Verónica Tintín Ing. Alvaro Uyaguari
ACTIVIDADES	Inauguración del evento. Desarrollo del evento. Clausura del evento.

I. CONTROL DE CAMBIOS

Fecha	Versión	Elaborado por	Descripción de la modificación
10 de diciembre de 2024	1	Ing. Verónica Tintín P., Mgtr Departamento de Ciencias de la Computación	Versión Inicial

J. APROBACIÓN

Rubro	Nombre	Unidad/Cargo	Firma
Elaborado por:	Ing. Verónica Tintín P., Mgtr.	Departamento de Ciencias de la Computación/Docente	Firmado electrónicamente por: VERONICA PAULINA TINTIN PERDOMO
	Ing. Alvaro Uyaguari., Mgtr.	Departamento de Ciencias de la Computación/Docente	Firmado electrónicamente por: ALVARO DANILO UYAGUARI UYAGUARI
Revisado por:	Ing. Jorge Pardo., Mgtr.	Director de la Carrera de Tecnología Superior en Redes y Telecomunicaciones	Firmado electrónicamente por: JORGE ALBERTO PARDO IBARRA
Aprobado por:	Ing. Patricio Navas, Mgtr.	Director Subrogante del Departamento de Ciencias de la Computación	Firmado electrónicamente por: MILTON PATRICIO NAVAS MOYA