DEL CONOCIMIENTO A LA ACCIÓN

III ENCUENTRO IBEROAMERICANO DE BLOCKCHAIN Y CIBERSEGURIDAD

ESTRATEGIAS TEMÁTICAS PARA LA FORMACIÓN DE UN CSIRT EN CIBERDEFENSA

Fabián Castillo Peña

CONTEXTO

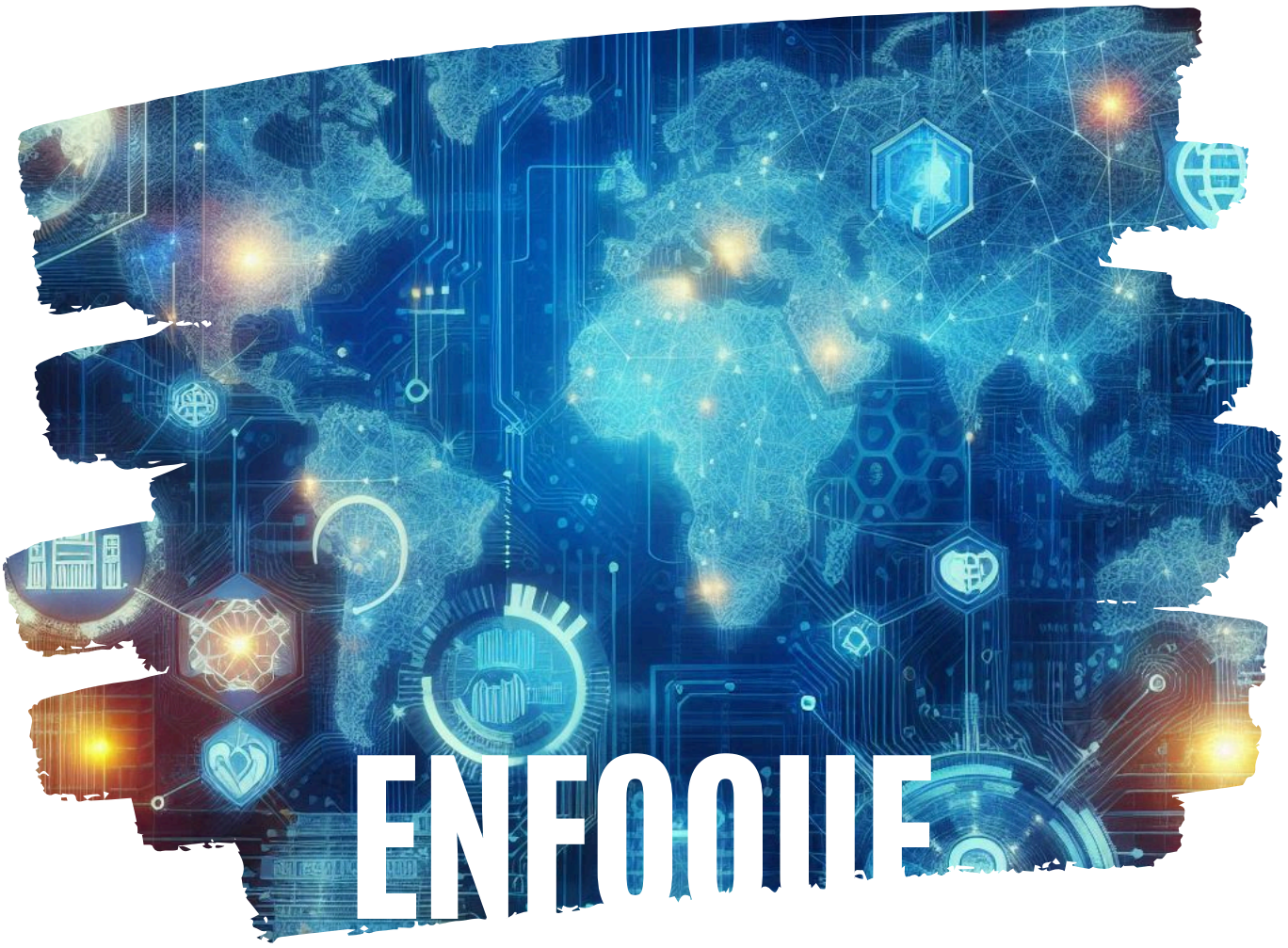
Organización con misión en seguridad y defensa.

Fortalecer su capacidad de respuesta.

Ante incidentes digitales.

Ingenieros, oficiales, técnicos de sistemas e investigadores.

Activos digitales, redes críticas, infraestructura híbrida y enlaces con entidades nacionales e internacionales



Evaluación de tiempo de respuesta, coordinación y liderazgo digital.

Ejercicios de toma de decisiones tácticas y estratégicas.

Escenarios de crisis cibernética militar (ataques a redes y control, telecomunicaciones).

Simulación de entornos críticos con interferencia, presión y escalamiento.

Juegos de guerra digital (War Games) con Red, Blue y White Team.

Red RIBCi
Red Iberoamericana de Blockchain y Ciberseguridad

CYTED

Universidad Libre

UxTIC

COTECMAR

UCLM Universidad de Castilla-La Mancha

Universidad de Chile

UNITECNAR

UdeCataluña

alitic

Los Libertadores

UCASAL

Universidad Tecnologica Nacional

ESTRATEGIAS

Fundamentos de TIC a...

Formación teórica-práctica co...

Desarrol...

Talleres de...

Gestión de Incidentes...

Simulación de incidentes rea...

Ciberint...

Entrenamie...

Sistemas Operativos (L...

Laboratorios prácticos, gestió...

Análisis Forense Digital

Recolección de evidencia, ca...

Redes y Segurid...

Diseño, simulación y...

Bases de Datos...

Gestión de bases, co...

Normativa, y éti...

Análisis jurídico y éti...

Simulación de...

Ejercicios conjuntos...

Red RIBCi
Red Iberoamericana de Blockchain y Ciberseguridad

CYTED

Universidad Libre

UxTIC

COTECMAR

UCLM Universidad de Castilla-La Mancha

Universidad de Chile

UNITECNAR

UdeCataluña

alitic

Los Libertadores

UCASAL

Universidad Tecnologica Nacional

Evaluación de tiempo de respuesta, coordinación y liderazgo digital.

Ejercicios de toma de decisiones tácticas y estratégicas.

Simulación de entornos críticos con interferencia, presión y escalamiento.

Escenarios de crisis cibernética militar (ataques a redes y control, telecomunicaciones).

Juegos de guerra digital (War Games) con Red, Blue y White Team.

Red RIBCi
Red Iberoamericana de Blockchain y Ciberseguridad

CYTED

Universidad Libre

UxTIC

COTECMAR

UCLM Universidad de Castilla-La Mancha

Universidad de Chile

UNITECNAR

UdeCataluña

alitic

Los Libertadores

UCASAL

Universidad Tecnologica Nacional

LECCIONES

Principales resultados:

· Reducción en los...

· Mejora en la com...

· Implementación de un plan de actual...

Lecciones clave:

· La formación téc...

· Es fundamental v...

· La integración de TIC en la formación...

Red RIBCi
Red Iberoamericana de Blockchain y Ciberseguridad

CYTED

Universidad Libre

UxTIC

COTECMAR

UCLM Universidad de Castilla-La Mancha

Universidad de Chile

UNITECNAR

UdeCataluña

alitic

Los Libertadores

UCASAL

Universidad Tecnologica Nacional

CONCLUSIONES

Formar un CSIRT es consolidar la primera línea de defensa de la infraestructura crítica a través del conocimiento.

Fortalecer las capacidades del equipo permiten anticipar amenazas, proteger la soberanía y transformar el conocimiento en defensa activa.

La formación de un CSIRT debe concebirse como un proceso integral, escalonado y adaptado a las amenazas reales del entorno donde opera.

El paso del conocimiento a la acción requiere planificación, evaluación continua y una conexión directa con los referentes de ciberdefensa.

Las estrategias temáticas basadas en TIC aplicadas al contexto de defensa son esenciales para dotar al equipo de competencias sólidas.

Red RIBCi
Red Iberoamericana de Blockchain y Ciberseguridad

CYTED
Ciencia y Tecnología para el Desarrollo

Universidad Libre

UxTIC
Red de Universidades

COTECMAR

UCLM Universidad de Castilla-La Mancha

Universidad de Chile

UNITECNAR

UdeCataluña

alitic
Formamos Líderes para el Futuro

Los Libertadores
Fundación Universitaria
Acreditación Institucional en Alta Calidad

UCASAL

Universidad Tecnológica Nacional