



Centro de Respuestas a Incidentes Informáticos
CIP - CSIRT Académico UNAD

Boletín Informativo - Técnico Número Nueve

Cyber Ranges

Un espacio de entrenamiento para el talento humano relacionado
con Ciberseguridad



INSTITUCIÓN UNIVERSITARIA
COLEGIO MAYOR DEL CAUCA



RedCIC
Red Colombiana de Investigación en
Ciberseguridad

VIEM
Vicerrectoría de Innovación
y Emprendimiento

ECBTI
Escuela de Ciencias
Básicas, Tecnología
e Ingeniería



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 Nueve
Septiembre de 2022

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

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CIP – CSIRT Académico UNAD

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>

Licencia Atribución – Compartir igual





Tabla de Contenido

Boletín informativo Número 9	4
Introducción	4
Desarrollo	5
Concepto de Cyber Ranges:	5
Características de un Cyber Ranges	5
Que Beneficios Conlleva su implementación	6
Tipos de Cyber Ranges	7
Algunas plataformas por conocer respecto a Cyber Range	8
Canales de comunicación	8
Recursos Bibliográficos Consultados	9



Cyber Ranges

Un espacio de entrenamiento para el talento humano relacionado con Ciberseguridad

Autores:

Fernando Zambrano Hernández
CIP – CSIRT Académico UNAD
<https://orcid.org/0000-0002-4690-3526>

Yeiner David Chicunque Zemanate
Colegio Mayor del Cauca
<https://orcid.org/0000-0002-6299-3154>

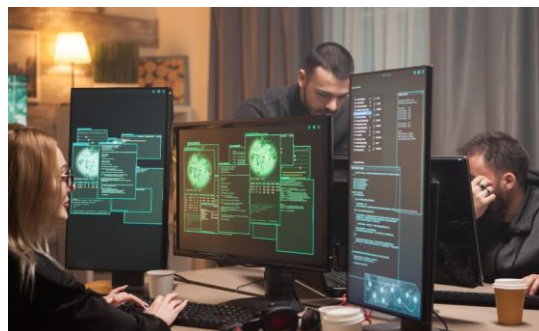
Carlos Julio Muñoz Rengifo
Colegio Mayor del Cauca
<https://orcid.org/0000-0003-3602-0364>

Katerine Marceles Villalba
Colegio Mayor del Cauca
<https://orcid.org/0000-0002-4571-0714>

Introducción

La necesidad de resguardar los entornos digitales de las organizaciones exige tres aspectos fundamentales: Infraestructura tecnológica que permita dar respuesta a un evento o incidente informático, procesos y procedimientos bien definidos que brinden lineamientos claros en caso de presentarse alguno de estos y un talento humano experto el cual integre lo mencionado de forma anterior, con el fin de dar respuesta a este requerimiento.

El presente boletín se construye a través de un trabajo articulado con el Colegio Mayor del Cauca y la Red Colombiana en Ciberseguridad - REDCIC y socializa una estrategia que aporta en la reducción de brechas de ciberseguridad y fortalece las capacidades de un equipo de respuesta.



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



Desarrollo

Concepto de Cyber Ranges:

Un **Cyber Range** es un tipo de plataforma virtualizada que básicamente simula entornos operativos reales que comprenden representaciones interactivas de redes y sistemas organizacionales locales, con herramientas y aplicaciones que brindan un entorno igualmente realista, seguro y legal. Es importante mencionar que éstos se caracterizan por ser estáticos o desplegables, clasificados o no clasificados, siendo su propósito la formación y el entrenamiento individual o colectivo del personal interesado en el área de la ciberseguridad.¹

De este modo, se logra capacitar a profesionales dentro de escenarios prácticos que replican la realidad con simulaciones de ciber amenazas de alta fidelidad, obviamente con toda la infraestructura de los dispositivos de red, servidores y hosts específicamente ajustados y similares a un entorno real para el entrenamiento.

Por otro lado, también permiten la experimentación, pruebas y validaciones de nuevas herramientas con sus respectivas tecnologías, conceptos, técnicas y tácticas que giran y son aplicadas a la ciberseguridad y ciberdefensa dentro de los sistemas.



Recuperado de: <https://securityintelligence.com/>

Características de un Cyber Ranges

Si se destaca la eficacia de un cyber range, es posible identificar las siguientes características²:

- **Accesibilidad:** Puede ser usada por profesionales que posean autorización.
- **Entorno seguro:** Una cyber range debe proporcionar un entorno donde los usuarios puedan acceder a procesos de formación y entrenamiento, sin poner en riesgo a los sistemas en producción y la información.
- **Escalabilidad y flexibilidad:** Estas características se basan en poder dar respuesta adecuada a aquellas necesidades de los profesionales en ciberseguridad en razón de los escenarios particulares (personalización y control) de las tareas que se deseen desarrollar

¹Recuperado de: <https://www.realinstitutoelcano.org/cyber-range-una-capacidad-estrategica>

²Recuperado de: <https://ruiacollege.org/software/penteston>. [Último acceso: 09 2022]



Que Beneficios Conlleva su implementación

Es menester resaltar que cuando las organizaciones adquieren un **Cyber Range**, no solo obtienen un sistema para realizar pruebas y prácticas de entorno a amenazas cibernéticas, sino además pueden aprender diferentes aspectos como son:

Aprender sobre identificación y defensa frente a los vectores de ataque

Actualmente la tecnología y sus aplicaciones avanzan continuamente y también lo hacen los vectores y las herramientas que son utilizadas contra los sistemas y las redes de información, así que, un enfoque efectivo para capacitar al personal de seguridad es a través de escenarios realistas, donde se enfrenten a un malware, errores y actividad de red maliciosa, permitiendo estar prevenido frente a un ataque en la vida real.

Con la constante practica se puede llegar a identificar y responder a las amenazas de forma más rápida y eficaz, tomando diferentes enfoques, como son:

- Identificación de patrones de amenazas de seguridad comunes.
- Reconocimiento del comportamiento anormal de la red o del sistema para su identificación y respuesta eficaz a incidentes.
- Protección de sistemas críticos e infraestructura vital para el funcionamiento de la organización.
- Trabajo colaborativo y mitigación de daños bajo prácticas y procedimientos de respuesta a incidentes.

Oportunidades de desarrollo profesional a los equipos de ciberseguridad.

La ciberseguridad es una industria que exige el continuo aprendizaje, debido a la constantes evolución de las amenazas en términos de innovación y adaptación. Es así, como los profesionales siempre deben estar en una constante adaptación y entrenamiento para fortalecer sus conocimientos y obtención de experiencia, como también, el desarrollo de nuevas habilidades para el fortaleciendo de su perfil profesional frente a un entorno laboral demandado, pero poco ofertado hoy en día.

Gracias a los **Cyber Ranges** y sus entornos de pruebas, permite a las organizaciones una forma de capacitar a los nuevos empleados para que reconozcan los aspectos clave de un ataque cibernético, mediante una formación práctica dentro de entornos muy similares a las organizaciones y la infraestructura que ellos posean y deseen proteger

Perfeccionamiento de habilidades para el uso de las herramientas de seguridad usadas en un entorno real.

Un Cyber Range implementado en una organización permite un alto nivel de personalización para replicar con precisión la configuración de redes, hosts, servidores y otras características que permiten la evaluación de los efectos



cuando se realizan cambios en las reglas del firewall, la efectividad de las nuevas herramientas de seguridad o la confiabilidad de los antivirus.

Lo anterior, permitiendo que antes de realizar un cambio en el entorno de producción real o se implemente una nueva herramienta dentro de la organización, los equipos (profesionales y empleados) sabrán exactamente cómo responderán las operaciones de la empresa, dejando a un lado el grado de incertidumbre que se produce cuando se debe realizar cambios o actualizaciones de los sistemas a nivel organizacional

Tipos de Cyber Ranges

Debido a que los usos de los **Cyber Ranges** son variados, estos se pueden alojar en varios entornos, escalas o necesidades de las organizaciones que los requieran, es así como generalmente se clasifican así

A nivel local dentro de las instalaciones de la organización.

Los **Cyber Ranges** locales se alojan en el sitio físico dentro de la infraestructura de una organización específica y, cuyas instalaciones usan equipos dedicados que son propiedad de la organización y están diseñados en un entorno similar a un laboratorio. Por lo general, están diseñados para replicar sus sistemas de producción, políticas y configuraciones existentes o un determinado entorno de prueba.

Al estar un **Cyber Ranges** dentro de las instalaciones tiene sus beneficios en términos de la capacidad de adaptabilidad a necesidades específicas o preocupaciones de seguridad, pero, el nivel de esfuerzo y recursos para implementar y mantener este tipo de **Cyber Ranges** es mayor debido a las necesidades de un espacio físico, sistemas, mantenimiento y personalización del entorno.

Servicio de Cyber Range basado en la nube.

Para las organizaciones con un **Cyber Range** basado en nube, le proporciona una infraestructura flexible, fácilmente reconfigurable y rentable que también puede ser un entorno aislado, seguro y controlado. Además, al estar basados en la nube, también poseen características de escalabilidad y modificación según las necesidades de capacitación para los profesionales y el presupuesto de la organización, solo se debe realizar un acuerdo con el proveedor externo del servicio en nube contratado.

Las organizaciones pueden fijar costos más predecibles y accesibles, ya que la implementación y mantenimiento se deja en manos del proveedor como parte de las tarifas del servicio acordado. Además, estos proveedores poseen capacitaciones previamente diseñadas o poseen la capacidad de crear una según las necesidades que se requieran, esto contribuyendo aún más a minimizar los costos potenciales de las organizaciones al momento de usar un **Cyber Range**.



Cyber Range mediante soluciones de virtualización remota.

Este tipo de **Cyber Range** combina aspectos de la infraestructura en la nube y a nivel local, mediante el uso de una red de máquinas virtuales centralizadas, el cual son gestionadas a través de acceso remoto por los usuarios. Esto hace que realice una gestión centralizada con una conectividad más diversa y flexible a través de redes privadas virtuales o un servicio de acceso remoto para los involucrados.

Algunas plataformas por conocer respecto a Cyber Range

A continuación, se comparten algunas plataformas similares a un **Cyber Range** cuyo propósito fundamental es entrenar mediante practicas a los profesionales frente a entorno reales de ataques o uso de herramientas de ciberseguridad son:

- **HackTheBox**: Es una plataforma en línea que permite probar habilidades frente a escenarios de prueba de penetración.
- **Vulnhub**: Proporciona materiales que permiten a cualquier persona adquirir experiencia práctica en seguridad digital, software informático y administración de redes.
- **TryHackMe**: Es una plataforma en línea para aprender y enseñar ciberseguridad.
- **PwnTillDawn Online Battlefield**: Es una plataforma en línea que permite poner en práctica las habilidades ofensivas de seguridad y técnicas de penetración al descubrir y explotar vulnerabilidades en laboratorios controlados.
- **LetsDefend**: Plataforma en línea de capacitación en respuesta a incidentes y análisis de SOC para miembros del equipo azul.
- **PENTESTON**: Es una plataforma que permite acceder a más de 40 herramientas, el cual se encuentran preconfiguradas para entrenar las habilidades de ciberseguridad.
- **Hackbox**: Plataforma de código abierto el cual facilita la práctica en sistemas vulnerables para mejorar las habilidades en ciberseguridad.
- **HackThisSite**: Plataforma de acceso gratuito, donde los usuarios pueden probar y mejorar sus habilidades de piratería.

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] C. R. u. c. Estratégica, «Real Instituto Elcano,» 12 12 2016. [En línea]. Recuperado:
<https://www.realinstitutoelcano.org/cyber-range-una-capacidad-estrategica/>

[2] A. a. PENTESTON, «Ruiacollege.org,» 9 07 2021. [En línea]. Recuperado: <https://ruiacollege.org/software/penteston>.
[Último acceso: 09 2022].