NIRIEN

CBRT

Cybersecurity Blue & Red Team

# Conoce lo que hacemos

NIRIEN CBRT
Cybersecurity Blue & Red Team

# Índice de contenidos

NIRIEN CBRT
Cybersecurity Blue & Red Team

CISO
CHIEF INFORMATION SECURITY OFFICER

# CISO Virtual

- Planificación estratégica
- Políticas y procedimientos
- Gestión de riesgos
- Clasificación de la Información
- Respuesta a Incidentes
- Preparación Auditoria
- Auditoria Cumplimiento
- Evolución Proveedores
- Mapa de Amenazas
- Evaluación de ciberseguridad
- Gestión de brechas

NIRIEN CBRT
Cybersecurity Blue & Red Team

# Respuesta a incidentes cibernéticos

Ayudamos a las organizaciones durante y después de los incidentes cibernéticos ayudándolos a comprender y navegar por los problemas regulatorios y las relaciones públicas, y mejorando los programas de seguridad cibernética en el futuro.

**Preparación**
- Estructura org. / CSIRT
- Capacitacion.
- Procedimientos, guías
- Inteligencia de amenazas
- Herramienta y equipamiento forence
- Roadmap

**Detección y Análisis**
- Logs, registros eventos
- Alertas, detección de intrusiones
- Correlación de eventos
- Triaje, priorización
- Escalamiento

**Contención, Erradicación y Recuperación**
- Estrategias de contención
- Adquisición y manejo de evidencia
- Erradicación de las amenazas
- Restauración de sistemas
- Cierre de brechas

**Acciones Post-Incidentes**
- Lecciones aprendidas
- Implementación de mejoras
- Generación de inteligencia
- Acciones legales y/o disciplinarias

europa press ciberseguridad

INTERNET DE LAS COSAS

Fira De Barcelona
La industria 5.0 abrirá las sesiones de IOT Solutions World Congress 2023

Economía Finanzas
Minsait, nombrado líder a nivel global en prestación de servicios IoT industriales a las

## Kingston IronKey presenta su primera unidad USB-C con cifrado de hardware

LONDRES INTERNACIONALES - 30 de octubre 2022 - 09:00hs

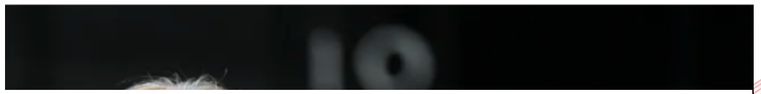
## Oposición británica pide investigar si se hackeó a Liz Truss

El Mail on Sunday dijo que la brecha se había descubierto en verano, cuando Liz Truss competía por el liderazgo del Partido Conservador

ITALIA TECNOLOGÍA - 10 de mayo 2022 - 11:27hs

## La cibercriminalidad costó más de 6 billones de dólares en 2021

La ciberseguridad se ha convertido en un tema clave para la Comisión Europea y para los miembros de la Unión Europea (UE).



PANAMÁ CONTENIDO PATROCINADO - 28 de abril 2022 - 15:49hs

## Las economías en la post-pandemia exigen seguridad de vanguardia

Visa ha invertido más de USD 9 mil millones en aumentar la ciberseguridad y reducir el fraude, en los últimos cinco años.

NIRIEN CBRT Cybersecurity Blue & Red Team

# Planificación de incidentes

Desarrollamos planes de respuesta a incidentes antes de los incidentes cibernéticos. Esto incluye ejercicios de simulación, y juegos de ataque y defensa.



TECNOLOGÍA - 17 de septiembre 2022 - 10:28hs

## Intrusión en Uber: hacker se habría hecho pasar por colega

Se desconoce cuántos datos robó el hacker o cuánto tiempo estuvo dentro de la red de Uber.

PANAMÁ CONTENIDO PATROCINADO - 28 de abril 2022 - 15:49hs

## Las economías en la post-pandemia exigen seguridad de vanguardia

Visa ha invertido más de USD 9 mil millones en aumentar la ciberseguridad y reducir el fraude, en los últimos cinco años.


EE. UU.

**Epic Games pagará 520 millones de dólares acusado de no proteger a menores**

**Preparación**

- Estructura org. / CSIRT
- Capacitacion.
- Procedimientos, guías
- Inteligencia de amenazas
- Herramienta y equipamiento forence
- Roadmap

**Detección y Análisis**

- Logs, registros eventos
- Alertas, detección de intrusiones
- Correlación de eventos
- Triaje, priorización
- Escalamiento

**Contención, Erradicación y Recuperación**

- Estrategias de contención
- Adquisición y manejo de evidencia
- Erradicación de las amenazas
- Restauración de sistemas
- Cierre de brechas

**Acciones Post-Incidentes**

- Lecciones aprendidas
- Implementación de mejoras
- Generación de inteligencia
- Acciones legales y/o disciplinarias

NIRIEN CBRT
Cybersecurity Blue & Red Team

## Analistas Nivel 1 y 2

Los analistas de nivel 1 son la primera línea de defensa y detección de CBRT. Este equipo está compuesto por analistas capacitados y certificados con una amplia experiencia en IT y seguridad. El equipo está a cargo de la primera alerta de intercepción, documentación, priorización e investigación inicial de acuerdo con una guía detallada.

## Analistas Nivel 3 y 4

Estos analistas son expertos en el campo que realizan análisis forenses y tienen una vasta experiencia en descubrimientos e investigaciones que involucran múltiples entidades. Los analistas de nivel 4 cuentan con profundo conocimiento de técnicas forenses y de cacería de amenazas, los protocolos de red, el malware y las técnicas de propagación de los atacantes y los escenarios de ataque.

NIRIEN CBRT
Cybersecurity Blue & Red Team

## Educación y cultura Ejecutiva

Apoyamos a las organizaciones con la educación de la junta directiva y los ejecutivos para ayudarlas a comprender las amenazas de seguridad cibernética que pueden enfrentar y desarrollar un marco de gobierno organizacional efectivo para mitigar estas amenazas potenciales.

## Programas de concienciación

A través de la identificación de brechas en la capacitación de los empleados, CBRT ayuda a obtener una mejor comprensión del conocimiento de seguridad de los colaboradores y a descubrir dónde se necesita más capacitación o recursos para reforzar la seguridad general de su organización.

NIRIEN CBRT
Cybersecurity Blue & Red Team

# Gestión de riesgos marcos de ciberseguridad de la industria

Desarrollado por cientos de expertos del gobierno, empresas tecnológicas y propietarios y operadores de infraestructura crítica, el marco de seguridad cibernética publicado por los Institutos Nacionales de Estándares y Tecnología (NIST) es ampliamente reconocido como un estándar líder para evaluar y administrar el riesgo organizacional.

# Manejo de crisis ante emergencias cibernéticas

La preparación eficaz ante crisis va más allá de la respuesta a incidentes cibernéticos para abordar todo el ciclo de vida de preparación, respuesta y recuperación de la gestión de crisis. La preparación implica no solo el monitoreo las 24 horas del día, los 7 días de la semana, sino también la preparación de los miembros de toda la organización para enfrentar un incidente o una crisis.

NIRIEN CBRT
Cybersecurity Blue & Red Team

# Auditorias y pruebas de penetración

## Prueba de penetración holística de 360°

Las pruebas de penetración son un ejercicio de seguridad en el que un experto en seguridad cibernética intenta encontrar y explotar vulnerabilidades en un sistema informático. El propósito de este ataque simulado es identificar cualquier punto débil en las defensas de un sistema que los atacantes reales podrían aprovechar.

### Caja negra

El equipo no sabe nada sobre la estructura interna del sistema de destino. Actúa como lo harían los ciber atacantes, buscando cualquier debilidad explotable.

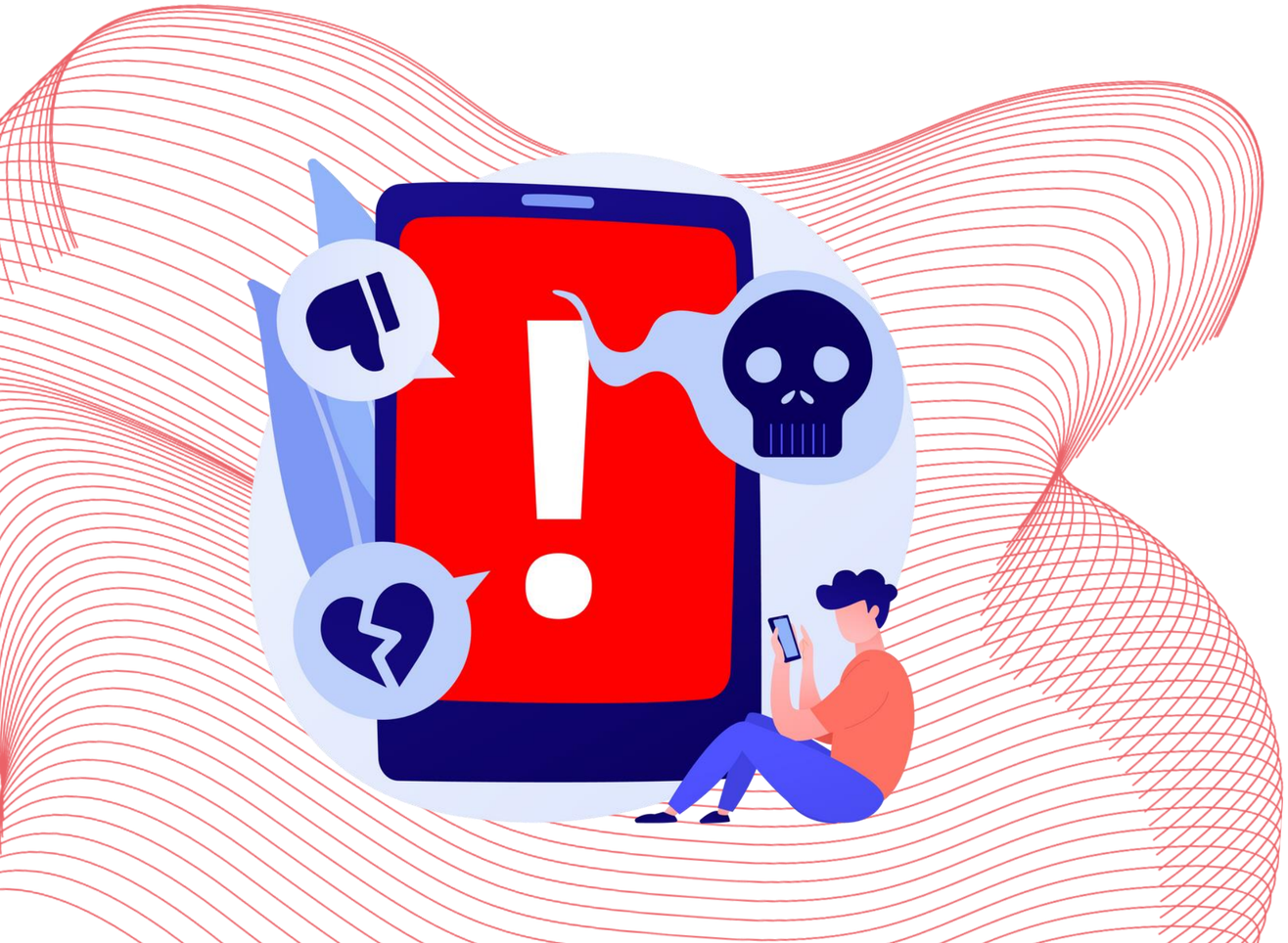
### Caja gris

El equipo tiene cierto conocimiento de uno o más conjuntos de credenciales. También conoce las estructuras de datos internas, el código y los algoritmos del objetivo.

### Caja blanca

Los evaluadores de penetración tienen acceso a los sistemas y artefactos del sistema, incluidos el código fuente, los archivos binarios, los contenedores y, a veces, incluso los servidores que ejecutan el sistema.

NIRIEN CBRT
Cybersecurity Blue & Red Team



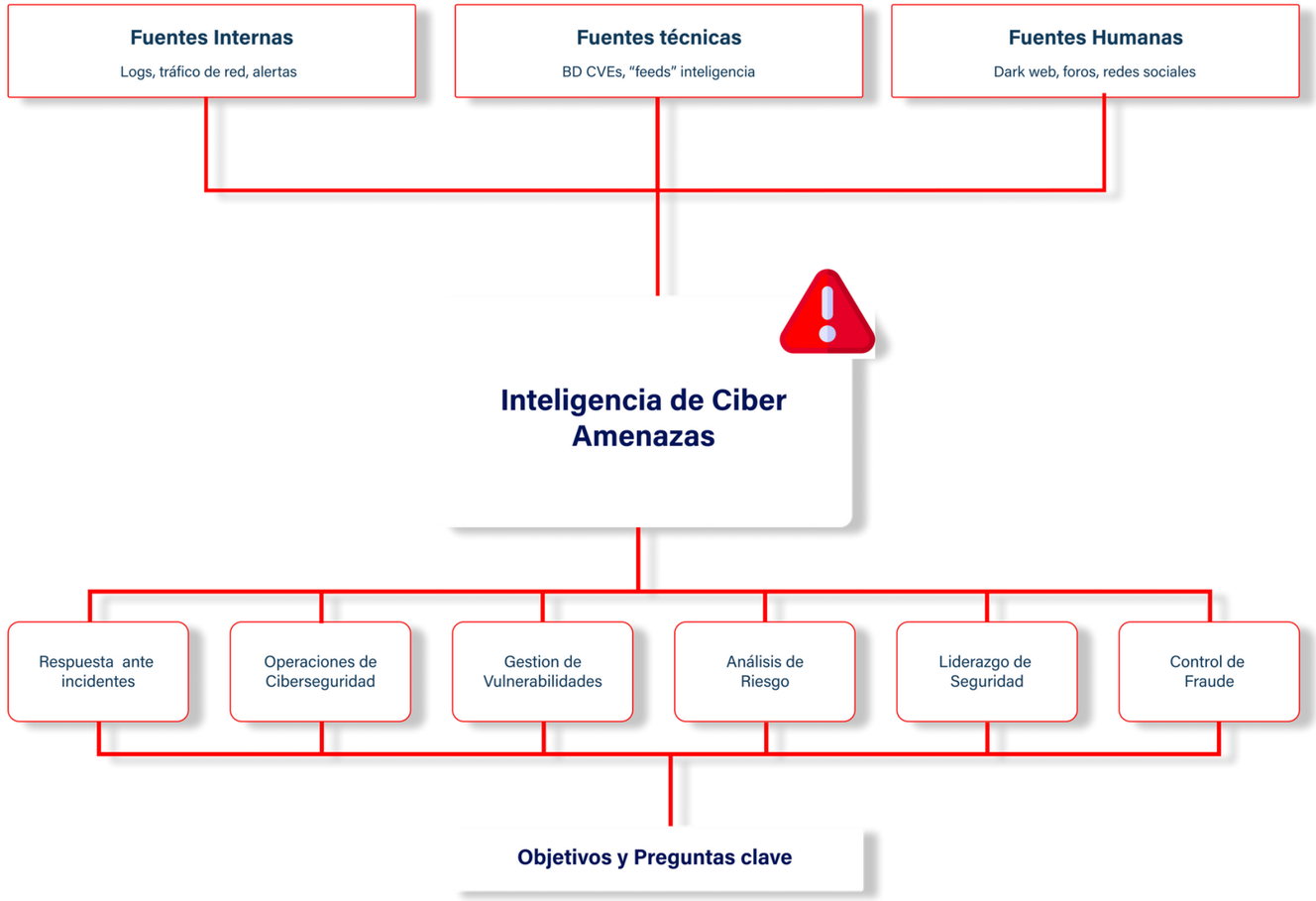
## Inteligencias de amenazas

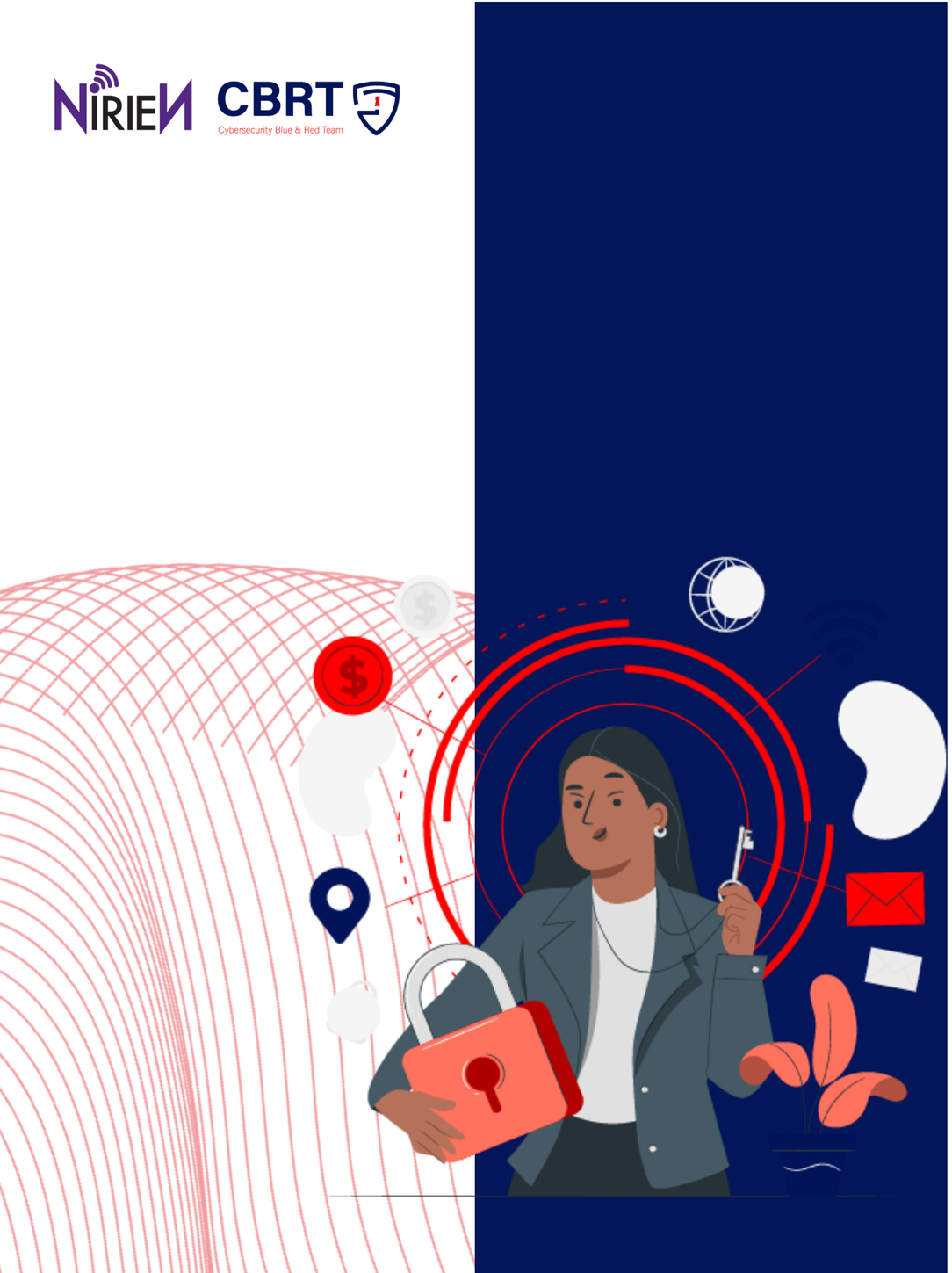
El equipo de Inteligencia de Amenazas Cibernéticas es responsable de la recopilación y el enriquecimiento de información de las operaciones y los recursos en línea de fuentes internas y externas para producir inteligencia accionable para compartir con los clientes de CBRT.

## Emulación de adversario

La emulación adversaria es una práctica que tiene como objetivo probar la resiliencia de una red contra atacantes avanzados o amenazas persistentes avanzadas. Es una forma en que se lleva a cabo la ejecución de las mismas tácticas, técnicas y procedimientos que los atacantes utilizarían en el contexto de la organización.

El equipo de inteligencia de amenazas procesa la información almacenada, incorpora exhaustivos IOC y amenazas, y agrega y correlaciona los datos recopilados. Esto proporciona a nuestros expertos los conocimientos necesarios para identificar las intrusiones y proporcionar los parches adecuados a medida que evolucionan las vulnerabilidades.





## Deception – Honeypots/disuasores

A forma de proteger los sistemas y la infraestructura TI, CBRT cuenta con sensores y sistemas señuelos, los cuales simularán parte de la infraestructura de la organización, dispositivos de redes y usuarios, con el objetivo de obtener alerta temprana sobre posibles intrusiones e inteligencia de amenaza de los riesgos cibernéticos que enfrenta la organización.

## Monitorio en tiempo real 24x7x365

Anule las enormes inversiones de capital y los requisitos de personal de construir y mantener un centro de operaciones de seguridad (SOC) interno con nuestras soluciones SOC como Servicio y Ciberseguridad como Servicio. Nuestros centros con base en República Dominicana, Israel y Estados Unidos cuentan con personal las 24 horas del día, los 7 días de la semana, los 365 días del año para brindar detección y protección día y noche.

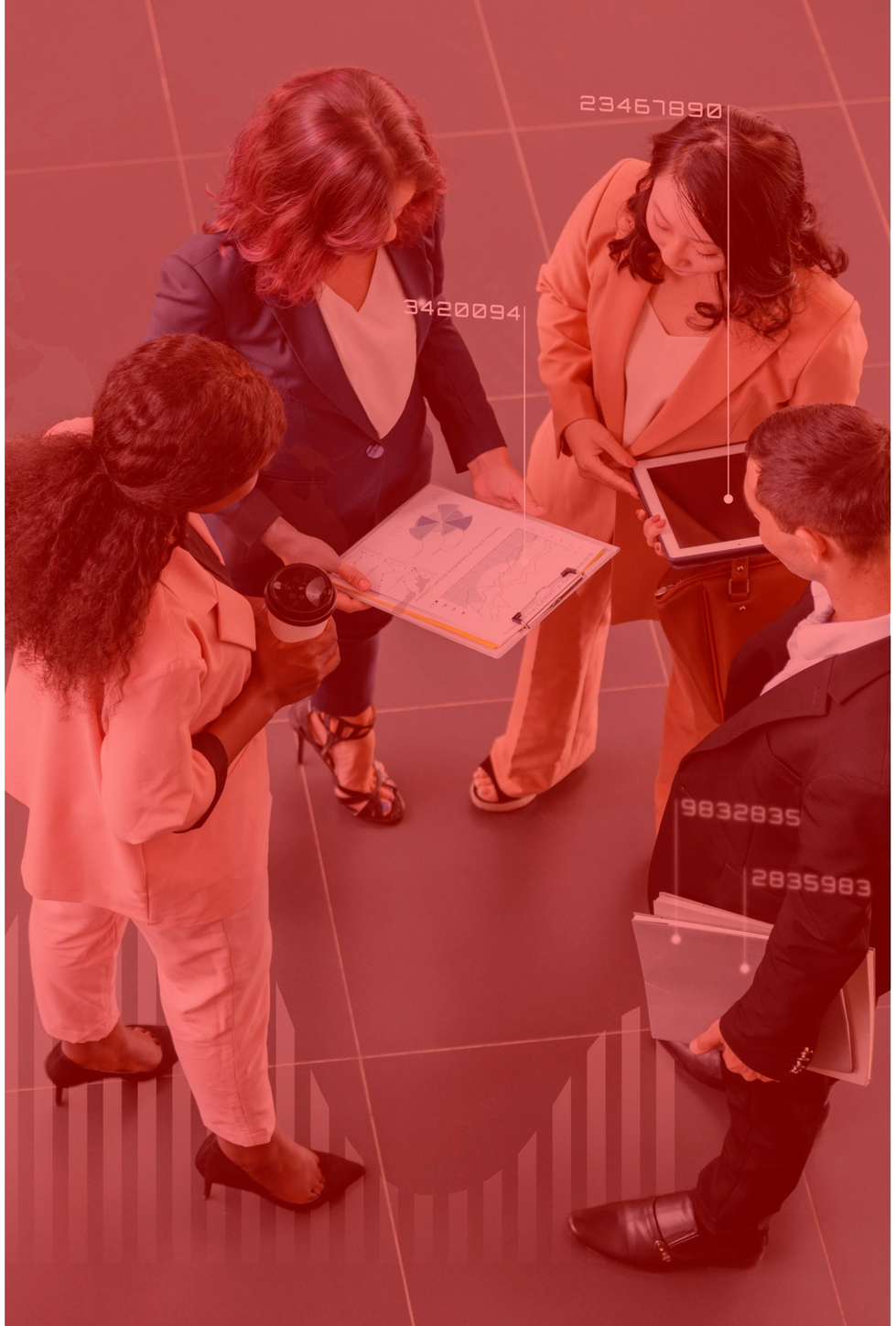
NIRIEN

CBRT

Cybersecurity Blue & Red Team

# Protección 360

**El CyberSOC de CBRT ofrece el servicio de XDR (Detección y Respuesta Extendida), UEBA (Análisis de Comportamiento de Usuarios y Entidades) y WAF (Aplicación de Cortafuegos Web) gestionados en tiempo real para la detección y defensa de situaciones de ataques externos y/o internos respecto a la seguridad de la Institución, permitiendo detección de intrusos y comportamientos anómalos**



# ¡Gracias!

NIRIEN CBRT
Cybersecurity Blue & Red Team

## Contáctanos


**Correo**

Mrepetto@nirien.com

**Móvil**

+507 6674-8586


Tus dudas son importantes para nosotros, si deseas más información, te invitamos a utilizar los medios de contacto sugeridos para apoyarte con tu solución.