

# 2

## CAPACIDAD DE RESPUESTA ANTE INCIDENTES



### CONTENIDO

- *Equipo de respuesta ante incidentes (ERI)*
- *Factores involucrados*
- *Unidad de ciberinteligencia*

# ¿QUÉ NECESITAMOS PARA DAR RESPUESTA A LOS INCIDENTES?

Lo primero todo, debemos de darnos cuenta que los incidentes de seguridad debe recibir una respuesta rápida y eficiente para poder minimizar el impacto.

Es por ello que necesitamos de un conjunto de recursos para resolver este tipo de problemas.

## HUMANOS - MATERIALES - ESTRATÉGICOS

A este conjunto de recursos es a lo que llamamos **IRC (Incident Response Capability)** que es la base para establecer una **estrategia**.

# GRUPO DE TRABAJO ESPECÍFICO

El grupo de trabajo no tiene un nombre en concreto pero en general suelen nombrarse como ERI o IRT en inglés (Equipo de Respuesta ante incidentes - Incident Response Team). En el sector de la seguridad informática también tenemos diferentes grupos: CIRT (Computer Incident Response Team) CIRC (Computer Incident Response Capability) SERT (Security Emergency Response Team) CERT (Computer Emergency Response Team)

**Según el ENS, la seguridad informática se concibe como una actividad integral en la que no caben actuaciones puntuales.**

# CAPACIDAD DE RESPUESTA

Las organizaciones deben de dar una capacidad de respuesta antes posibles incidentes de forma que puedan cumplir con unos requisitos mínimos:

- Se minimice la probabilidad de ocurrencia de incidentes y en caso de que puedan ocurrir que se minimice su impacto.
- La gestión de los incidentes debe seguir una metodología aprobada y apoyada por la dirección de la organización.
- Se mejore la seguridad a través de incidentes ya ocurridos.

# 1. EQUIPO DE RESPUESTA ANTE INCIDENTES

El **equipo de respuesta** de una organización es el conjunto de analistas especializados que, junto con los recursos proporcionados deben de dar respuesta a cualquier amenaza. Deben estar disponibles en cualquier momento para analizar y actuar antes cualquier posible amenaza para limitar los daños.



# TIPOS DE EQUIPOS

Los equipos de respuesta pueden estar configurados de dos modos:

## CENTRALIZADOS

Empresas pequeñas (PYMES)  
Empresas grandes (pero centralizadas)

Un único equipo encargado de  
toda la gestión de incidentes

## DISTRIBUIDOS

Empresas de gran tamaño

Diferentes equipos diferenciados  
por áreas

CIBERSEGURIDAD INDUSTRIAL  
INCIDENTES EN PUESTOS DE  
TRABAJO  
DISTRIBUCIÓN GEOGRÁFICA

¿CUÁL ES LA MEJOR OPCIÓN?



# PUES OS ADELANTO QUE NUNCA HAY UNA OPCIÓN ÚNICA

En una organización los equipos pueden estar compuestos por una empresa contratada que nos ofrece esos servicios, sabiendo que van a estar más relacionados con los principales incidentes, ya que trabajan para otros clientes a la vez.

De igual manera, si la empresa es externa no contará con el conocimiento de la infraestructura de la organización Y **posiblemente no podrá resolver algunos problemas de manera tan eficiente.**

Una **solución intermedia** sería utilizar un equipo que tenga delegados ciertos aspectos con proveedores externos y se puedan centrar en los aspectos importantes de la seguridad.

# FACTORES PARA UN MODELO

Los factores que nos harán seleccionar un modelo u otro son:

TAMAÑO, ESTRUCTURA Y DISPERSIÓN  
GEOGRÁFICA DE LA EMPRESA

DISPONIBILIDAD DE  
LOS EMPLEADOS

NECESIDAD DE RESPUESTA (24/7)

COSTE ECONÓMICO

CONOCIMIENTO DEL EQUIPO

# RESPONSABILIDADES DE UN ERI

Un ERI tiene como función principal la gestión de incidentes, pero también suelen ser los responsables de:

- La operación de los sistemas de detección de intrusos (IDS)
- El despliegue y gestión de sistemas de vigilancia
- Gestión de sistemas antimalware / antrootkits
- Gestión de sistemas de prevención de perdida de datos (DLP)
- Sistema de constraintelencia (Honeypots)
- Realización de auditorías de vulnerabilidades
- Desarrollo de campañas de concienciación

*También es posible encontrar equipos de respuesta ante incidentes con un modelo de organización con entidad propia (**CERT**, **CSIRT**) o formando parte de centros de operación (**SOC**).*

# CSIRT, CERT SOC

Tanto el término CSIRT o CERT son términos similares, la única diferencia es que CERT es un término registrado por la Universidad *Carnegie Mellon de Pensilvania, Estados Unidos*.

## ***Un poco de historia ...***

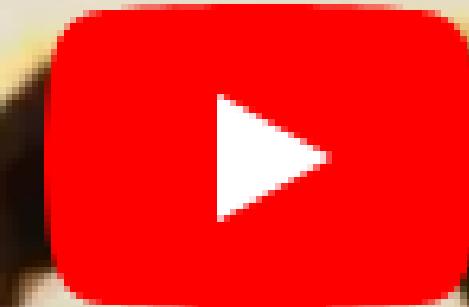
En el año 1988 se tuvo constancia de la creación del primer ejemplar de malware auto replicable, el gusano Morris, que afectó casi el 10 % de los sistemas conectados a ARPANET, el antecesor de Internet. Este incidente de seguridad manifesto la necesidad de coordinar el trabajo personal de un TI de manera agil y eficaz. A raiz de este caso la DARPA (Agencia de Proyectos de Investigacion Avanzados de Defensa, de las siglas en ingles Defense Advanced Research Projects Agency) patrocino la creaccion del primer Equipo de Respuesta ante Incidentes, el CERT.



Analizando a Gusano Morris | El Primer Malware Autorr...  
Analizando a Gusano Morris



# Morris



Watch on  YouTube

Después de todo esto, empezó a aparecer el término CSIRT para completar el concepto inicial de CERT, añadiendo al término el valor de los servicios preventivos y de gestión de seguridad.

Tal y como se describe en la Guía de Seguridad (CCN-STIC-810). “Guía de Creación de un CERT/CSIRT” del CCN, tradicionalmente la definición de un CERT engloba un equipo o capacidad de un organismo de ofrecer servicios y soporte a un colectivo determinado (ámbito de actuación) para prevenir, gestionar y responder a los accidentes de seguridad de la información que puedan surgir.

- Communication Liaison \*
- Incident Analyst \*
- Incident Responder
- Incident Triage Coordinator \*
- IT Administrator
- Malware / Forensic Analyst \*



### Information Security Incident Management

- Data Manager  
Incident Analyst \*  
Incident Triage Coordinator \*  
System and Sensor Administrator  
Use Case Manager



### Information Security Event Management

## SERVICE AREAS



### Vulnerability Management

- Incident Analyst \*
- IT Security Administrator
- Malware/Forensic Analyst \*
- Vulnerability Analyst
- Vulnerability Assessment Analyst
- Vulnerability Coordinator
- Vulnerability Disclosure Coordinator
- Vulnerability Researcher
- Vulnerability Triage Coordinator



### Knowledge Transfer



### Situational Awareness

- Awareness Coordinator
- Policy Advisor
- Risk & Continuity Advisor \*
- Staff Developer
- Technical Policy Advisor
- Training Developer
- Training Instructor

- Communication Liaison \*
- Risk Analyst / Risk & Continuity Advisor \*
- Situational Awareness Data Analyst
- Situational Awareness Manager
- Threat Warning Analyst

\* role defined for multiple service areas



SGG

**CCN-cert**  
centro criptológico nacional

 **incibe**

INSTITUTO NACIONAL DE  
CIBERSEGURIDAD

**FIRST**  
*Improving Security Together*



# ¿QUÉ DIFERENCIA HAY CON UN SOC?

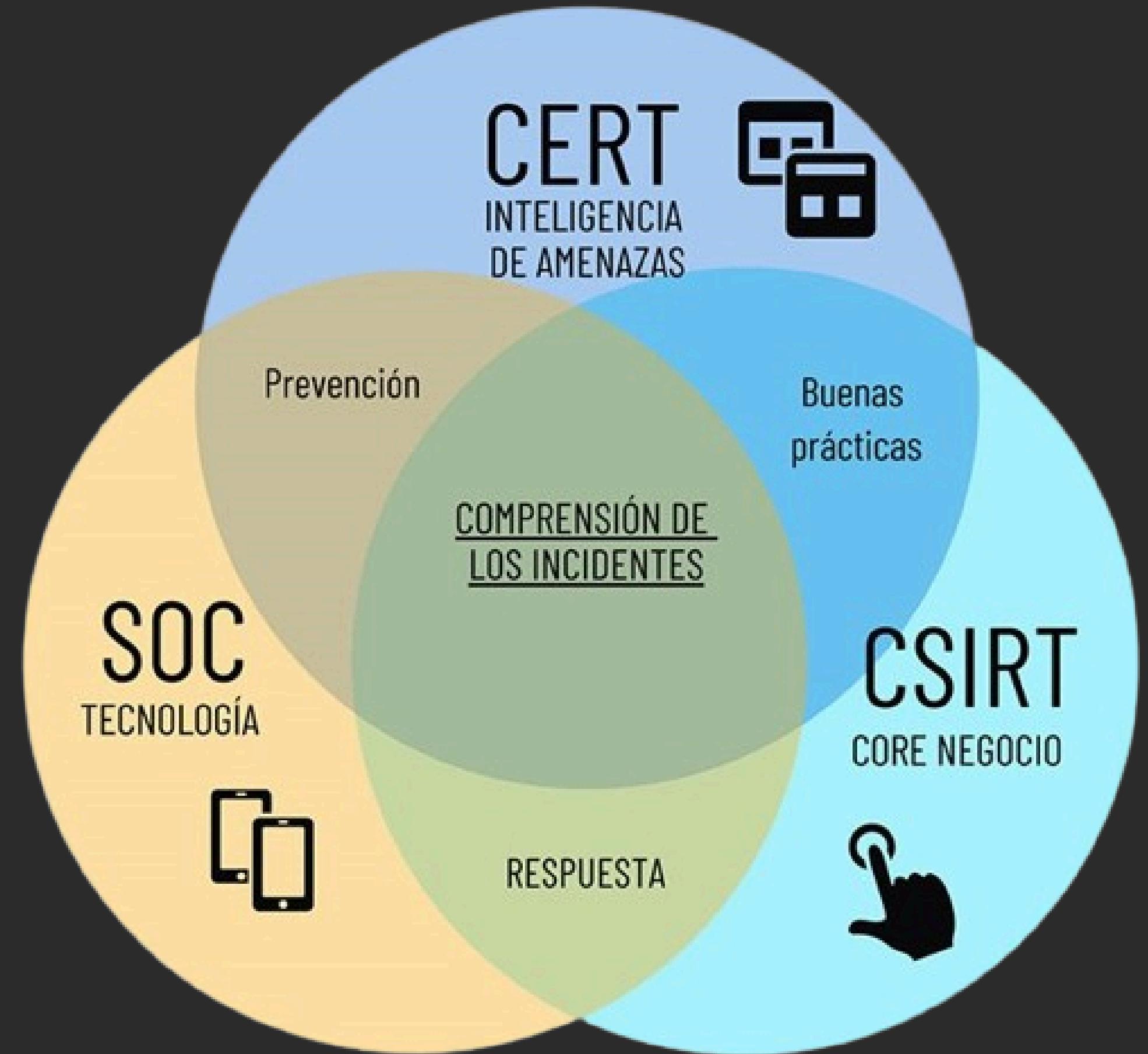
Un SOC es más amplio en su alcance y puede incluir la función de respuesta al incidente, tanto parcial como total, así como otras tareas como podrían ser:

Supervisar y operar monitorización el despliegue de los sistemas de monitorización de eventos de seguridad y recolección de información.

Administrar tareas como la gestión de identidades

Administrar dispositivos perimetrales de seguridad como firewalls (reglas de filtrado, gestión de cambios,...)

Realizar análisis forenses



# EQUIPO HUMANO

Para la resolución de un incidente podemos separar al equipo en dos ambientes distintos, por un lado la parte del equipo operativa que responde al incidente y por otro lado la organizativa y estratégica de como afrontar ese incidente.

Aunque el número de miembros del equipo dependerá de la forma en la que queramos actuar ante un incidente y otros factores como los visto anteriormente.

# EQUIPO HUMANO

Aun así hay que contar con figuras como:

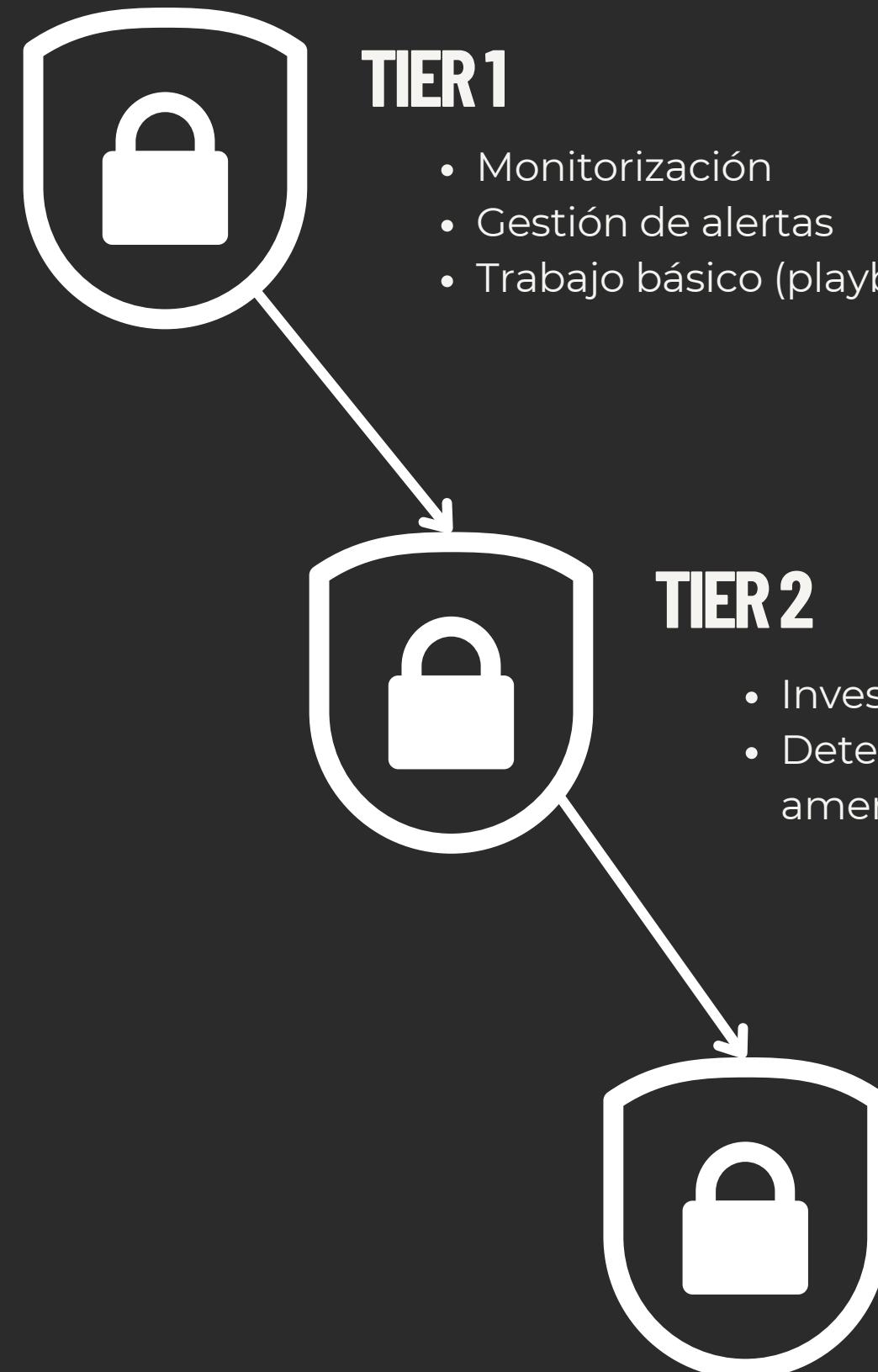
- **Responsable global.** Persona con formación y amplia experiencia en la ciberseguridad y gestión de incidentes.
- **Especialistas.** Son aquellos que tienen un perfil mucho más técnico, los que básicamente realizan las propias tareas de seguridad. Estas personas se dedican de forma completa a la gestión de la seguridad informática o la fortificación y defensa de sistemas.
- **Experto en leyes y normativas.** Aquella persona que apoye la gestión de incidentes y de soporte de forma legal al equipo.

# MODELO TIERS

## ALERTAS



Las alertas pueden provenir de la propia plataforma de seguridad que use la organización, ayudas o solicitudes de los propios usuarios o empleados y de otros departamentos IT.



# ESTAR EN CONTINUO APRENDIZAJE Y FORMACIÓN

## 2. OTROS FACTORES INVOLUCRADOS

EQUIPO DIRECTIVO DE LA ORGANIZACIÓN

DEPARTAMENTO DE SEGURIDAD

DEPARTAMENTO/S TI

DEPARTAMENTO LEGAL

RELACIONES PÚBLICAS Y CON LOS MEDIOS DE COMUNICACIÓN

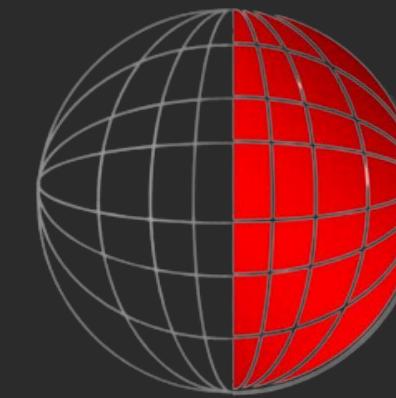
RECURSOS HUMANOS

EQUIPO DE PLAN DE NEGOCIO

# ¿QUE SON LOS BLUE TEAM Y RED TEAM?

# ACTORES EXTERNOS

El Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) es el Órgano del Ministerio del Interior encargado del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad en relación con la Protección de Infraestructuras Críticas en el territorio nacional.



## CNPIC

CENTRO NACIONAL DE PROTECCIÓN  
DE INFRAESTRUCTURAS CRÍTICAS



## PROVEEDORES Y FABRICANTES

PROVEEDORES DE  
DISPOSITIVOS

SERVICIOS EXTERNOS

PROVEEDORES DE ISP



El CIBER-ATAQUE más grande de la historia... ¿Empezó ...



Watch on  YouTube

### 3. UNIDAD DE CIBERINTELIGENCIA

La **OTAN** define el término inteligencia como el producto resultante del procesamiento de información relativa a naciones extranjeras, fuerzas o elementos potencialmente hostiles o áreas de operaciones reales o potenciales, y también aplica el término a la actividad cuyo resultado es justamente este producto, esta inteligencia. Simplificando, podríamos hablar de inteligencia como el producto resultante de un análisis de información cuyo objeto es facilitar la toma de decisiones.



# INTELLIGENCE GATHERING

- HUMINT
- GEOINT
- MASINT
- OSINT
- SIGNIT
- TECHINT

# TIPOS DE INTELIGENCIAS

Aquí podemos encontrarnos diferentes tipos:

- **Inteligencia estratégica.** Realizar recolección de información que nos permita detectar una amenaza. Como puede ser la creación de perfiles de riesgo.
- **Inteligencia táctica.** Se refiere a aquellas acciones concretas para planificar y diseñar medidas de prevención y de actuación antes riesgos cibernéticos.
- **Inteligencia operativa.** Aunque pueda ser parecida a la estratégica, esta se encarga a mayor escala de las incidencias y en el entorno inmediato de una organización.

# SERVICIOS DE UNA UNIDAD DE CIBERINTELIGENCIA

- **Difusión o divulgación.** Se encargan de realizar informes o alertas de incidentes relacionados con la ciberseguridad. Así como de informes periodicos.
- **Modelado de ciberamenazas.** El objetivo es obtener las diferentes TTP de los atacantes para definir una estrategia de defensa.
- **Vigilancia digital.** Consiste en identificar posibles amenazas que afecten de forma corporativa o particular, como son:
  - Prevencion de fraudes y estafas (phising)
  - Control de registro de dominios no legítimos
  - Leaks de información
  - Monitorización de aplicaciones falsas
  - Seguimiento de grupos de hackers
- **Huella digital.** Control de la información no autorizada que tiene Internet de la organización o de sus empleados.

HAGA CLICK PARA  
MATARLOS A TODOS

