Preparación y respuesta ante ciberataques

iagua (26/05/2020)

CIC Consulting Informático

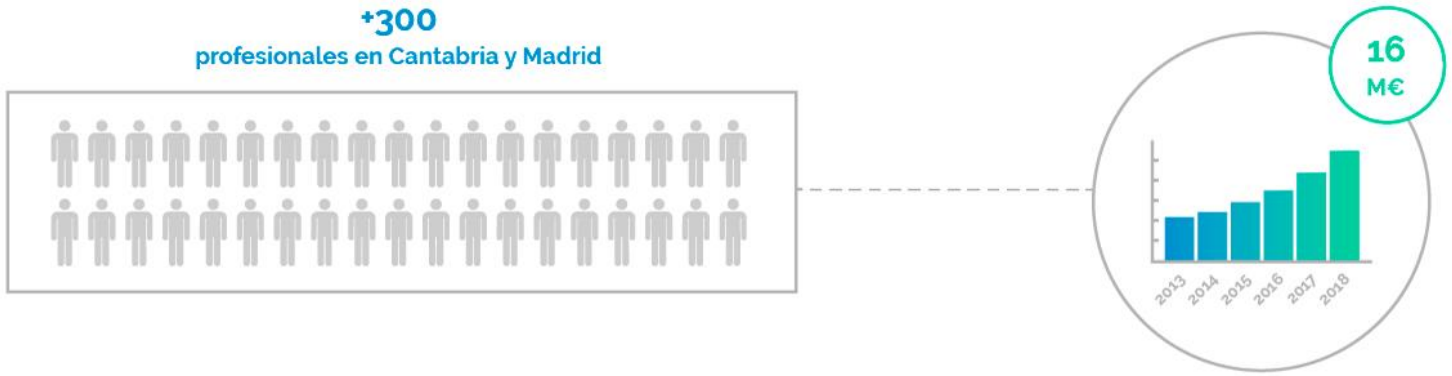
01.

Sobre nosotros

Quiénes somos

Somos **CIC Consulting Informático**, una compañía especializada en el desarrollo de soluciones software e integración, ofrecemos servicios de consultoría de procesos de negocio, operación y mantenimiento de red, seguridad de la información e informática.

Nos dedicamos a realizar **soluciones software** que maximizan la **eficiencia** de los procesos de gestión de las empresas, aumentando su **competitividad**.



Calidad

Nuestro afán es brindar la **máxima calidad de los productos y servicios** a nuestros clientes, el respeto por el **medio ambiente** y la **seguridad de la información**, nos apoyamos en un sistema de gestión integrado iniciado en 2004, según las normas ISO9001:2015, ISO14001:2015 e ISO27001:2014 certificados todas ellas por AENOR.

Además, CIC ha sido acreditada por el Software Engineering Institute (SEI) de la Carnegie Mellon University en el proceso de acreditación formal frente al **Nivel 2 de madurez del modelo de CMMI**.

CMMI DEV/2 SM
Exp. 2021-06-14 / Appraisal #32755

CERTIFIED IQNet MANAGEMENT SYSTEM

AENOR Empresa Registrada UNE-EN ISO 9001 ER-1736/2004

AENOR Gestión Ambiental UNE-EN ISO 14001 GA-2009/0008

AENOR Seguridad Información UNE-ISO/IEC 27001 SI-0095/2009

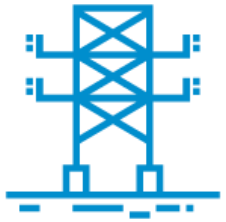
Achilles Repro Registrado 301587 Válido hasta: Octubre 2020

CIC Consulting Informático

Sectores

Las principales industrias donde prestamos servicios pertenecen al sector utilities (energía, agua, gas y petróleo), a la logística, a la industria de automoción, la manufactura y la gestión de infraestructuras críticas.

El conocimiento de la **dinámica de los negocios** en estos sectores permite a CIC proporcionar **soluciones realmente eficientes** y que se traducen en beneficios tangibles a corto plazo para su empresa.



ENERGÍA Y UTILITIES

INDUSTRIA Y SERVICIOS

SECTOR PÚBLICO

TRANSPORTE Y LOGÍSTICA

TELE-COMUNICACIÓN

01.2.

Nuestros productos

Productos

Nos dedicamos a realizar soluciones software que maximizan la eficiencia de los procesos de gestión de las empresas, aumentando su competitividad.

Algunas de nuestras soluciones con más proyección las hemos convertido en productos propios.

IDbox RT

FIELDEAS easy field services

SGRwin

LUCA BDS

FOR 3

CIC Consulting Informático

01.3.
Referencias

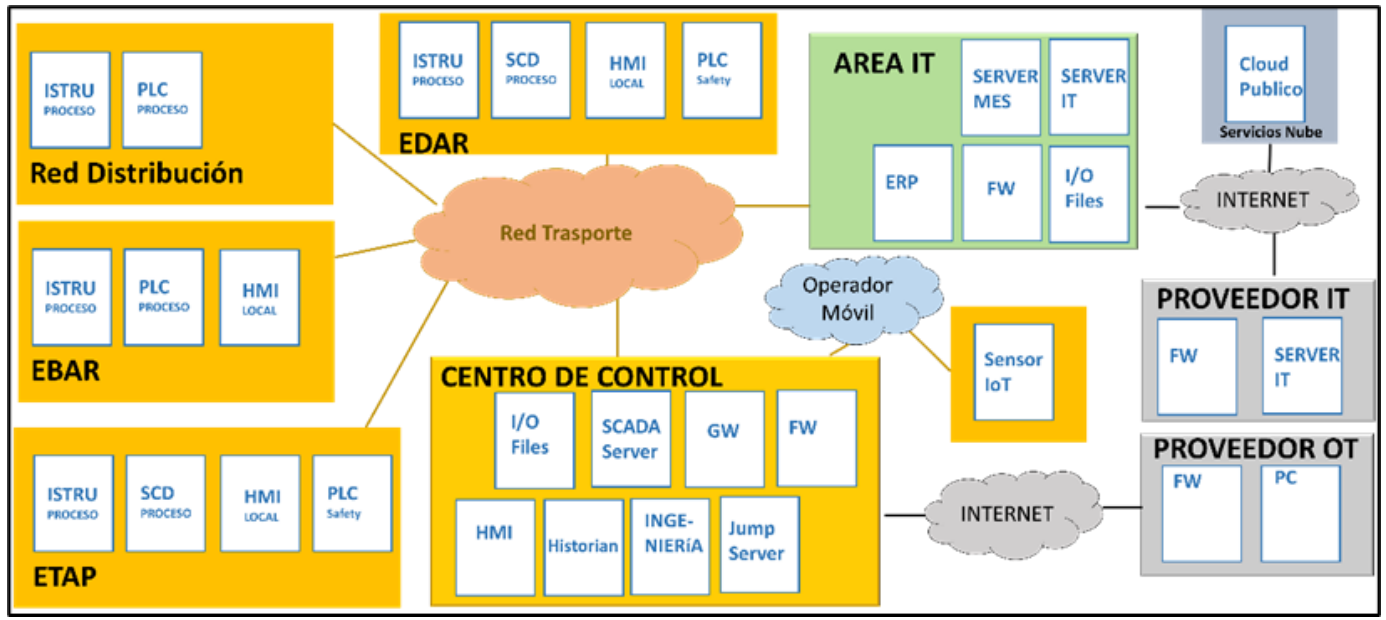
Nuestros partners


Algunos clientes

02.

Aguas de Arrakis

Representación alto nivel de compañía de aguas



1. **Área OT** compuesta por:
   a. Estación Depuradora de Aguas Residuales (EDAR)
   b. Estación Tratamiento de Agua Potable (ETAP).
   c. Estación de Bombeo de Aguas Residuales (EBAR)
   d. Red de Distribución de agua formada por depósitos, canalizaciones, …etc
   e. Centro de Control desde el que se supervisa y telemanda los diferentes procesos industriales.
   f. Red de trasporte que comunica las diferentes ubicaciones y componentes.
   g. Red de sensores IoT

2. **Área IT**
   a. Compuesta por los sistemas y componentes “clásicos” de sistemas de información y comunicaciones.
   b. Servicios cloud públicos.

3. **Proveedores**
   a. Proveedores de servicios de mantenimiento y soporte tanto de la red IT como OT.

04.

Riesgo alto de ciberataque en las empresas

Riesgo alto e impacto alto

[Global Risks Report 2020 - Reports - World Economic Forum]

¿Cuál es el impacto de una parada?

- Pérdida de ingresos
- Daño reputacional
- Incumplimientos contractuales:
  - Pérdida de clientes
  - Penalizaciones económicas
- Incumplimientos regulatorios por pérdidas de información (RGPD) o incumplimiento de plazos
- Pérdida de análisis por ausencia de información
- Pérdida de oportunidades comerciales.
- Estrés laboral
- Riesgo de quiebra


Buscar

elEconomista.es

Mercados y Cotizaciones | Ibex 35 | M.Continuo | Coronavirus | Empresas | Economía | Vivienda | Status | Opinión | Más leídas

Aragón

El 70% de las empresas que sufre una pérdida de datos cierra en menos de un año

¿Le puede pasar a mi empresa?

La mejor postura de diseño que podemos adoptar ante esta respuesta es:

Sí, me va a pasar

por lo que me tengo que preparar para

- Saber ¿cúando me va a a pasar?
- ¿cómo me puede pasar? y ¿cómo tengo que actuar para resistir el ataque?
- ¿Cuánto me va a costar sobreponerme?

05.

Ciber Resiliencia

¿Qué es la ciber-resiliencia?

La **ciber-resiliencia**, es la capacidad para resistir, proteger y defender el uso del ciberespacio de los atacantes. (Incibe)

Fuente: "Ciber-Resiliencia: Aproximación a un marco de medición" (Inteco-Incibe, 2014)

06.

NIST Cyber Security Framework

Marco de ciberseguridad de NIST v1.1

Existen múltiples marcos normativos orientados a la protección de nuestras organizaciones, siendo uno de los más recientes y mejor adaptados a la protección de infraestructuras críticas el NIST Cyber Security Framework v.1.1 publicado en abril de 2018

- **Identificar**: Gestionar los riesgos de ciberseguridad que puedan afectar a sistemas, datos y otros activos críticos para las organizaciones.
- **Proteger**: Implementar contramedidas para proteger nuestros activos críticos
- **Detectar**: Ejecutar actividades de identificación de amenazas y potenciales incidentes.
- **Responder**: Realizar acciones de respuesta ante un incidente de seguridad.
- **Recuperar**: Desarrollar la capacidad de resiliencia para volver al estado anterior al incidente con los menores daños posibles.

Fuente: https://www.nist.gov/cyberframework/framework

Marco de ciberseguridad de NIST v1.1

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

5 Functions 23 Categories 108 Subcategories 6 Informative References

Marco de ciberseguridad de NIST v1.1

Identificador único de función	Función	Identificador único de categoría	Categoría
ID	Identificar	ID.AM	Gestión de activos
		ID.BE	Entorno empresarial
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	Proteger	PR.AC	Gestión de identidad y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología protectora
DE	Detectar	DE.AE	Anomalías y eventos
		DE.CM	Vigilancia continua de seguridad
		DE.DP	Procesos de detección
RS	Responder	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
RC	Recuperar	RC.RP	Planificación de recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Marco de ciberseguridad de NIST v1.1

- Disaster Recovery
- Recuperación de datos
- Informes post-incidente
- Seguros de ciberseguridad

- Auditorías técnicas
- BIA,
- BCP
- Plan Director de Ciberseguridad

- Forensic
- Peritaje judicial
- Gestión de crisis

- Despliegue de Contramedidas
- Hacking Etico, Pentesting, Red Team
- Formación y concienciación
- Seguridad de red
- Protección del puesto de trabajo
- Backup

- Monitorización
- SIEM
- IDS
- SOC

07.

Cyber Security Incident Response

Respuesta a Incidentes de ciberseguridad (CSIR)

Entre las diferentes disciplinas de la ciberseguridad la respuesta ante incidentes se ocupa de las funciones de

Dentro de esta disciplina encontramos standares y guías de buenas prácticas que nos ayudarán a gestionar nuestro CSIR, destacamos:

- ISO/IEC 27035-1:2016.Gestión de incidentes de seguridad de la información (https://www.iso.org/standard/60803.html)
- NIST Special Publication 800-61 Rev 2. Computer Security Incident Handling Guide (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)

Organiza tu capacidad de respuesta

El punto inicial es la planificación y organización de tu CSIR

Planea

- Plantea un plan simple, claro y preciso.
- Que determine de forma clara quién hace qué, cómo y cuándo
- Debe permitir reaccionar de forma rápida y precisa ante un ataque

Crea Equipo

- Crea roles detallados y responsabilidades claras
- Pon juntos a equipos técnicos (equipo de seguridad) y no tecnicos (legal, RRHH, Relaciones Públicas)
- Debe permitir reaccionar de forma rápida y precisa ante un ataque

Clasifica incidentes

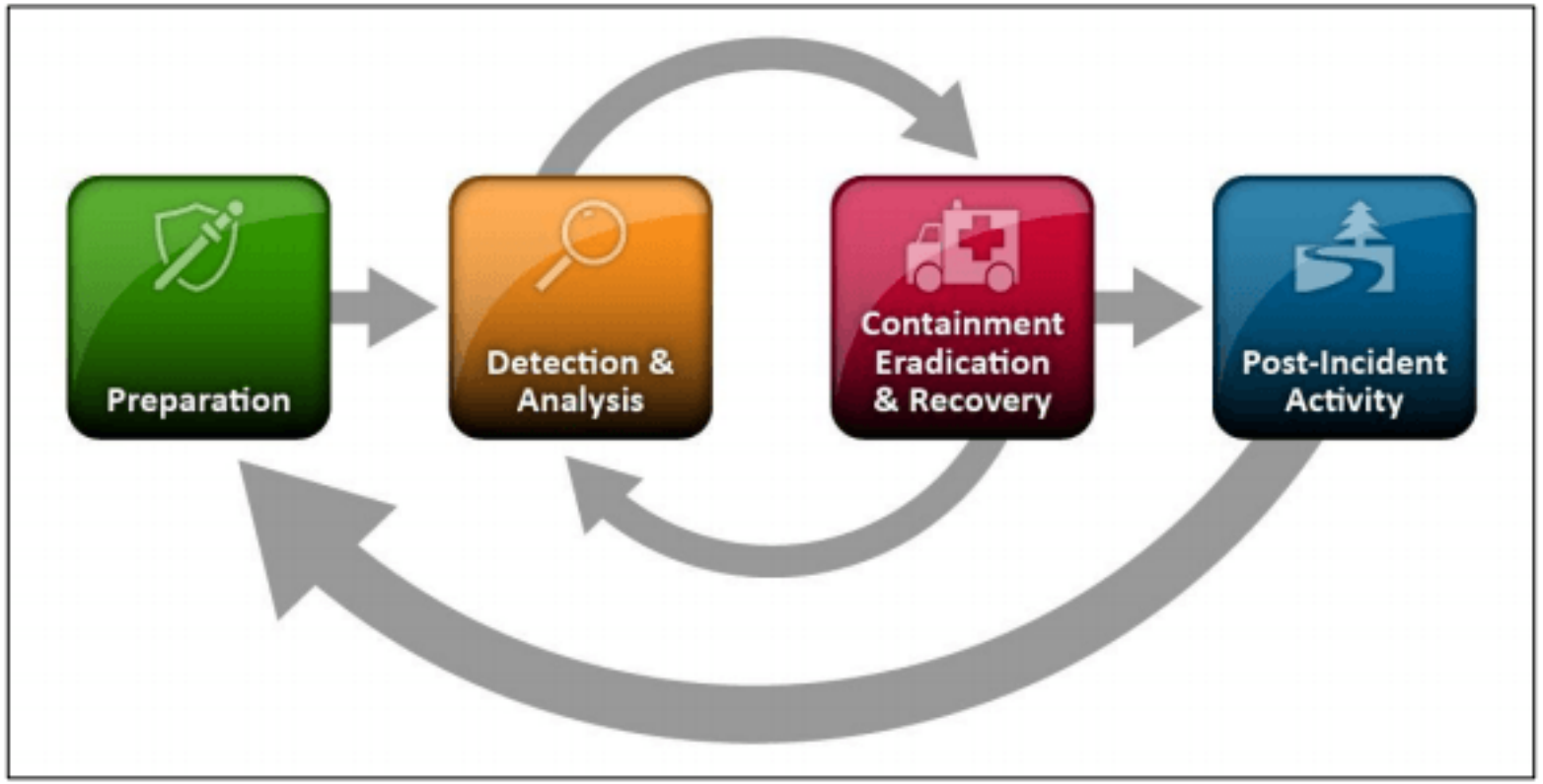
- Crea una clasificación de incidentes
- Establece criticidades, vectores de ataque, impactos, causas raiz.

Prioriza el negocio

- Se debe entender las prioridades del negocio
- Alinéa el plan con las necesidades del negocio.

Maneja el incidente

Debemos establecer unas buenas prácticas para la gestión del incidente como las establecidas en la



Fuente :NIST Special Publication 800-61 Rev 2. Computer Security Incident Handling Guidev(https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)

Maneja el incidente

- Desarrolla y documenta las políticas de respuesta ante incidentes
- Define las guías y mecanismos de comunicación.
- Incorpora fuentes de inteligencia de amenazas.
- Ejecuta ejercicios cyber-hunting y entrena al equipo.
- Evalúa tu capacidad de detección de amenazas (red team)

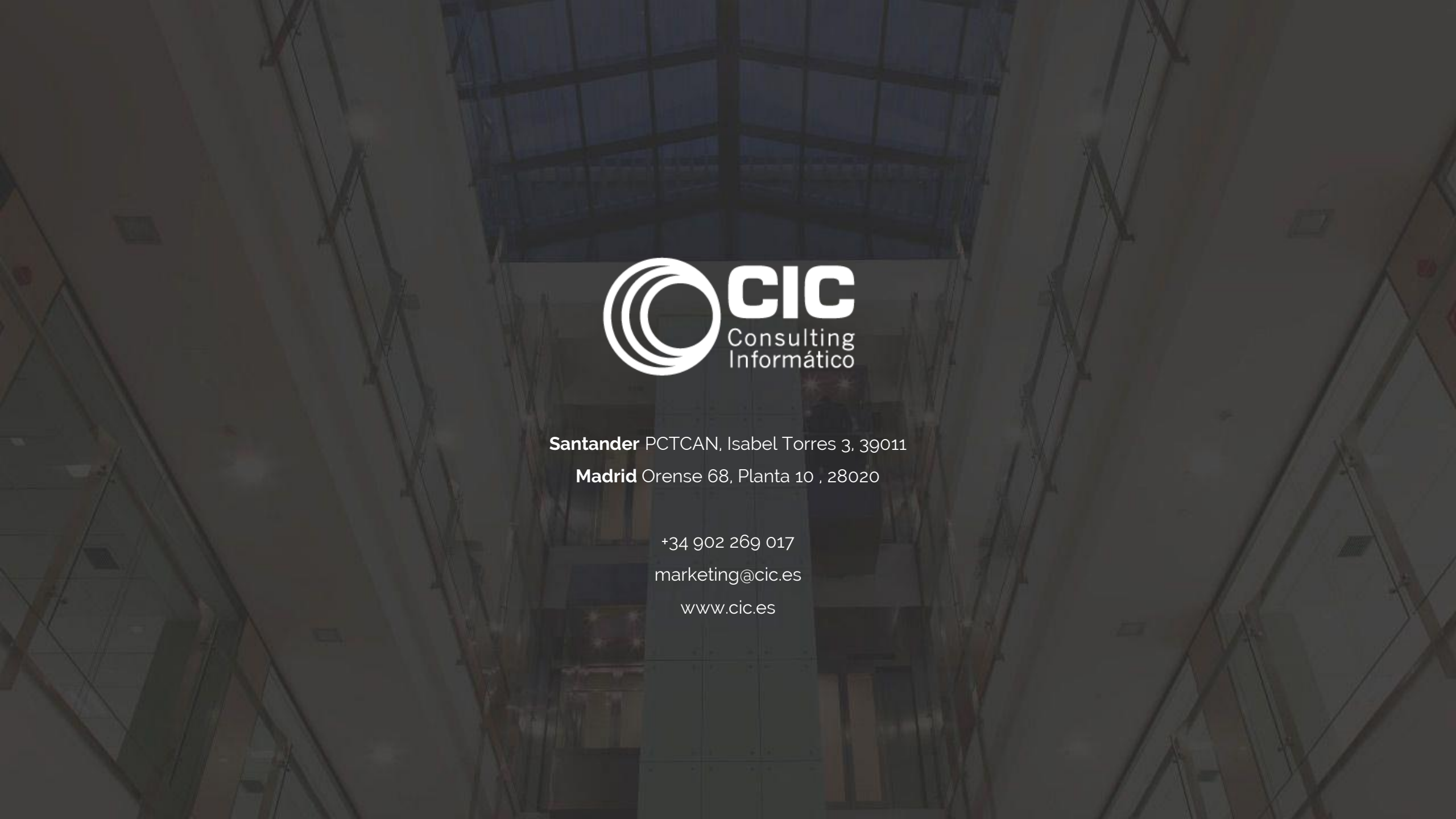
- Monitoriza los eventos de seguridad usando fw,IPS y DLP
- Detecta potenciales incidentes de seguridad mediante correlación de alertas con un SIEM
- Alerta: Los analistas abrirán tickets de incidente, documentarán indicios iniciales y asignarán una clasificación inicial al incidente.
- Creación de informes técnicos, a negocio y regulatorios.

Maneja el incidente

- Elije una estrategia de contención entre las disponibles.
- Recoje evidencias
- Identifica los host atacantes.
- Erradicación de la amenaza
- Recuperación

- Realiza un completo informe del incidente
- Monitorización posterior al incidente por si la amenaza reaparece.
- Actualiza fuentes de inteligencia de amenazas.
- Identifica medidas preventivas
- Realiza analisis de lecciones aprendidas.

Para cualquier pregunta contactar con rhidalgo@cic.es



Santander PCTCAN, Isabel Torres 3, 39011

Madrid Orense 68, Planta 10 , 28020

+34 902 269 017

marketing@cic.es

www.cic.es