FEVAL Institución Ferial de Extremadura

Role Play Ciberincidentes

30 Junio 2026
Badajoz

Agenda

HORARIO	ACTIVIDAD
09:30 – 10:00	Recepción de Asistentes y Acreditaciones
10:00 – 10:20	Introducción a la Dinámica
10:20 – 11:00	Caso 1: Ataque de Ransomware
11:00 – 11:45	Evolución de la Crisis
11:45 – 12:00	Resolución del Caso Ransomware
12:00 – 12:45	Caso 2: Fraude del CEO (BEC)
12:45 – 13:15	Resolución del Caso y Debate Abierto
13:15 – 13:45	Conclusiones y Networking

Caso1: Ataque Ransomware

CASO 1 : RANSOMWARE

LUNES TENÍA QUE SER...

Son las 08:20 de la mañana de un lunes. Varios empleados comunican al departamento de informática que no pueden acceder a los archivos compartidos y que sus equipos muestran un mensaje indicando que todos los datos han sido cifrados. Al mismo tiempo, algunos servicios corporativos dejan de funcionar y la página web de la empresa presenta errores en las áreas de servicios a clientes.

A las 8:50 se asume que hay un ataque de ransomware y se comunica la situación a la dirección de operaciones. Se ha visto afectado el acceso a los ficheros en red y locales y no se puede acceder al ERP. El correo y los servicios en cloud funcionan.

Es vuestro turno!!!! ¿Por dónde empezamos?

CASO 1 : RANSOMWARE

SIEMPRE SE PUEDE IR A PEOR...

A las 9:30 se recibe por correo electrónico en el buzón de dirección general, un mensaje de los supuestos atacantes en el que afirman haber cifrado la infraestructura y haber copiado información confidencial de la empresa, que en caso de no acceder al pago, harán pública. Exigen el pago de un rescate de 80.000 € en bitcoin en un plazo de 48 horas para facilitar la clave de descifrado y no publicar la información robada.

¿Pagamos y ya?

CASO 1 : RANSOMWARE

SIEMPRE SE PUEDE IR A PEOR (II)

Son las 10:30. El call center está saturado de llamadas de clientes quejándose de que no pueden cursar pedidos. Se confirma que se han exfiltrado datos de carácter personal, y la reputación del presunto grupo de atacantes indica que no dudarán en publicarlos.

¿No habíamos dicho de pagar y olvidarnos?

CASO 1 : RANSOMWARE

NO CONFIARSE, LA REALIDAD SIEMPRE SUPERA LA FICCIÓN...

A las 11 horas se recibe un correo de Incibe indicando que se han bloqueado los ataques de la organización criminal y que está disponible la herramienta de descifrado. Nos la facilitan y en 4 horas la situación vuelve a la normalidad.

Comentar sobre las decisiones adoptadas a lo largo del ejercicio, en materia de plan de continuidad, backup, comité de crisis, copias de seguridad, seguros, cumplimiento, etc..

RANSOMWARE

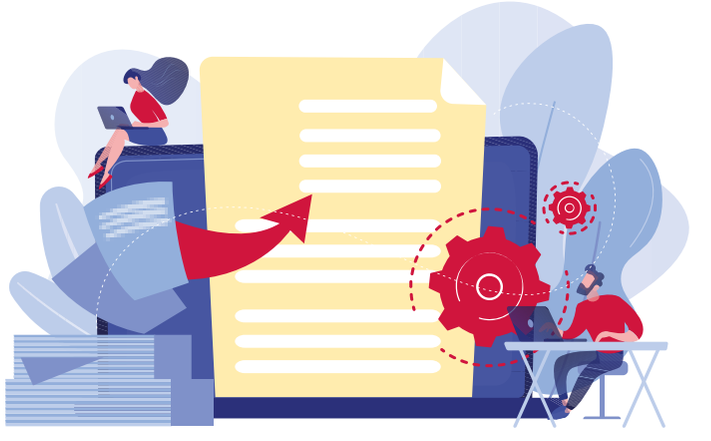
¿QUÉ ES UN ATAQUE DE RANSOMWARE?

Malware que cifra los sistemas de una organización y exige un rescate económico para recuperar el acceso.

España experimentó un incremento del **61%** en ataques de ransomware durante **2025**.

El coste consta del rescate más la parada operativa, el primero oscilando entre 10.000 € y varios millones. El segundo de miles de euros diarios.

Las sanciones, en doble extorsión, pueden llegar hasta 20 M€ o 4% de la facturación.



Empresa de 20 empleados
Facturación anual: 1 M€
Parada de actividad: 5 días
Recuperación TI: 15.000 €
Servicios externos: 8.000 €
Pérdida de ventas: 12.000 €
Coste total estimado: **35.000–50.000 €**

ROLE PLAY
CIBERINCIDENTES

Caso2: Bussiness Email Compromise

CASO 2 : BEC, Bussiness Email Compromise

MALDITAS FACTURAS...

- Hace dos semanas, administración recibió la llamada de un proveedor habitual reclamando el pago de una factura vencida hacía cuatro días.
- Administración comprobó que el pago se había realizado en fecha y en conversaciones con el cliente concluyen que se ha pagado en una cuenta distinta a la esperada por el cliente.
- Se comprobó que el pago se había realizado en la cuenta que figura en la factura, pero el proveedor insiste en que esa no es su cuenta y en que en su factura figuraba otra cuenta, la correcta.
- El importe son 7.480,00 € y se trata de un proveedor habitual, de confianza.
- Se cierra la comunicación con el proveedor mandándole copia de la transferencia y de la factura recibida, dónde coinciden los datos de pago e indicándole que esto ya está pagado y no vamos a pagar dos veces. No se toman acciones a mayores, pero se notifica a dirección.

CASO 2 : BEC, Bussiness Email Compromise

SI, LA COSA PUEDE IR A PEOR...

- A fecha de hoy, recibimos una demanda por impago del proveedor, en la que arguye que hemos sufrido una violación de nuestro correo electrónico que ha dado lugar a una manipulación de una factura y que por ese motivo a él no se la ha pagado.
- La demanda se apoya en un informe pericial que indica que el correo salió inmediatamente de su servidor por lo que no hubo tiempo de modificarlo en su extremo y afirma por tanto que es en el nuestro en el que se ha sufrido la vulneración.

BEC, Bussiness Email Compromise

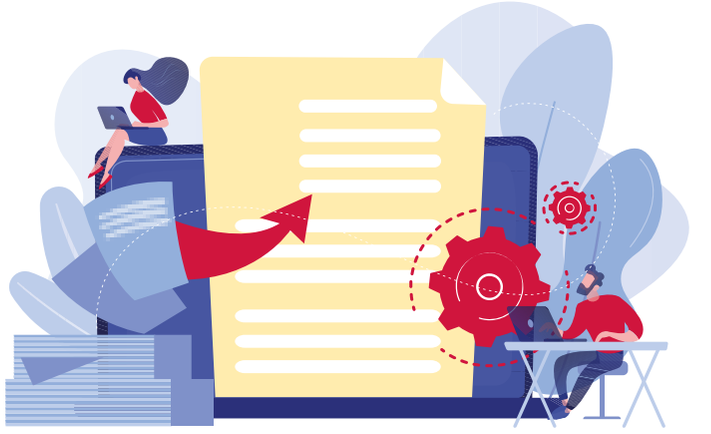
¿QUÉ ES UN ATAQUE BEC?

Fraude basado en la suplantación de correos electrónicos corporativos para inducir a empleados o directivos a realizar pagos o compartir información sensible.

Las organizaciones más afectadas suelen ser las **Pymes** con procedimientos financieros poco formalizados.

1 correo puede ser suficiente para provocar una transferencia fraudulenta.

El FBI atribuye al BEC pérdidas superiores a 50.000 millones de dólares acumulados desde 2013.

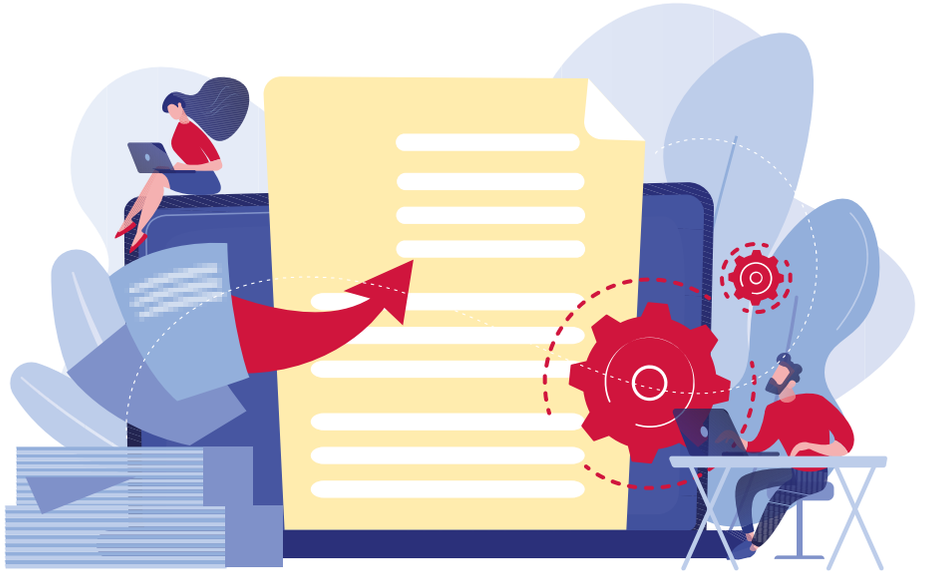


Empresa de 15 empleados
Facturación anual: 1,2 M€
Correo aparentemente enviado por el gerente.
Solicitud urgente de pago a proveedor.
Transferencia realizada: 28.500 €.
El fraude se detecta dos días después.

Recursos de apoyo

INFORME CCN-CERT

“EL CCN-CERT ES LA CAPACIDAD DE RESPUESTA A INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN DEL CENTRO CRIPTOLÓGICO NACIONAL (CCN), ADSCRITO AL CENTRO NACIONAL DE INTELIGENCIA (CNI). ESTE SERVICIO SE CREÓ EN EL AÑO 2006 COMO CERT GUBERNAMENTAL NACIONAL ESPAÑOL Y SUS FUNCIONES QUEDAN RECOGIDAS EN LA LEY 11/2002 REGULADORA DEL CNI, EL RD 421/2004 DE REGULACIÓN DEL CCN Y EN EL RD 311/2022, DE 3 DE MAYO, QUE REGULA EL ESQUEMA NACIONAL DE SEGURIDAD.”

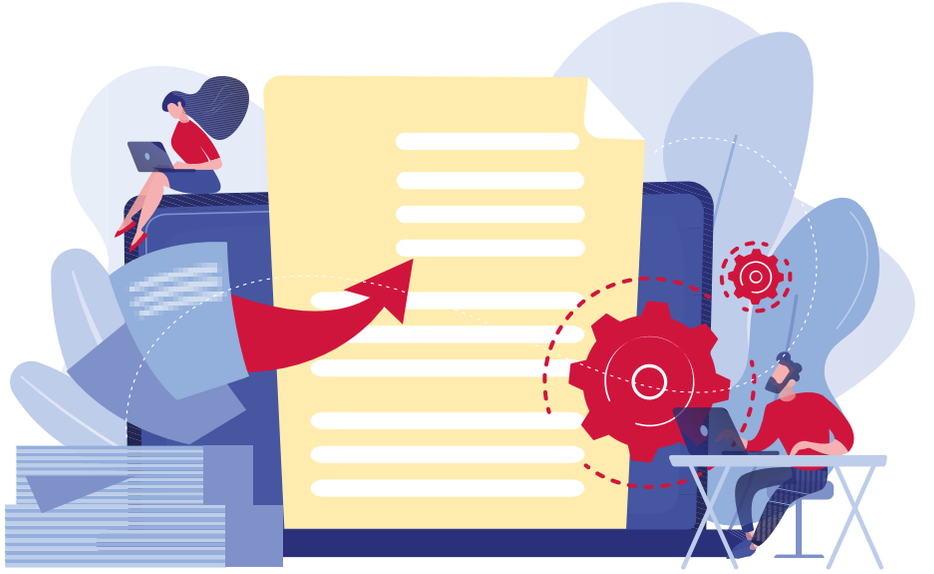


https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7364-ccn-cert-ia-04-25-ciberamenazas-y-tendencias-edicion-2025/file.html

Recursos de apoyo

ENTORNO LEGISLATIVO

- LOPDyGDD, RGPD
- ENS e Infraestructuras críticas.
- Directivas NIS, (Network & Information Systems)
    - NIS 2016, primeras exigencias.
    - NIS2, 2022, exigencias extendidas. Amplía a otros sectores, como salud, infraestructura pública, gestión de residuos, industria alimentaria, proveedores de servicios digitales...
    - En cuanto a medidas, incluye la implementación de políticas de seguridad, análisis de riesgos, gestión de incidentes y continuidad del negocio.
    - Fecha límite de adopción, 17 de octubre de 2024.



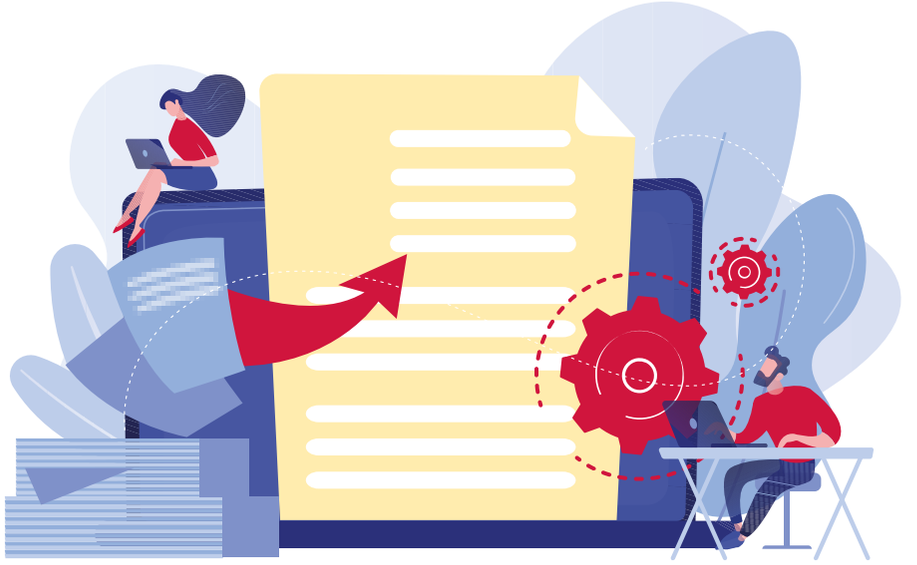
¿Alguno de mis clientes me exigirá cumplir NIS2, DORA u otra normativa por participar en la cadena de suministro?

https://www.vintegris.com/es/blog/aplicacion-directiva-nis2/

Recursos de apoyo

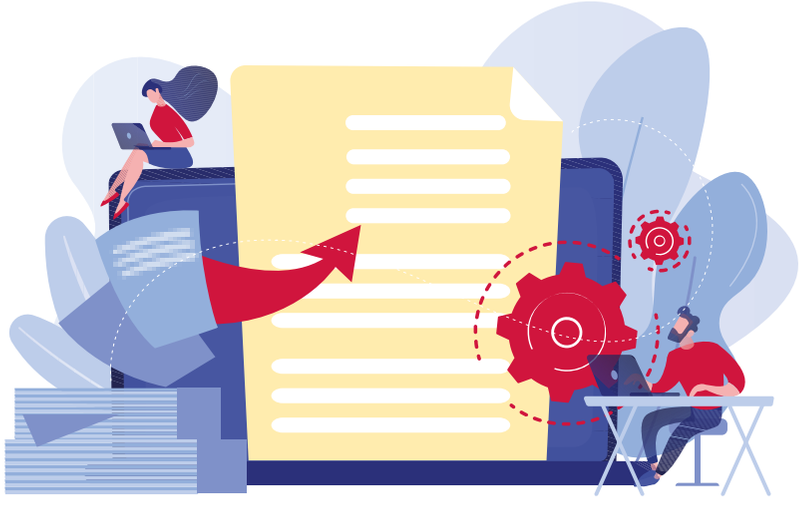
ENTIDADES DE INTERÉS

- ✓ **INCIBE**, Ciudadanos y Pymes
- ✓ **CCN**, Administraciones Públicas e Infraestructuras críticas.
- ✓ **AEPD**
- ✓ **ENISA**



https://www.incibe.es/linea-de-ayuda-en-ciberseguridad

¿Por dónde empezamos? (I)



MEJORES PRÁCTICAS

- ✓ Lo primero, cumplir la ley. Si aún no estamos obligados, lo estaremos: *Análisis de riesgos*.
- ✓ Lo segundo, seguir mejores prácticas.

Recomendaciones:

- ✓ **Copias de seguridad probadas.**
- ✓ **MFA en todos los accesos críticos.**
- ✓ **Plan de respuesta a incidentes y gestión de proveedores.**

La familia ISO/IEC 27000 es un conjunto de estándares internacionales que proporcionan directrices y mejores prácticas para la gestión de la seguridad de la información. Estos estándares ayudan a las organizaciones a proteger sus activos de información mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). El más conocido de estos estándares es el ISO/IEC 27001, que establece los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI.

¿Por dónde empezamos? (II)

¿ME VOY DE VIAJE ESTA NOCHE?

ANÁLISIS DE RIESGOS

- ✓ Una versión reducida: https://www.incibe.es/sites/default/files/contenidos/dosieres/plan-director-seguridad/plan_director_de_seguridad_hoja_para_el_analisis_de_riesgos.xlsm

- ✓ Establecer un plan de trabajo: https://www.incibe.es/empresas/que-te-interesa/plan-director-seguridad

Establecer un SGSI es un proceso complejo, que debe hacerse de forma progresiva
EL PASO MÁS DIFICIL ES EMPEZAR

¿Por dónde empezamos? (III)

CONJUNTO MÍNIMO DE MEDIDAS DE SEGURIDAD

Depende de necesidades particulares de cada negocio, en todo caso:

- ✓ Política general expresando compromiso de la organización.
- ✓ Cumplimiento legal con datos personales y por lo tanto, AR y adopción de medidas.
- ✓ Políticas de uso de los SSII y servicios, a la incorporación de los empleados.
- ✓ Política de clasificación de la información.
- ✓ Política de privilegios de acceso, otorgamiento, revocación, aprobación y revisión.
- ✓ Formación continua en materia de ciberseguridad al empleado y dirección (NIS2).
- ✓ Control de acceso a la información, basado en la política, auditado.
- ✓ Plan de disponibilidad de la información, AKA Backup.
- ✓ Monitorización de los SSII a efectos de detección de incidentes.
- ✓ Definición de responsabilidades en materia de Ciberseguridad.
- ✓ Plan de respuesta ante incidentes.

Conclusiones

BUENAS NOTICIAS

- ✓ El pilar en el que descansa la ciberseguridad es en las medidas administrativas. Está al alcance de cualquier empezar a pensar cómo quiere operar su empresa en esta materia, escribirlo y darlo a conocer.
- ✓ No es necesario invertir en lo último de lo último en tecnología, habiendo muchas soluciones adecuadas de uso libre.
- ✓ Tenemos mucha información previa, buenas prácticas y apoyo de Incibe.
- ✓ Se puede empezar en modo “aprendizaje” con alcance reducido, extendiendo el ejercicio poco a poco.
- ✓ Ya hemos hecho ejercicios similares, adecuación a la LOPD del 99 o prevención de riesgos laborales, siendo hoy día algo natural en nuestras empresas.

Conclusiones

MALAS NOTICIAS

- ✓ No hay ninguna excusa o motivo para no abordar de una manera seria e integral la ciberseguridad. No hacerlo es una temeridad.
- ✓ El panorama del ciberdelito es complicado, y al ser productivo económicamente, los retos seguirán creciendo.
- ✓ Una empresa no preparada va a tener difícil seguir operando en el corto/medio plazo.
- ✓ Las exigencias que ahora son por responsabilidad, serán legales más pronto que tarde, motivo adicional para aprovechar la oportunidad de adaptarse progresivamente.

Conclusiones

LA BOLA DE CRISTAL

- ✓ Es sabido que la seguridad resultante del conjunto es la del eslabón más débil.
- ✓ Si no hay obligación legal, habrá obligación contractual de una gestión adecuada. Ya se está dando especial relevancia a la cadena de suministro (NIS2).
- ✓ El ENS parece la legislación más avanzada del marco nacional. Consultarla y tenerla en cuenta para tomar decisiones puede ser una decisión acertada a futuro por los puntos anteriores.
- ✓ Esperar una solución global del ciberdelito parece una quimera, dada la dificultad de regular globalmente, de la ubicuidad de los atacantes y de la capacidad de anonimato que la red ofrece.

URL's de interés

- ✓ **Nomoreransom**, servicio de apoyo de iniciativa privada, pero con colaboración de múltiples entidades públicas europeas:
  https://www.nomoreransom.org/es/index.html
- ✓ Instituto nacional de Ciberseguridad, **INCIBE**:
  https://www.incibe.es/aprendeciberseguridad/ransomware
  https://www.incibe.es/linea-de-ayuda-en-ciberseguridad
  https://www.incibe.es/empresas
- ✓ Herramientas para gestión de riesgos basadas en la metodología **MAGERIT**: https://shop.ar-tools.com/
- ✓ Agencia Española de Protección de Datos, **AEPD**, guías y herramientas:
  https://www.aepd.es/guias-y-herramientas/guias
  https://www.aepd.es/guias-y-herramientas/herramientas
- ✓ Plataforma de formación de **CCN-CERT** (Angeles): https://angeles.ccn-cert.cni.es/es/

Autoevaluación

✓ Con la información obtenida en el rol play, independientemente del papel desempeñado, responde el cuestionario pensando en tu organización...

https://form.typeform.com/to/Lwpg7zC5

Datos de contacto

Alfredo Vizcaino: https://www.linkedin.com/in/alfredovizcaino/
Nacho Barnés: https://www.linkedin.com/in/nachobarnescibersecurity/