



Potencial Digital

Cáceres, 24 y 25 de septiembre

Taller 3 – Empezar en la gestión de Ciberseguridad

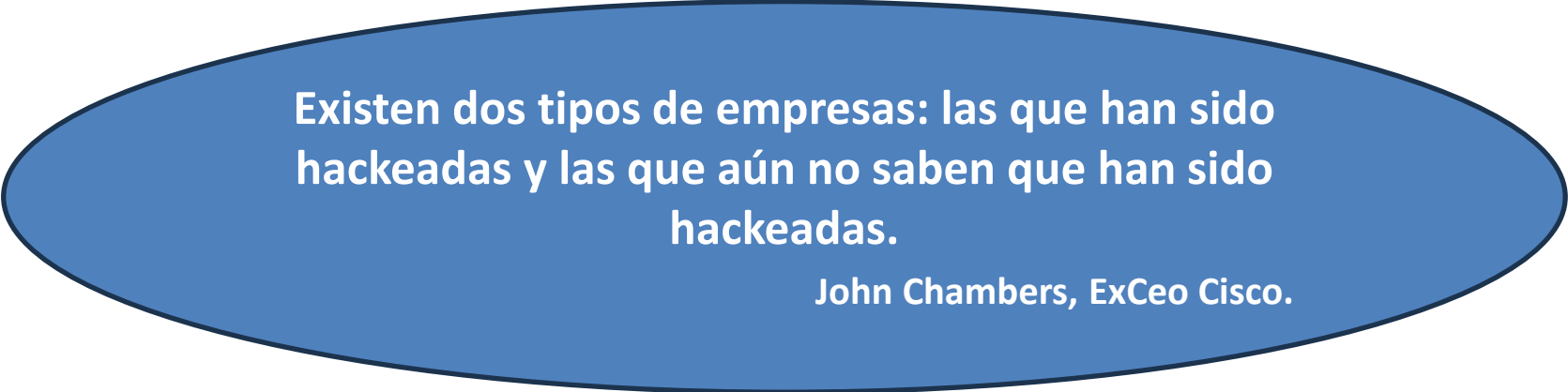


Taller 3: Análisis de Riesgos

SI, LO SABEMOS, TENEMOS QUE HACER ALGO...

SISTEMAS INFORMÁTICOS E INCIDENTES DE SEGURIDAD

- ✓ En primer lugar, debemos asumir que tenemos unos sistemas de información de los que dependemos para hacer negocios.
- ✓ En segundo lugar, tenemos que observar lo que pasa alrededor y nos llevará a asumir que tarde o temprano, tendremos un incidente de seguridad.



Existen dos tipos de empresas: las que han sido hackeadas y las que aún no saben que han sido hackeadas.

John Chambers, ExCeo Cisco.

¿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)

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.xlsx

- ✓ Establecer un plan de trabajo:

<https://www.incibe.es/empresas/que-te-interesa/plan-director-seguridad>



¿ME VOY DE VIAJE ESTA NOCHE?

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

¿Por dónde empezamos? (III)

CONJUNTO MÍNIMO DE MEDIDAS DE SEGURIDAD

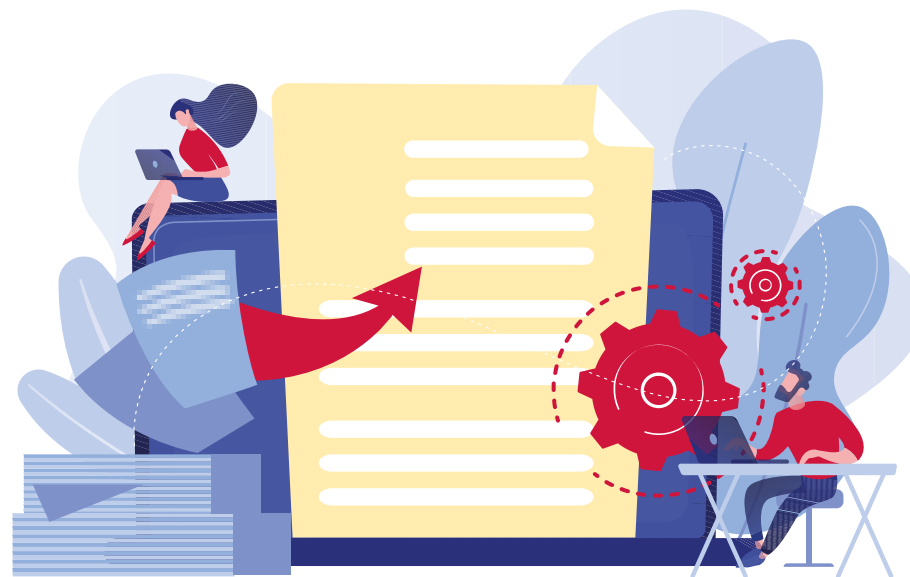
Depende de necesidades particulares de cada negocio, en todo caso:

- ✓ 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.
-

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.



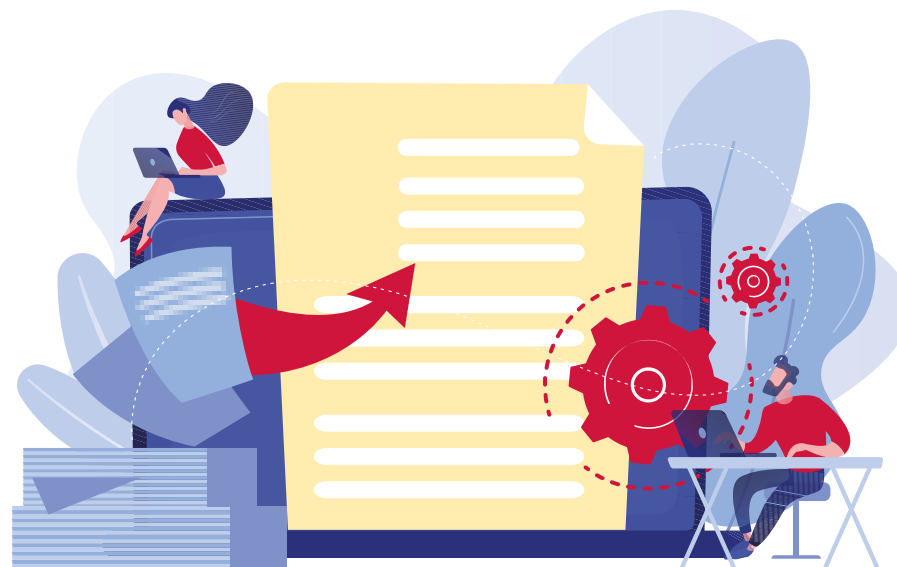
¿Alguno de mis clientes me exigirá cumplir NIS2, DORA u otra normativa por participar en la cadena de suministro?

<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>

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/>
-

TALLER 3 – EMPEZAR EN LA GESTIÓN DE LA CIBERSEGURIDAD.

PREGUNTAS

¿DUDAS, PREGUNTAS COMENTARIOS?

MUCHAS GRACIAS POR TU PARTICIPACIÓN, Y RECUERDA QUE PODEMOS HACER MUCHO POR LA CIBERSEGURIDAD CON SÓLO NO ACTUAR DE FORMA IMPROVISADA!!!!!!

Datos de contacto



Alfredo Vizcaino: <https://www.linkedin.com/in/alfredovizcaino/>

Nacho Barnés: <https://www.linkedin.com/in/nachobarnescibersecurity/>