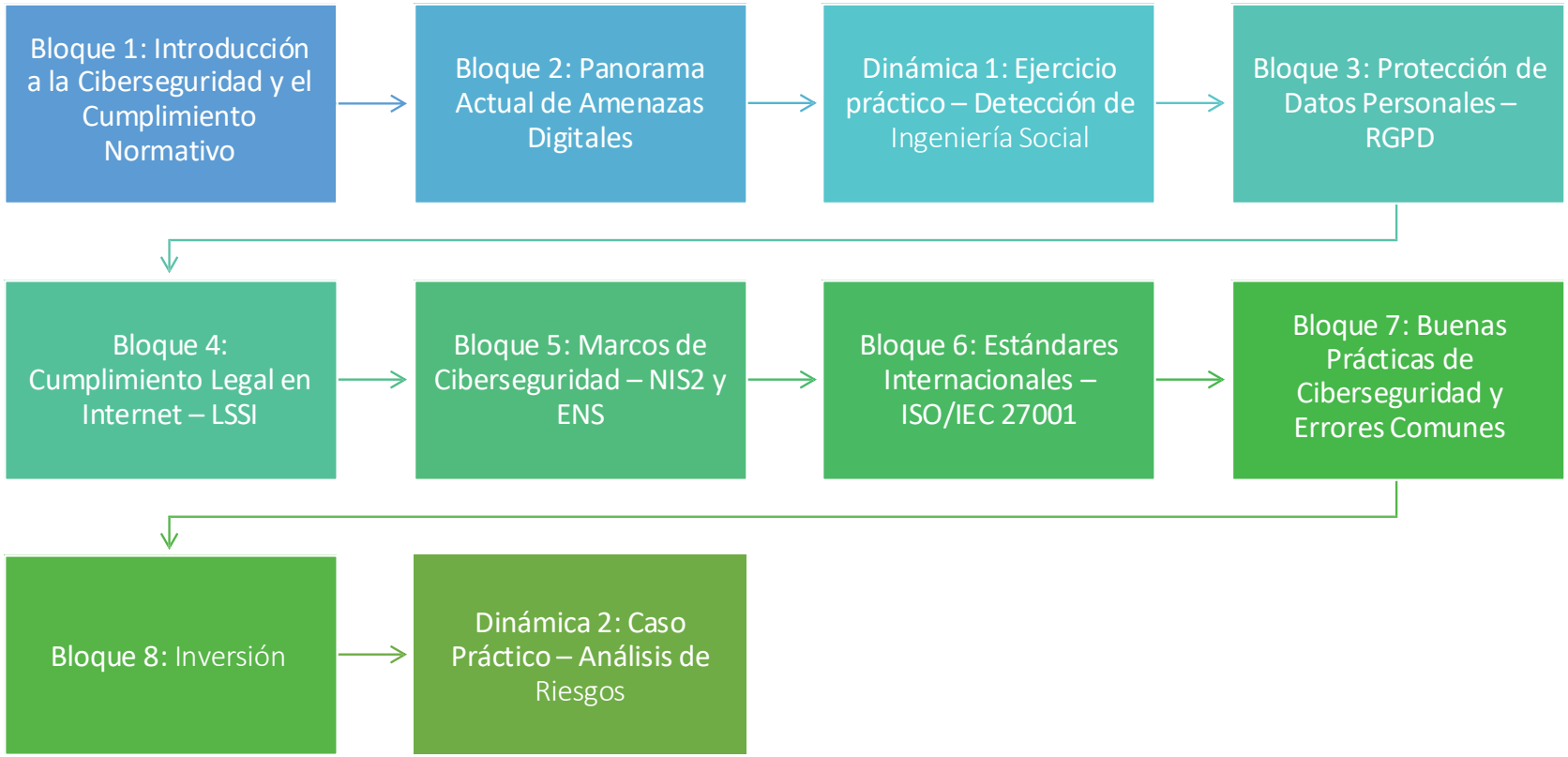
# 8.1. Ciberseguridad

# AGENDA


Bloque 1: Introducción a la Ciberseguridad y el Cumplimiento Normativo
Bloque 2: Panorama Actual de Amenazas Digitales
Dinámica 1: Ejercicio práctico – Detección de Ingeniería Social
Bloque 3: Protección de Datos Personales – RGPD
Bloque 4: Cumplimiento Legal en Internet – LSSI
Bloque 5: Marcos de Ciberseguridad – NIS2 y ENS
Bloque 6: Estándares Internacionales – ISO/IEC 27001
Bloque 7: Buenas Prácticas de Ciberseguridad y Errores Comunes
Bloque 8: Inversión
Dinámica 2: Caso Práctico – Análisis de Riesgos

# DESCRIPCIÓN DE LA SESIÓN

Sesión formativa de 3–4 horas dirigida a mandos intermedios, autónomos y directivos de pequeñas empresas, dentro del programa de Transformación Digital de ENAE Murcia.

El objetivo es formar y concienciar sobre **ciberseguridad** y **cumplimiento normativo** de forma visual, directa y pedagógica, sin tecnicismos.

Se abarcan las principales normativas (RGPD, LSSI, NIS2, ENS, ISO 27001) con ejemplos reales, buenas prácticas y ejercicios participativos.

# Bloque 1

# Introducción Ciberseguridad & Cumplimiento

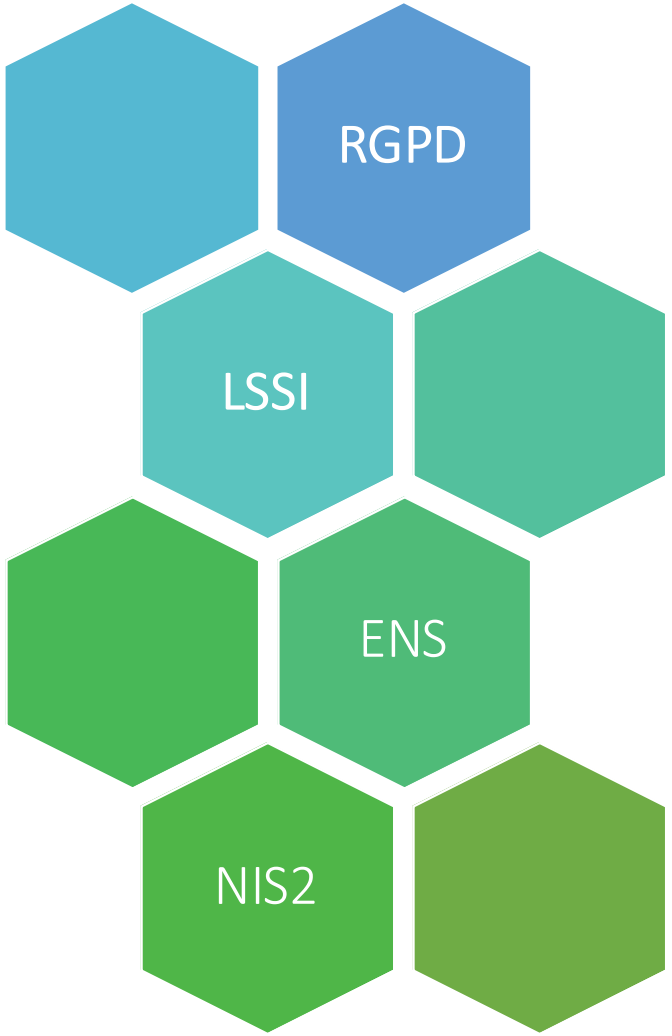
# IDEA GENERAL

¿QUÉ SENTIDO TIENE TODO ESTO PARA UNA PYME?

¿QUÉ TENGO SABER Y HACER?

¿CUÁNTO CUESTA?

# NORMATIVA



# IDEAS CLAVE

- Las pymes y autónomos también son objetivo de ciberataques
- Las pymes y autónomos deben cumplir ciertas leyes de protección de datos y seguridad.
- No vale pensar “esto le pasa solo a las grandes empresas”.
- No existe "el riesgo 0". Debemos practicar una gestión del riesgo tecnológico.
- Un ataque o sanción puede afectar seriamente la continuidad de un pequeño negocio.

# DATOS

## Impacto Económico

- Un incidente grave tiene un impacto económico aproximado de 75.000€
- Tiempo de parada y coste de recuperación. No se incluyen posibles sanciones

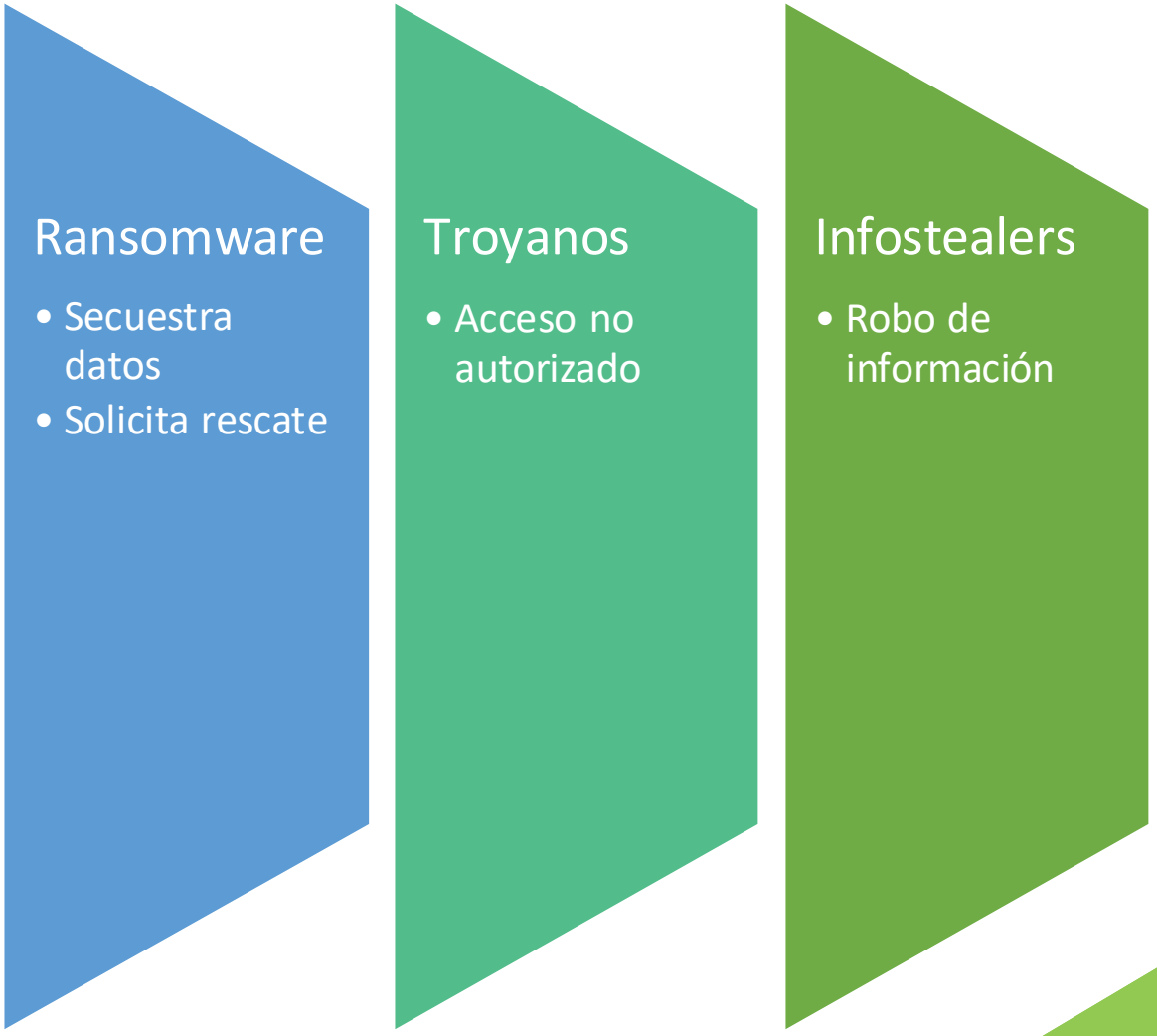
## Continuidad Operaciones

- El 60% de las pymes atacadas cierran en los 6 meses siguientes

# Bloque 2

# Amenazas Digitales

# MALWARE


Ransomware
• Secuestra datos
• Solicita rescate
Troyanos
• Acceso no autorizado
Infostealers
• Robo de información

# INGENIERÍA SOCIAL I

## Phishing

- Uso de correos electrónicos
- Robo de credenciales
- Engaño a usuarios

## Técnica más común

- Despiste del usuario
- Confianza del usuario
- Sentimientos Humanos

## Spear Phishing

- Variación "Sofisticada"
- Ataque Dirigido
- Información Precisa

# INGENIERÍA SOCIAL II

## Vishing: Engaño Telefónico

- Fingir ser una entidad confiable como un banco
- Obtener datos personales a través de llamadas

## Smishing: Engaño SMS

- Mensajes de texto que parecen legítimos
- Solicitar información personal o financiera

## WhatsApp*

- Mensajes engañosos en la plataforma
- Intentos de obtener datos personales

## No Técnico

- No es un ataque sofisticado
- No hay un gran conocimiento técnico

# CASOS

## Fraude Digital

- La Guardia Civil de la Región de Murcia ha desarticulado un grupo delictivo por cometer una estafa consistente en suplantar la identidad de una empresa para cobrar más de 100.000 euros a otra compañía hortofrutícola de Alhama de Murcia y transferir el dinero de forma inmediata a 30 cuentas bancarias diferentes.

https://bit.ly/4l9tEkb

## Ransomware

- El Ayuntamiento de Torre Pacheco ha sufrido un ciberataque que ha comprometido la operatividad y la seguridad de los datos personales de sus ciudadanos. El ataque, perpetrado mediante *ransomware*, fue descubierto cuando la Policía Local perdió acceso a los servidores municipales, encontrándolos cifrados.

http://bit.ly/4lbovbd

# CIBER HIGIENE BÁSICA

## Precaución

- La valoración del riesgo de lo que NOS PIDEN debe guiar cualquier acción que hagamos en un sistema informático.
- Riesgo Máximo: Dinero, Contraseñas y Descarga / Instalación Software.
- Riesgo Medio: Envío de Información.

## Medidas Técnicas Elementales

- Sistema Actualizado
- Antivirus Funcionando
- Contraseñas Robustas

# Dinámica 1

# Detección de Ingeniería Social

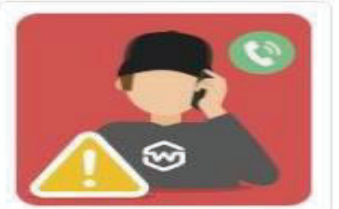
# Ingeniería Social ¿Sí o No?

A continuación, te mostramos 7 casos muy distintos en los que la Ingeniería Social afectan a la familia Cibernauta. Entra en cada uno de ellos y pon en práctica tus conocimientos.

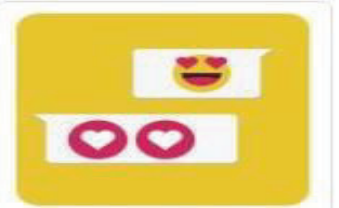
*Phishing, vishing, smishing, sexting... ¡Encuentra las soluciones correctas!*

Problema en red social

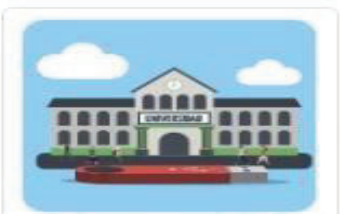

Factura disponible



Soporte técnico



Relación de pareja

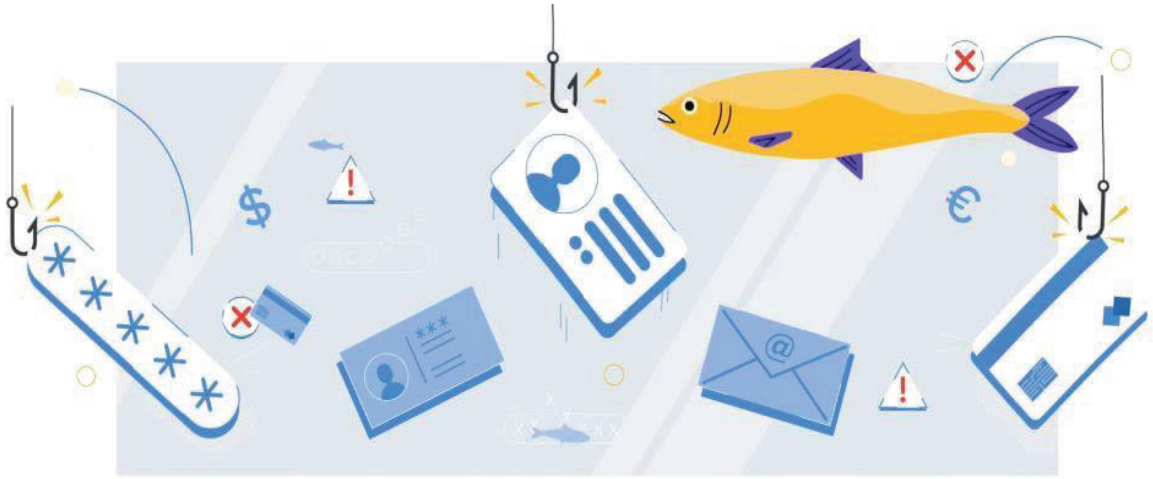


Usb perdido

Cupón WhatsApp

Código Sms

https://bit.ly/4jbZT0l



# ¿Puedes detectar cuándo te están engañando?

En los ataques de phishing, los atacantes intentan engañar a los usuarios desprevenidos para que revelen información personal o financiera, a menudo haciéndose pasar por empresas conocidas y de confianza.

La IA ya está haciendo que los ataques de phishing sean más sofisticados, personalizados y frecuentes.

¿Crees que puedes distinguir lo que es real de lo que no lo es?

Hacer el test

https://phishingquiz.withgoogle.com/

# Bloque 3

# Protección de Datos Personales – RGPD

# LOPD FÁCIL

## PRINCIPIOS FUNDAMENTALES

- Licitud, lealtad y transparencia
- Minimización de datos (sólo lo necesario)
- Limitación de la finalidad
- Exactitud (datos correctos y actualizados)
- Limitación del plazo de conservación
- Integridad y confidencialidad
- Responsabilidad proactiva

## OBLIGACIONES

- Consentimiento y consentimiento explícito
- Notificar brechas (72 horas)
- DPO cuando sea necesario
- Evaluar riesgos (incluyendo EIPD)
- Medidas técnicas y organizativas adecuadas

## DERECHOS

- Derecho de acceso
- Derecho a la rectificación
- Derecho al olvido (supresión)
- Derecho a la limitación del tratamiento
- Derecho a la portabilidad
- Derecho de oposición

## INCUMPLIMIENTO

- Multas de hasta 20 millones de euros o el 4% de la facturación
- Reclamaciones legales*
- Pérdida de confianza y daño reputacional

# SANCIONES

## ENDESA

- 6,1M€ a la eléctrica por exponer datos de clientes debido a que credenciales internas de acceso se publicaron accidentalmente en Facebook

## UNIQLO

- 270.000€ por un error humano. Un empleado envió por correo las nóminas de 447 trabajadores a toda la plantilla por equivocación.

## ¿Y MURCIA?

- 20.000€ a una óptica de Murcia por el envío de comunicaciones comerciales
- La cliente había solicitado que dejaran de enviarle comunicaciones comerciales

# CONSEJOS

- Saber qué datos recoges y para qué los reconges (Excel)
- Informar a los usuarios qué se va a hacer con sus datos y no hacer nada más que eso
- Solicitar consentimiento expreso para tratamientos que impliquen fines comerciales.
- Atender cualquier reclamación de derechos de los usuarios
- Tener un aviso legal y contar con una política de privacidad
- Implementar medidas de seguridad básicas (contraseñas, cifrado, backups)
- Eliminar datos innecesarios

# Bloque 4

# Cumplimiento Legal en Internet – LSSI

# LSSI FÁCIL

## Aviso Legal en la Web:

- Toda página empresarial debe identificar al titular (nombre/razón social, NIF/CIF, dirección, email, datos registrales).
- Ejemplo: Sección "¿Quiénes somos?" o "Aviso Legal" en el pie de página.

## Política de Cookies:

- Informar y obtener consentimiento del usuario antes de instalar cookies (exceptuando las técnicas).
- Ofrecer la opción de rechazar cookies no esenciales.

## Comunicaciones Comerciales (Email/SMS):

- La LSSI prohíbe el spam; se requiere consentimiento previo o ser cliente de productos/servicios similares.
- No se deben comprar listas de emails ni añadir a usuarios sin su permiso.

## Venta Online – Información y Proceso:

- El e-commerce debe proporcionar descripción clara de productos, precios (con impuestos), gastos de envío, proceso de compra y confirmación de pedidos.
- Obligaciones adicionales incluyen políticas de devolución y medios de pago seguros.

# SANCIONES

## SEAT

- La agencia de protección de datos sanciona con hasta 20.000 euros a Seat por su política cookies.

## IBERIA

- La Audiencia Nacional ha confirmado la multa de 30.000 euros que la Agencia Española de Protección de Datos (AEPD) impuso a Iberia por incumplimiento de la LSSI en relación a la política de cookies de su página web.

# CONSEJOS

## Revisa tu web

- Incluir *Aviso Legal*, *Política de Privacidad* y *Política de Cookies*.
- Puedes usar plantillas online, pero lo ideal es adaptarlas con asesoramiento profesional.

## Gestor de cookies

- Usa herramientas como Cookiebot (plan gratuito) o scripts manuales para bloquear cookies hasta que el usuario acepte.
- Si no eres técnico, pide ayuda a tu desarrollador web.

## Email marketing responsable

- Solo envía correos a usuarios que hayan dado su consentimiento expreso (doble opt-in).
- Siempre incluye un enlace claro para darse de baja (obligatorio por ley).

## No “apures” la ley

- Aunque se permita contactar a exclientes hasta 1 año, es mejor pedir permiso explícito.

# Bloque 5

# Marcos de Ciberseguridad ENS & NIS2

# ENS DE UN VISTAZO

## ¿Qué es?

- Marco normativo español que fija un nivel mínimo de ciberseguridad para la Administración Pública y sus proveedores.

## ¿A quién afecta?

- Obligatorio para organismos públicos y para empresas que trabajen con ellos (por ejemplo, en licitaciones públicas).
- Te afecta si eres proveedor de la Administración Pública (o si trabajas con ellos).

## Beneficios:

- Certificar tu nivel de seguridad puede ser una ventaja competitiva.

# ¿DE QUÉ HABLAMOS?

**Control de accesos:**

- Gestión de usuarios y permisos para asegurar que solo personal autorizado acceda a los sistemas.
- Implementación de autenticación robusta (contraseñas seguras, autenticación multifactor).

**Protección de la información:**

- Cifrado de datos sensibles, tanto en reposo como en tránsito.
- Mecanismos de respaldo y recuperación de datos (backups periódicos).

**Actualizaciones y parches:**

- Instalación y actualización regular de sistemas operativos y aplicaciones para corregir vulnerabilidades.

**Seguridad en la red:**

- Uso de firewalls y sistemas de detección de intrusiones.
- Cifrado de las comunicaciones

**Monitorización y auditoría:**

- Registro y seguimiento de eventos de seguridad para detectar y responder rápidamente a incidentes.
- Auditorías internas periódicas de las medidas de seguridad aplicadas.

**Concienciación y formación:**

- Capacitación básica del personal sobre buenas prácticas de ciberseguridad y gestión de incidentes.

# ESTADO ENS


Administración General del Estado
5
9
25
11
Comunidades Autónomas
2
7
57
48
Entidades Locales
28
1
250
221
Universidades
1
3
11
7
Sector Público Institucional
64
18
1174
1092
Empresas Certificadas
33
536
1538
969

# NIS2 DE UN VISTAZO

## ¿Qué es?

- Nueva ley europea (en vigor desde 2023, obligatoria desde 2024) para reforzar la ciberseguridad en sectores críticos.

## ¿A quién afecta?

- Energía
- Transporte
- Banca y entidades financieras
- Salud
- Telecomunicaciones
- Proveedores digitales y servicios en la nube
- Otros sectores críticos (p.ej. gestión de residuos, fabricantes de productos sanitarios)

## Tamaño

- Empresas medianas y grandes.
- ¿Y los pequeños? Si eres proveedor de una empresa afectada, tendrás que cumplir ciertos requisitos de seguridad.

## Obligaciones

- Implantar medidas técnicas y organizativas proporcionales a tus riesgos.
- Notificar incidentes de seguridad en plazos muy breves.

# ¿DE QUÉ HABLAMOS?

## BLOQUE V - ENS & NIS2

# ENS & NIS2


¿DISPONE DE CERTIFICADO ENS?
ens
Esquema Nacional de Seguridad
SÍ
NO
ALTA
MEDIA | BÁSICA
Tomar medidas técnicas, operativas y de organización adecuadas y proporcionales para gestión de riesgos e incluir al menos los elementos Art.21 NIS2.
En base a análisis de riesgos: completar medidas con gestión servicios externos (cadena suministro)
+
continuidad.
CUMPLE MEDIDAS DE LA NIS2

# UN APUNTE SOBRE NIS2

## Sanciones y responsabilidades

- NIS2 endurece sanciones por incumplimiento (10M€ e inhabilitación de directivos en casos graves)

## Relevancia

- La alta dirección debe implicarse en gestionar el riesgo cibernético, no delegarlo ciegamente.

# Bloque 6

# ESTÁNDARES INTERNACIONALES ISO27001

# ISO27001 DE UN VISTAZO

## ¿Qué es?

- Norma internacional voluntaria para gestionar la seguridad de la información.
- Guía integral para establecer un Sistema de Gestión de Seguridad de la Información (SGSI) con políticas, procedimientos y controles continuos.

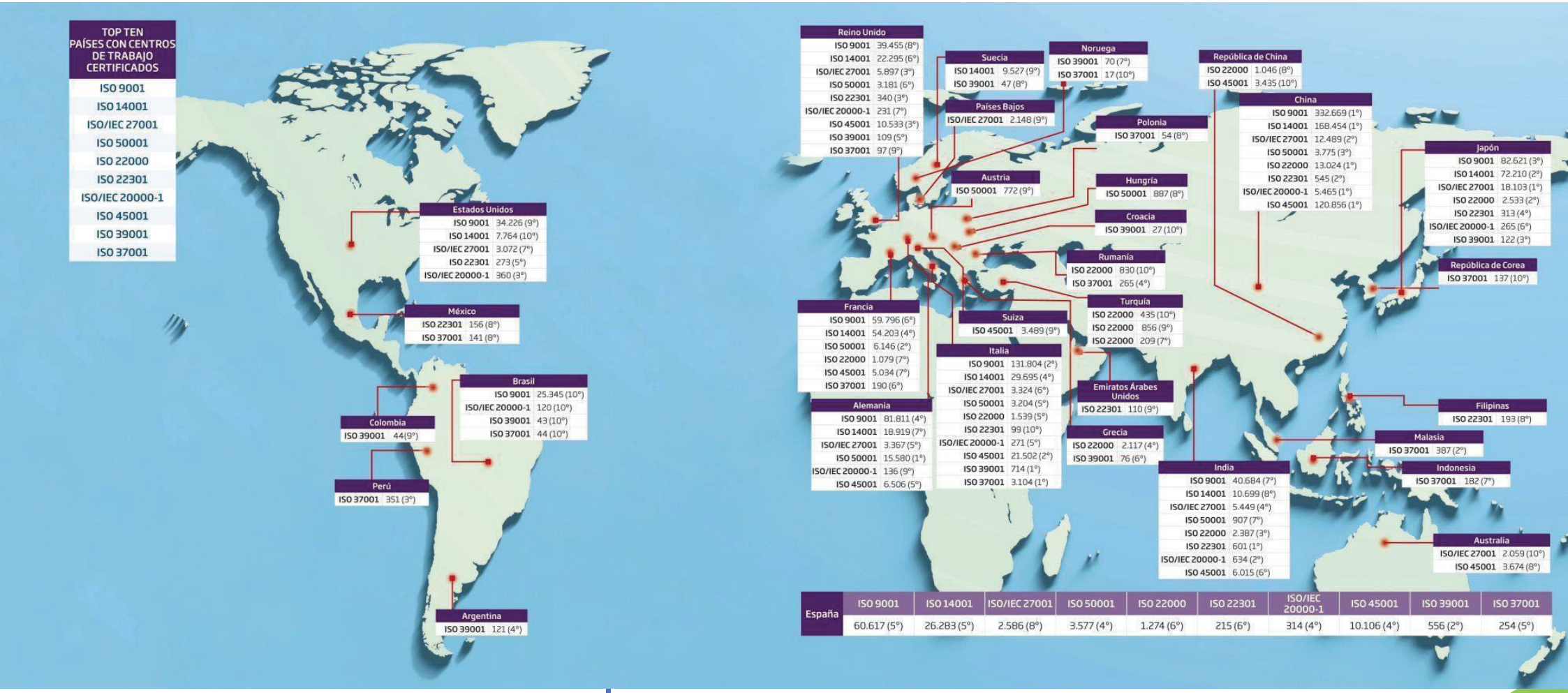
## Beneficios

- Identifica y mitiga riesgos.
- Protege activos (datos, sistemas).
- Facilita el cumplimiento de requisitos legales (RGPD, NIS2, ENS, etc.).
- Mejora la organización interna y la concienciación de empleados.
- La certificación oficial (por ejemplo, AENOR) avala el compromiso en ciberseguridad.

## Aplicabilidad

- No solo para grandes empresas; los principios pueden adoptarse sin certificación formal.
- Útil para startups y empresas de servicios que manejan datos de terceros para competir en contratos con grandes clientes.

# BLOQUE VI - ISO27001

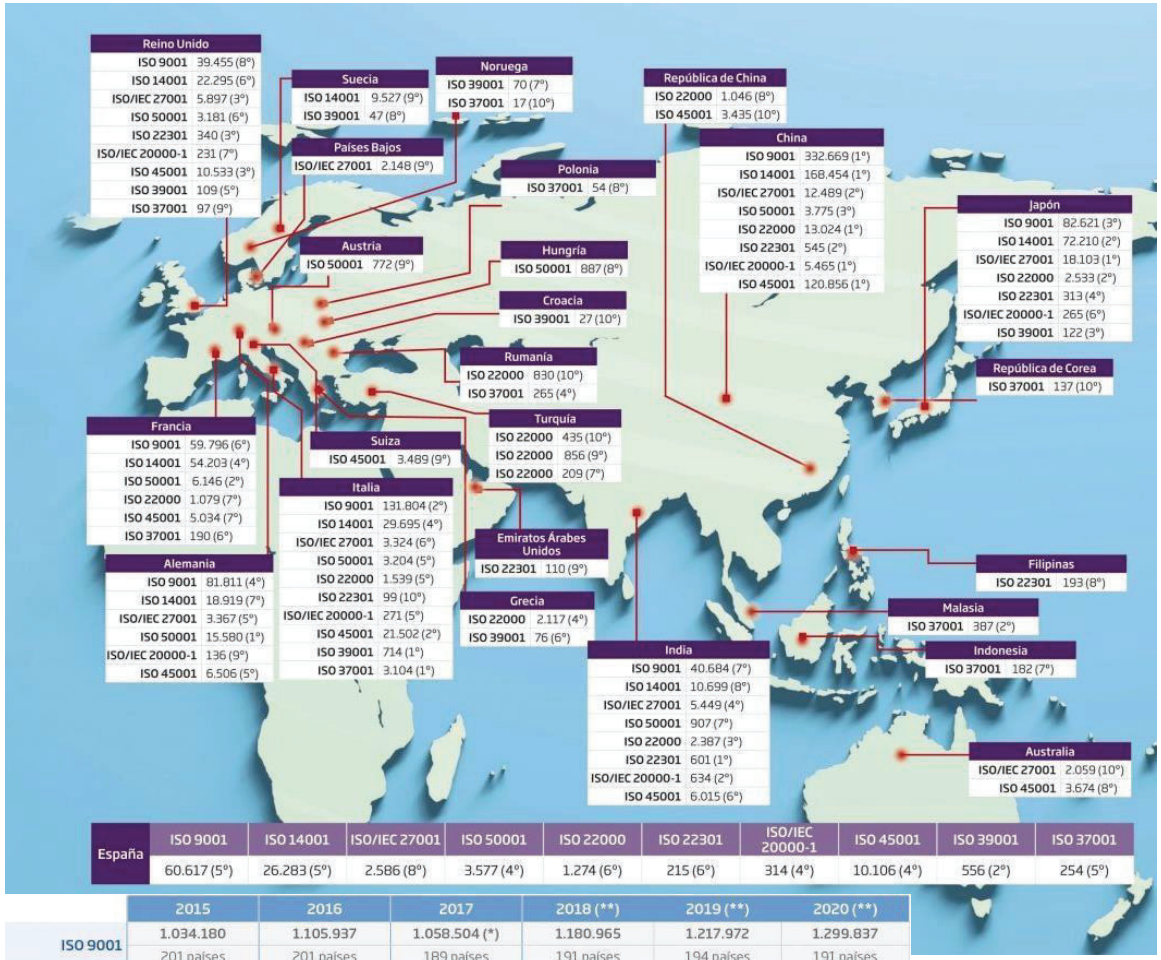



| España | ISO 9001 | ISO 14001 | ISO/IEC 27001 | ISO 50001 | ISO 22000 | ISO 22301 | ISO/IEC 20000-1 | ISO 45001 | ISO 39001 | ISO 37001 |
|---|---|---|---|---|---|---|---|---|---|---|
| | 60.617 (5°) | 26.283 (5°) | 2.586 (8°) | 3.577 (4°) | 1.274 (6°) | 215 (6°) | 314 (4°) | 10.106 (4°) | 556 (2°) | 254 (5°) |

# ISO27001 COMO INSPIRACIÓN

- Realizar un análisis de riesgos simplificado (tabla de riesgos, probabilidades, impacto y medidas).
- Definir políticas básicas (seguridad, uso de dispositivos personales, backups).
- Fomentar la formación y concienciación continua (recordatorios mensuales, cursos online gratuitos).
- Revisar y actualizar periódicamente las medidas de seguridad.
- Evaluar proveedores y sistemas contratados.

# ISO27001 EN CIFRAS




| España | ISO 9001 | ISO 14001 | ISO/IEC 27001 | ISO 50001 | ISO 22000 | ISO 22301 | ISO/IEC 20000-1 | ISO 45001 | ISO 39001 | ISO 37001 |
|---|---|---|---|---|---|---|---|---|---|---|
| | 60.617 (5°) | 26.283 (5°) | 2.586 (8°) | 3.577 (4°) | 1.274 (6°) | 215 (6°) | 314 (4°) | 10.106 (4°) | 556 (2°) | 254 (5°) |

| | 2015 | 2016 | 2017 | 2018 (**) | 2019 (**) | 2020 (**) |
|---|---|---|---|---|---|---|
| ISO 9001 | 1.034.180 | 1.105.937 | 1.058.504 (*) | 1.180.965 | 1.217.972 | 1.299.837 |
| | 201 países | 201 países | 189 países | 191 países | 194 países | 191 países |
| ISO 14001 | 319.496 | 346.147 | 362.610 | 447.547 | 487.950 | 568.798 |
| | 201 países | 201 países | 181 países | 183 países | 183 países | 180 países |
| ISO/IEC 27001 | 27.536 | 33.290 | 39.501 | 59.934 | 68.930 | 84.181 |
| | 150 países | 150 países | 160 países | 162 países | 157 países | 165 países |

| Marco | ¿Qué regula? | ¿A quién aplica? | ¿Es obligatorio? | Enfoque principal | Clave |
|---|---|---|---|---|---|
| **RGPD / LOPD / LSSI** | Protección de datos personales y confianza digital | Toda empresa o profesional que trate datos personales o tenga un sitio web | ✅ Sí (obligatorio por ley en la UE) | Derechos de los usuarios, tratamiento de sus datos y comercio electrónico | Debes aplicarlas *siempre* |
| **ENS** | Seguridad en la Administración Pública | AAPP y empresas que prestan servicios a la Administración | ✅ Sí (para AAPP y proveedores públicos) | Requisitos técnicos, operativos y organizativos de ciberseguridad | ¿Licitas con la AAPP? Te interesará |
| **NIS2** | Seguridad en sectores esenciales | Empresas medianas y grandes en sectores críticos o importantes | ✅ Sí (obligatorio desde 2024 en la UE) | Gestión de riesgos e incidentes de ciberseguridad | ¿Trabajas con sectores esenciales? Te interesará |
| **ISO/IEC 27001** | Gestión de la seguridad de la información | Cualquier organización que quiera certificar su SGSI | ❌ No (voluntario, pero reconocido) | Estándar internacional, enfoque sistemático y auditable | Certificación para ganar confianza o diferenciarse |

# Bloque 7

# BUENAS PRÁCTICAS & ERRORES COMUNES

# PASSWORDS

## La Base

- Contraseñas fuertes
- Contraseñas únicas
- Si tienes que recordarla, mejor una frase.

## Error común

- Reutilizar la misma en todo (si te la roban en un sitio, comprometes todos).

## Recomendación

- Gestores de contraseñas para no tener que recordarlas todas (p.ej. Keepass)

# MFA

## La Base

- Habilitar MFA (Segundo Factor) en todos los sitios que puedas
- Correo, RRSS, Accesos Remotos, ..
- El MFA permite bloquear muchos de los accesos no autorizados aunque conozcan la clave

## Error común

- Confiar solo en la contraseña "porque es robusta".

## Recomendación

- **Google Authenticator, Microsoft Authenticator o mensajes SMS al móvil.**
- **Son capas extra que añaden mucha seguridad con poco esfuerzo.**

# UPDATES

## La Base

- TODO el software debe actualizarse al menos cada 3 meses.
- Esto aplica a sistema operativo, navegadores, aplicaciones, teléfonos móviles, etc, etc.

## Error común

- Posponer los parches indefinidamente y ejecutar software EoL (Fuera de soporte)

## Recomendación

- Usa actualización automática siempre que puedas.
- Migra software obsoleto antes de que finalice su vida útil
- Si no actualiza automáticamente, planifica un calendario.

# BACKUP

## La Base

- Realizar backups periódico de la información (y en función de tu necesidad de los sistemas).
- Valora cuanto tiempo de información puedes perder en caso de desastre.

## Error común

- No tener una copia deslocalizada e inalterable y perder todos los datos tras una catástrofe (p.ej. Ransomware)

## Recomendación

- 3 copias de la información (una primaria y dos copias de seguridad), 2 copias locales en diferentes medios, 1 copia fuera de sitio principal, 1 copia inmutable y 0 réplicas que no validen de manera automática que la restauración funcionará cuando sea necesaria.

# ENDPOINT

## La Base

- Tener un producto antivirus/antimalware lo más avanzado que podamos permitirnos.
- Cifrar los discos de los dipositivos móviles (portátiles y móviles)
- No usar dispositivos de terceros o personales en el ámbito profesional

## Error común

- Utilizar dispositivos sin medidas de seguridad básicas (incluyendo equipos personales)

## Recomendación

- Usa un NGAV como CrowdStrike o equivalente.
- Usa Bitlocker para cifrar tus dispositivos Windows.
- Usa Cifrado en tus dispositios móviles (activo por defecto*)

# REDES Y WIFI

## La Base

- **Wi-Fi con WPA2/3 y contraseña robusta (no usar la que viene por defecto en el router si es débil)**
- **Segmentar** la red de tal forma que los **invitados** estén separados **de** los usuarios y los servidores (si hay) de cualquier otro dispositivo
- No conectar a redes no confiables

## Error común

- Tener WIFIs con contraseña debil o sin contraseña que dan acceso a toda la red de la empresa
- Conectar a redes wifi públicas de cualquier lugar

## Recomendación

- Utiliza un firewall que proteja tu tráfico de red corporativo
- Usa un AP que permita, al menos, 2 redes diferentes y tráfico segregado para ellas
- Utiliza siempre tu dispositivo 4G/5G para acceder a Internet en sitios públicos

# PERMISOS Y PRIVILEGIOS

## La Base

- Asegurar que cada empleado o colaborador tenga acceso solo a lo necesario (principio de mínimo privilegio).
- Revocar accesos cuando alguien deja de colaborar inmediatamente.

## Error común

- Cuentas antiguas activas, o todos usando la misma cuenta genérica. Eso dificulta responsabilidades y aumenta riesgo.
- Silos de información por falta de control centralizado

## Recomendación

- Invierte en una plataforma de colaboración corporativa (gSuite, Microsoft 365, …)
- Asigna roles y privilegios razonables a tu tamaño
- Ten un procedimiento de alta, baja y modificación de permisos y cúmplelo.

# SHADOW IT & SOHO IT

## La Base

- No se puede usar cualquier aplicación o producto que se nos pase por la cabeza.
- Una empresa debería fijar qué soluciones IT de mercado profesional, adaptadas a nuestras necesidades y respaldadas por fabricantes se puden usar.

## Error común

- Permitir usar cualquier aplicación, producto o tecnología asumiendo riesgos innecesarios (pérdidas de información, robos de información, falta de soporte, ...) *¿Alguien dijo GPT?*
- Usar productos del sector SOHO (muchas veces producto doméstico remarcado) como si fuera una solución profesional.

## Recomendación

- Define tu "stack" tecnológico: qué aplicaciones vas a usar y por qué.
- Evalua racionalmente entradas y salidas de estas.
- Invierte en productos de sector profesional, amparados por fabricantes y con garantías de seguridad.

# INCIDENTES

## La Base

- Vas a tener incidentes de seguridad.
- Debes tener mínimamente claro qué hacer en cada uno de ellos.

## Error común

- Pensar que por tener medidas de protección estamos exentos de sufrir un incidente de seguridad. *¿Acaso por tener una alarma los ladrones no entran a robar?*
- *Ante un incidente, entrar en pánico y no saber que hacer.*

## Recomendación

- Tener 2 o 3 protocolos básicos de actuación, por ejemplo, ante un ransomware y ante un phishing.
- Ten un soporte informático especializado preacordado.
- Practica pequeños ejercicios de simulación de qué pasaría si sufrieras un incidente.
- Un seguro de ciberriesgo te puede ayudar*

# CULTURA DE SEGURIDAD

## La Base

- Fomentar una cultura de ciberseguridad en la empresa.
- Enviar píldoras, recordatorios y fomentar la concienciación sobre los riesgos más comunes.

## Error común

- Pensar que la ciberseguridad es "un problema técnico" del que se encargarán "los informáticos.

## Recomendación

- Aprovecha los recursos gratuitos de INCIBE para concienciación.
- Si puedes, invierte en alguna acción de concienciación específica para tu negocio y desarollada por profesionales.

# Bloque 8

# INVERSIÓN

# BLOQUE VIII – INVERSIÓN

| Categoría | Producto / Solución | Costo Estimado | Observaciones |
|---|---|---|---|
| **Licencias & Servicios en la Nube** | Microsoft 365 para 10 usuarios | ~2.520 €/año (210 €/mes) | Incluye licencia Windows, Correo, Paquete Office, Almacenamiento en la nube y funciones seguridad integradas. |
| **Firewall & Enrutamiento** | Firewall Empresarial (amortizado a 5 años) | ~550 €/año (~1.100€ en HA) | Dispositivo de seguridad perimetral y enrutamiento, inversión a largo plazo. |
| **Switches & AP** | Switch & AP Empresarial (amortizado a 5 años) | ~180 €/año (~360€ en HA) | Permite conectar y segmentar la red interna. |
| **Protección Endpoint** | NGAV para 10 usuarios | ~600 €/año | Solución avanzada para proteger endpoints contra amenazas y malware. |
| **Mantenimiento & Soporte** | Contrato de mantenimiento (soporte, actualizaciones, monitorización) | ~4.800 €/año (400 €/mes) | Asegura el correcto funcionamiento y actualización de sistemas y dispositivos. |
| **Formación y Concienciación** | Talleres de ciberseguridad para empleados | ~1.500 €/año | Capacita al equipo para prevenir incidentes (ej. phishing, uso inadecuado de herramientas). |
| **Seguro de Ciberriesgo** | Seguro que cubra incidentes y brechas de seguridad | ~1.000€/año | Mitiga el impacto económico de posibles ciberataques o brechas de seguridad. |
| **Total Aproximado** | | **10.000 ~ 12.000 €/año** | Inversión integral para una pequeña empresa 10 trabajadores , que combina soluciones tecnológicas, soporte, formación y cobertura de riesgos. |

# BLOQUE VIII – INVERSIÓN

| Amenaza | Impacto Económico Directo Estimado (€) | Descripción |
|---|---|---|
| **Phishing** | 10.000€ ~ 50.000€ | Robo de credenciales y fraude en transacciones; puede afectar a la operativa y generar costes en recuperación y soporte. |
| **Ransomware** | 75.000€ ~ 120.000€ | Cifrado de datos críticos y exigencia de rescate, interrupción del negocio; costos asociados a la restauración, notificación y, en ocasiones, multas. |
| **Malware/Virus** | ~1.000€ | Impacto en productividad y costes de recuperación de sistemas infectados; puede requerir reparaciones técnicas y gastos en soporte IT. |
| **Brecha de Datos** | 10.000€ ~ 50.000€ | Filtración de datos de clientes o empleados, multas regulatorias. No se valora la pérdida de confianza. |

# Dinámica 2

# Análisis de Riesgos

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

# Herramienta de Autodiagnóstico

## Conoce tus riesgos en cinco minutos

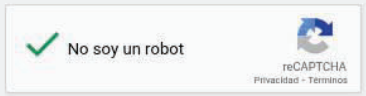
**Las empresas dependen para su funcionamiento de la información y de la tecnología: ordenadores, teléfonos móviles y tabletas, bases de datos, líneas de comunicaciones...**

Pero, ¿has pensado alguna vez en lo que ocurriría si, de repente, perdieses la información de tu negocio o la capacidad de acceder a ella? Seguro que tu empresa está expuesta a amenazas que ni siquiera imaginas.

### ¿Quieres gestionar la seguridad de tu negocio?

Te proponemos una evaluación inicial del riesgo de seguridad de tu negocio en función de cómo utilizas la tecnología: correo electrónico, página web, tabletas, smartphones, etc.

Reflexiona sobre estas sencillas cuestiones para conocer el estado de ciberseguridad de tu empresa y cuáles son los riesgos que te afectan. Así sabrás por dónde empezar a mejorar.




Calcula el riesgo de tu negocio

Esta herramienta es un primer paso para mejorar la ciberseguridad de tu negocio. Si necesitas más información consulta el apartado **Protege tu empresa. ¿Qué te interesa?**

https://adl.incibe.es/