Club de Calidad
Noviembre 2025

GUÍA DE CIBERSEGURIDAD PARA PYMES

Diagnóstico, primeros pasos y estrategias

Club de calidad
Avanzando en gestión

Principado de Asturias
Consejería de Ciencia, Industria y Empleo

¿Para quién es esta Guía?

Esta guía está dirigida a responsables y equipos de pequeñas y medianas empresas asturianas que buscan mejorar su seguridad digital mediante medidas prácticas, accesibles y adaptadas a distintos niveles de madurez, sin necesidad de conocimientos técnicos avanzados, y con especial atención a los riesgos reales que enfrentan en su día a día.

ÍNDICE

ENTREVISTAS

Enrique Pérez de Tena
Responsable de la Oficina de Relaciones Institucionales del Mando Conjunto del Ciberespacio (MCCE)

— Página 29

Santos González
Catedrático Emérito de Álgebra de la Universidad de Oviedo

— Página 43

Cristina Fernández Caldueño
Directora de Operaciones de Castroalonso

— Página 51

Félix Barrio
Director General de INCIBE

— Página 11

Esta guía nace para dar respuesta a una necesidad real y urgente: **ayudar a las PYMES asturianas a protegerse frente a los riesgos digitales y avanzar en su transformación digital de forma segura.**

La necesidad de este proyecto surge del análisis y la experiencia compartida por el Grupo de Trabajo de CIOs, formado por responsables tecnológicos de empresas asturianas, que han puesto de manifiesto los retos y carencias en materia de ciberseguridad en el tejido empresarial regional. Su visión ha sido fundamental para identificar la importancia de contar con una herramienta práctica y adaptada a la realidad de las PYMES.

El proyecto, **financiado por la Consejería de Ciencia, Industria y Empleo del Principado de Asturias**, pone en manos de las PYMES una herramienta útil y accesible, validada por expertos y empresas, que facilita la adopción de buenas prácticas y refuerza la competitividad y la confianza en el entorno digital.

INTRODUCCIÓN

La ciberseguridad no es un lujo reservado a grandes empresas, sino una necesidad real también para las pequeñas y medianas empresas (las "PYMES") asturianas, que cada día dependen más de la tecnología para relacionarse con clientes, proveedores y administraciones. No se trata de gastar grandes presupuestos ni de dominar la informática, sino de adoptar hábitos sencillos y responsables que protejan lo más valioso de cualquier negocio: la información propia y ajena y la confianza de los clientes.

Esta guía está pensada como un manual práctico, con pasos claros y estrategias realistas para que cada PYME pueda reforzar su seguridad digital sin importar su tamaño o sector. Porque en un mundo conectado, la mejor ventaja competitiva es estar prevenidos.

Para la elaboración de esta guía, se ha recopilado información actualizada de instituciones nacionales clave en materia de Ciberseguridad, como el Instituto Nacional de Ciberseguridad INCIBE-CERT, el Centro Criptológico Nacional CCN- CERT y se han seguido además directrices emitidas por la Agencia de la Unión Europea para la Ciberseguridad, ENISA, por sus siglas en inglés.

CONCEPTOS BÁSICOS

Antes de pasar a la acción, conviene aclarar algunos conceptos básicos. No es necesario ser experto en informática: basta con entender qué protegemos y de qué amenazas debemos cuidarnos. A continuación, se muestra la definición de algunos de los términos más comunes en esta materia. Además, al final de la guía se incluye un listado de definiciones que servirá como referencia práctica para reforzar la comprensión de los conceptos clave.

Tríada de la seguridad de la información

("CIA", por sus siglas en inglés: **C**onfidentiality, **I**ntegrity, and **A**vailability)

Confidencialidad

Sólo acceden quienes están autorizados

Integridad

La información no se altera de forma indebida

Disponibilidad

Los sistemas y datos están accesibles cuando se necesitan

Amenazas comunes

- **Phishing**: correos falsos que buscan robar contraseñas o datos bancarios.
- **Vishing**: Tipo de fraude en el que un atacante intenta engañar a una persona por teléfono para que revele información confidencial.
- **Smishing**: Tipo de fraude mediante mensajes de texto (SMS). El atacante envía mensajes que parecen legítimos para que la víctima haga clic en enlaces maliciosos o entregue información personal.
- **Ransomware**: bloquea tus archivos y pide un rescate.
- **Malware**: programas que dañan equipos o roban información.
- **Fuga de información**: pérdida de datos por errores humanos o accesos indebidos.
- **Suplantación de identidad**: hacerse pasar otra persona con intenciones fraudulentas. Ejemplo: por directivos o clientes (fraude del CEO).

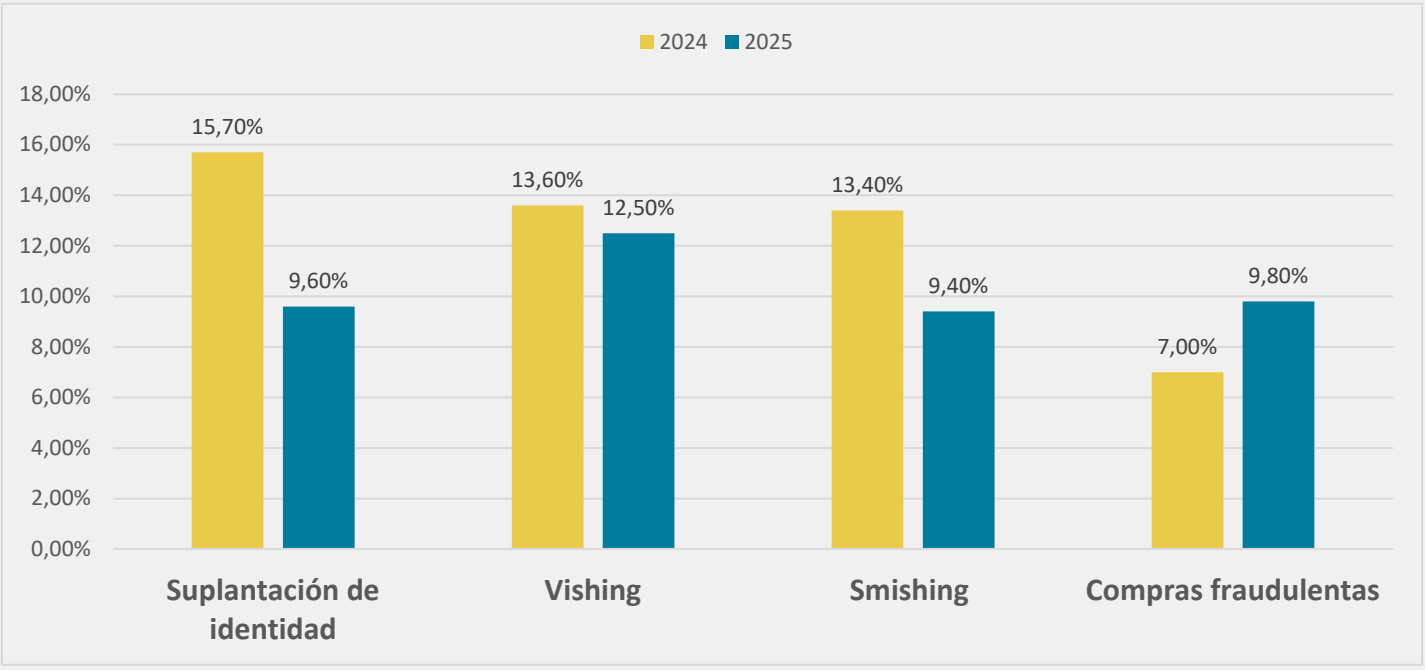
Diagnóstico de la situación actual

Según datos del INCIBE, en **2024** Asturias registró **81.947 dispositivos afectados por problemas de ciberseguridad**, concentrados principalmente en las ciudades de Oviedo, Gijón y Avilés. De ese total, el **8,49 %** correspondió a incidentes reportados por **empresas asturianas**.

En el primer semestre de **2025** ya se han contabilizado **31.252 dispositivos comprometidos,** lo que representa un 8,39 % de los incidentes registrados y atendidos en la región. Aunque la mayoría de los incidentes son notificados por ciudadanos, resulta evidente que las empresas continúan enfrentando un riesgo significativo de sufrir ciberataques.

En **2024**, en Asturias, los incidentes más consultados fueron: suplantación de identidad, vishing , smishing y compras fraudulentas.

En **2025** las temáticas o incidentes más consultados: vishing , compras fraudulentas, suplantación de identidad por robo y Smishing.



En cuanto a la tipología de ataques, podríamos centrarnos en dos categorías genéricas de ciberataques que engloban una gran parte de los problemas informáticos detectados:

- **Fraude de ingeniería social**: Se basa en manipular a la víctima para obtener información confidencial. Su característica principal es el aprovechamiento de la confianza del usuario, combinada con la creación de una falsa sensación de urgencia que induce a actuar bajo presión. Ejemplos de este fraude son:
  - Phishing / Suplantación de identidad (email o web)
  - Vishing (teléfono)
  - Smishing (SMS)
- **Fraude económico o transaccional:** Este tipo de fraude tiene como objetivo obtener dinero o bienes de forma ilícita. Se centra en la obtención de un beneficio financiero directo, generalmente mediante engaño o estafa online. El típico ejemplo de este tipo de fraude es:
  - Compras fraudulentas

Para la elaboración de esta guía también llevamos a cabo un estudio anónimo sobre la gestión de la ciberseguridad en el ámbito empresarial asturiano, a través de un formulario específico. Esto se hizo conjuntamente con la recolección y el análisis de estos datos estadísticos, y con el propósito de garantizar la máxima transparencia, fiabilidad y actualidad en los datos utilizados.

Los resultados de este análisis constituyen una base objetiva fundamental para orientar primeros pasos y estrategias dirigidas a fortalecer las capacidades de protección digital en el tejido empresarial regional.

En este estudio participaron un total de **21 PYMES socias del Club de Calidad**, cuyos indicadores de comportamiento se evaluaron en torno a aspectos clave como la inversión digital, la gestión con proveedores, la formación del personal, la realización de auditorías, la implicación de los órganos de administración, la existencia de responsables designados de ciberseguridad y el nivel de concienciación organizativa.

El diagnóstico revela varios hallazgos relevantes:. **Más del 85% de las empresas encuestadas declara estar familiarizada con la ciberseguridad y reconoce el riesgo digital,** pero la frecuencia con la que abordan estos asuntos varía: unas pocas lo hacen mensual o trimestralmente, mientras casi un tercio solo de forma esporádica. Esto refleja que, pese al interés creciente, la ciberseguridad aún no está plenamente integrada en la planificación estratégica.

En cuanto a la **formación interna, dos tercios de las empresas realizan campañas periódicas**, pero un grupo significativo no ofrece entrenamientos regulares, lo que deja al personal más expuesto a riesgos como phishing o fraude por ingeniería social. A ello se suma la **falta de auditorías**, muchas veces parciales o inexistentes, que limitan la detección de vulnerabilidades y la mejora continua.

La relación con proveedores también es crítica: cerca de **la mitad de las organizaciones no aplica controles suficientes**, pese a que gran parte de los incidentes se produce a través de la cadena de suministro digital. Además, la inversión en ciberseguridad sigue siendo baja o poco transparente, con grandes diferencias entre sectores y tamaños de empresa.

Aun así, **varias empresas reconocen haber sufrido incidentes en los últimos años, lo que ha generado mayor conciencia**. Sin embargo, la ausencia de políticas sistemáticas, responsables definidos y protocolos claros convierte estas debilidades en riesgos reales para la continuidad del negocio, la confianza de clientes y el cumplimiento legal.
En conclusión, la ciberseguridad no es un lujo para grandes corporaciones, sino una necesidad esencial para cualquier PYME.

Adoptar medidas preventivas, invertir en formación e implementar protocolos de respuesta es clave para ganar resiliencia, fortalecer la competitividad y garantizar la sostenibilidad en un mercado cada vez más digitalizado y regulado.

¿CÓMO UTILIZAR LA GUÍA?

Esta guía tiene como propósito aportar un marco inicial de actuación, mediante un conjunto de medidas que constituyen primeros pasos y estrategias, las cuales apoyarán a las PYMES asturianas a establecer las bases para el fortalecimiento progresivo de la seguridad de sus activos digitales.

Ahora bien, no todas las acciones de ciberseguridad implican el mismo nivel de esfuerzo. Por ello, distinguimos entre medidas de rápida aplicación y aquellas que requieren mayor planificación.

Esta guía distingue las medidas en dos categorías:

- **PRIMEROS PASOS:** acciones de bajo o nulo coste para la PYME, sencillas de implementar y que apenas requieren planificación previa, pero que ofrecen resultados muy efectivos.
- **ESTRATEGIAS:** medidas que demandan una planificación y coordinación por parte de la gerencia, y que en algunos casos pueden implicar una inversión adicional.

A continuación, se incluye un autodiagnóstico de ciberseguridad que permite identificar el nivel de madurez de cada empresa y avanzar paso a paso en la aplicación de medidas adaptadas. El autodiagnóstico, inspirado en marcos nacionales e internacionales, distingue tres niveles de madurez:

- **Básico**: medidas esenciales de higiene digital.
- **Intermedio**: gestión y organización de la seguridad.
- **Avanzado**: madurez y mejora continua.

¿Qué hacer después de realizar el autodiagnóstico?

Una vez realizado el diagnóstico y, según la puntuación obtenida, la empresa se situará en un nivel específico:

- **Si la empresa se encuentra en el Nivel Básico**, puede empezar de inmediato con el kit de primeros pasos: son medidas rápidas y efectivas que le permitirán construir la base de su seguridad digital.
- **Si la empresa ha alcanzado el Nivel Intermedio o Avanzado**, el siguiente paso será aplicar las estrategias recomendadas. Estas son acciones más estructuradas y de mayor alcance, diseñadas para consolidar el nivel de madurez alcanzado y preparar a la organización frente a amenazas más complejas. En esta guía se presenta un conjunto de estrategias específicas para cada nivel. Se recomienda implementar tantas medidas como sea posible, adaptándolas siempre a la realidad y recursos de la empresa.

Al final de esta guía encontrarás una selección de recursos y enlaces de interés para fortalecer la cultura de ciberseguridad. Asimismo, se incluyen anexos con material adicional que amplía y refuerza las recomendaciones presentadas en el contenido central.

Recomendación general

No importa en qué punto comience, lo esencial es avanzar con constancia. Cada medida implementada representa un paso hacia una PYME más segura, resiliente y competitiva.

AUTODIAGNÓSTICO DE CIBERSEGURIDAD para PYMES

Instrucciones

- ◊ Marca con una "X" cada medida que tu empresa ya cumpla.
- ◊ Suma los puntos obtenidos en cada bloque (cada casilla = 1 punto).
- ◊ Identifica tu nivel de madurez según los resultados:

NIVEL BÁSICO

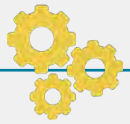
- ☐ Hay un antivirus actualizado en todos los dispositivos.
- ☐ Las actualizaciones automáticas están activadas en ordenadores y móviles.
- ☐ Se realizan copias de seguridad al menos una vez por semana.
- ☐ Las contraseñas cumplen criterios de robustez y/o utilizan gestores de contraseñas.
- ☐ Se usa autenticación multifactor (MFA) en correos y servicios críticos.

Resultados del bloque (5 puntos posibles)

0–4 puntos: En riesgo
Tu empresa aún no cuenta con todas las medidas esenciales de protección. Es prioritario implementar las que faltan para reducir vulnerabilidades básicas.

5 puntos: Nivel Básico completo
Ya has cubierto las medidas mínimas de higiene digital. Puedes avanzar hacia el Nivel Intermedio para consolidar tu gestión de seguridad.

NIVEL INTERMEDIO



- ☐ Existe un responsable designado de Seguridad.
- ☐ Existe una política escrita sobre uso de sistemas y datos.
- ☐ El personal recibe formación en seguridad al menos 1 vez al año.
- ☐ Se revisa la seguridad de nuestros proveedores.
- ☐ Se hacen revisiones/auditorías al menos una vez cada dos años.

Resultados del bloque (5 puntos posibles)

0–2 puntos: Gestión insuficiente
Faltan medidas organizativas clave (responsable, políticas, formación). Debes reforzar la estructura interna de seguridad.

3–4 puntos: En progreso
Tu empresa ya aplica buenas prácticas de gestión, pero es necesario completar las que faltan para tener un sistema consistente.

5 puntos: Nivel Intermedio completo
Has consolidado las medidas organizativas. Estás preparado para avanzar al Nivel Avanzado, centrado en marcos reconocidos y mejora continua.

NIVEL AVANZADO

- ☐ Se sigue un marco reconocido (ISO 27001, ENS, NIST, etc.).
- ☐ Se realizan simulacros de incidentes (phishing, recuperación de back ups).
- ☐ Existe un plan formal de respuesta a incidentes.
- ☐ Se cuenta con mecanismos de monitorización y mejora continua de seguridad.
- ☐ Se utilizan métricas e indicadores clave (KPIs) para medir la eficacia de la seguridad y orientar la toma de decisiones.

Resultados del bloque (5 puntos posibles)

0–4 puntos: Madurez parcial.
Ya has dado pasos hacia la madurez, pero aún faltan controles avanzados como simulacros, métricas o auditorías externas. Revisa y completa estos aspectos para alcanzar la excelencia en ciberseguridad.

5 puntos: Nivel Avanzado completo.
Tu empresa cuenta con un sistema de seguridad robusto y alineado con buenas prácticas internacionales. El siguiente reto es mantener el ciclo de mejora continua y anticiparte a nuevas amenazas.

RESULTADOS ESCALA GLOBAL DE MADUREZ EN CIBERSEGURIDAD

Suma de todos los puntos obtenidos en los tres bloques. (Máximo 15 puntos). El resultado del autodiagnóstico te permitirá conocer el estado real de tu empresa, reforzar áreas débiles, optimizar recursos y anticiparte a posibles riesgos.

Básico (0–5 puntos)
Aplica el kit de primeros pasos, con acciones simples y de bajo coste que cubren los riesgos esenciales.

Intermedio (6–10 puntos)
Implementa las estrategias de gestión y organización para consolidar la seguridad interna.

Avanzado (11–15 puntos)
Aplica las estrategias avanzadas, centradas en marcos reconocidos, auditorías y mejora continua.

0–5 puntos
Nivel Básico

Tu empresa está en una fase inicial. Aún faltan varias medidas esenciales de higiene digital, lo que aumenta el riesgo de incidentes de seguridad.

Qué hacer: empieza de inmediato por el kit de primeros pasos (antivirus, copias de seguridad, contraseñas robustas, MFA). Esto te dará una base sólida para seguir avanzando.

6–10 puntos
Nivel Intermedio

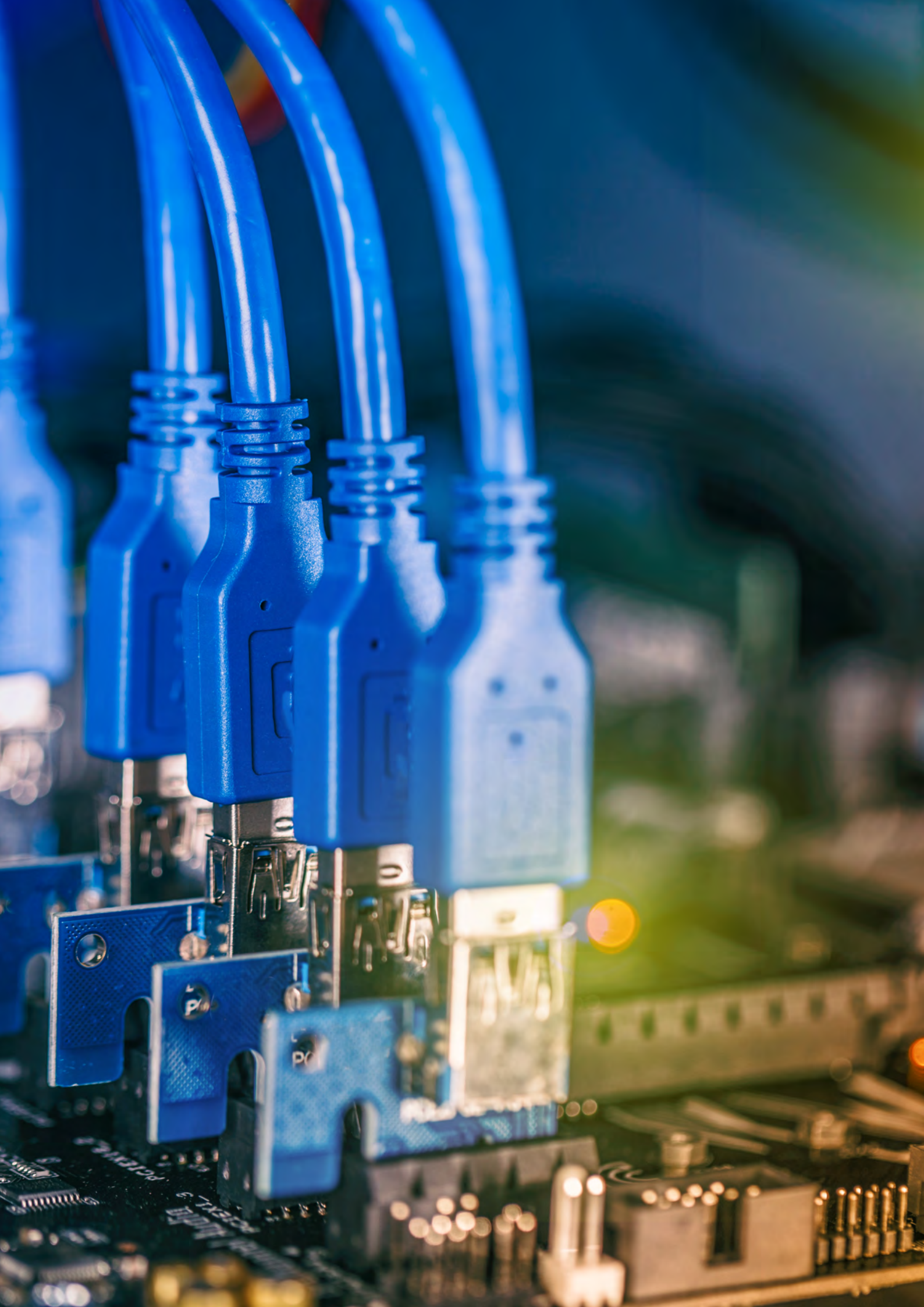
Tu empresa ya cuenta con algunas medidas técnicas y organizativas, pero todavía hay puntos débiles que podrían comprometer la seguridad.

Qué hacer: consolida la gestión interna (designar responsable, políticas escritas, formación periódica, auditorías). Una vez completadas, podrás dar el salto al nivel avanzado.

11–15 puntos
Nivel Avanzado

Tu empresa ha integrado marcos reconocidos de gestión de seguridad (ISO 27001, ENS, NIST, etc.) y aplica prácticas de mejora continua.

Qué hacer: mantén este nivel con métricas, auditorías externas y simulacros periódicos. Refuerza la cultura de seguridad en toda la organización y actualiza procesos frente a nuevas amenazas.



Félix Barrio

Director General de INCIBE

Si me definiera la Inteligencia Artificial diria que:

Soy un servidor público convencido de que la tecnología debe estar al servicio de las personas. Al frente de INCIBE trabajo cada día para que la experiencia digital sea más humana, cercana y segura.

Mi misión es ayudar a que la ciudadanía, las empresas y las instituciones puedan aprovechar todo lo que ofrece la tecnología sin miedo y con confianza, poniendo siempre a las personas en el centro.

AL VUELO

¿En qué gastarías 100 euros en ciberseguridad?
En un servicio de Internet con buena protección, no en el más barato.

¿Qué es lo último que aprendiste?
La urgencia de diseñar sistemas de cifrado resistentes a la criptografía cuántica.

¿La consulta más sorprendente que llegó a INCIBE?
Una estafa con falsos mensajeros que recogían móviles que nunca se habían pedido.

En casa del INCIBE, ¿cuchillo de palo?
Tenemos los mismos problemas que cualquiera; hacemos simulacros de ciberataques.

En tu familia, todos saben que...
Hay que cuidar lo que se publica en redes: detrás siempre hay alguien mirando.

¿Qué superpoder ciber pedirías?
Poder aprender y procesar innovación sin límite, como una IA.

¿Cómo será el empleado de ciberseguridad del futuro?
Un perfil imprescindible en cualquier empresa, como el abogado o el contable.

El INCIBE gestiona incidentes de ciberseguridad en empresas y ciudadanos. ¿Qué radiografía hace de la situación actual en España?

España cuenta con más de 40 millones de usuarios de dispositivos digitales activos, lo que nos coloca en un nivel de exposición muy elevado. En el último año hemos gestionado casi 97.300 incidentes de ciberseguridad. El fraude en línea, sobre todo a través del phishing —correos electrónicos o páginas falsas que suplantan a bancos y empresas para robar datos—, representa ya el 43% de los casos. Otro bloque relevante son los 42.000 incidentes de malware, especialmente ransomware, que secuestra datos en ordenadores o móviles y exige un rescate económico. Y en el ámbito de menores, que nos preocupa especialmente, el 90% de las llamadas que hemos recibido estaban vinculadas con acoso o abuso sexual en Internet.

¿Qué papel juega la concienciación ciudadana? ¿Estamos bien informados?

Diría que en España tenemos un nivel de sensibilización medio-alto. Sin embargo, eso no basta para estar a salvo, porque las técnicas de ataque evolucionan a gran velocidad. Un dato revelador: cuatro de cada diez españoles no tienen instalado un antivirus en su móvil, aunque exista la opción gratuita en nuestra web. Muchos alegan que ralentiza el dispositivo o que no lo consideran necesario. La concienciación debe traducirse en hábitos responsables, desde no abrir mensajes sospechosos hasta evitar difundir bulos o instalar aplicaciones inseguras.

> ***"La ciberseguridad es una responsabilidad de todos: sector público, privado y ciudadanía.***

¿Qué recursos ofrece INCIBE a la ciudadanía?

Nuestro servicio más conocido es el teléfono gratuito 017, operativo de 8 de la mañana a 11 de la noche. Se puede llamar también por WhatsApp o Telegram. Contamos con psicólogos especializados en atender a menores, porque hay casos de niños de 8 o 9 años que prefieren pedir ayuda directamente. Además, elaboramos guías prácticas, materiales didácticos y campañas de concienciación que llevamos a colegios, ferias y municipios de toda España. Queremos que ningún ciudadano se quede atrás por falta de recursos.

¿Y en el caso de las empresas?

El reto es mayor, porque de su nivel de ciberseguridad depende la competitividad y, en algunos casos, servicios críticos. Desde INCIBE promovemos programas de apoyo a PYMEs y autónomos: les guiamos en la identificación de riesgos, fomentamos que inviertan en soluciones profesionales y facilitamos el acceso a programas de ayudas como el kit digital, que financia al 100% la implantación de medidas básicas de protección. También organizamos jornadas con asociaciones empresariales, Policía Nacional y Guardia Civil para explicar cómo prevenir ciberdelitos.

Ha mencionado la inversión en innovación. ¿Qué importancia tiene para INCIBE?

Es clave. En los últimos tres años hemos invertido más de 320 millones de euros en proyectos de innovación, apoyando a 150 empresas españolas para desarrollar soluciones de ciberseguridad "made in Spain". Queremos soberanía tecnológica, no depender solo de proveedores extranjeros. A esto se suman 80 millones destinados a impulsar el emprendimiento, con 32 incubadoras y aceleradoras repartidas por todo el país. La idea es que cada provincia cuente con empresas de proximidad capaces de dar soporte a colegios, ayuntamientos o centros de salud.

Uno de los ámbitos más sensibles es la protección de menores. ¿Qué medidas han puesto en marcha?

España cuenta con un programa específico dentro de la Unión Europea. Llevamos casi dos décadas trabajando en alfabetización digital y protección de la infancia. Disponemos de un centro de seguridad en Internet para niños, niñas y adolescentes, con materiales dirigidos a educadores y familias. Además, más de mil cibervoluntarios acreditados por INCIBE imparten talleres en colegios de todo el país. Gestionamos también el centro de denuncia de contenidos de abuso infantil en la red, en coordinación con Interpol y la Fiscalía de delitos telemáticos. Y trabajamos en proyectos de investigación para anticipar nuevas amenazas: por ejemplo, el uso indebido de Inteligencia Artificial en la generación de contenidos falsos.

> ***El eslabón más débil en ciberseguridad son las personas.***

La Inteligencia Artificial y el Internet de las Cosas están transformando la ciberseguridad. ¿Qué riesgos nos esperan en el futuro inmediato?

Vivimos una paradoja: cuanto más accesible es la tecnología, más difícil resulta garantizar que sea segura. Hoy nuestros hogares tienen decenas de dispositivos conectados —televisores, consolas, altavoces, pulseras deportivas, incluso neveras—, y cada uno de ellos puede ser una puerta de entrada para un ciberdelincuente. Lo mismo ocurre con la Inteligencia Artificial: se ha democratizado su uso, pero eso multiplica los riesgos. Desde INCIBE estamos monitorizando dispositivos médicos, juguetes conectados o apps basadas en IA para asegurarnos de que cumplen unos mínimos requisitos de seguridad. El objetivo es que la innovación avance sin poner en peligro al usuario, pero hay que tener en cuenta que el eslabón más débil en ciberseguridad son las personas.

España aparece en los primeros puestos internacionales en ciberseguridad. ¿Qué nos ha llevado hasta ahí?

Principalmente, la apuesta decidida del país. Estamos en el top 4 mundial según Naciones Unidas, junto a Estados Unidos o Estonia. Esto se debe a una inversión sostenida y a la coordinación entre organismos: INCIBE para ciudadanía y empresas, el CNI en la administración pública, y el Mando Conjunto del Ciberespacio en defensa. Pero sobre todo a que entendemos la ciberseguridad como un asunto de país, que debe llegar hasta el último eslabón: desde una gran empresa energética hasta un pequeño ayuntamiento rural.

¿Está bien dimensionado INCIBE para afrontar todos estos retos?

Siempre se puede crecer, pero lo esencial no es tanto el tamaño de la agencia como la capacidad de coinversión. La ciberseguridad no depende solo de INCIBE, sino de un esfuerzo compartido entre sector público, privado y ciudadanía. Podemos tener los mejores expertos, pero si una familia no protege su red doméstica, o un colegio no actualiza sus equipos, la cadena se rompe. Por eso insistimos tanto en que la seguridad digital es responsabilidad de todos.

> ***La concienciación debe traducirse en hábitos responsables, desde no abrir mensajes sospechosos hasta evitar difundir bulos.***

NIVEL BÁSICO

NIVEL BÁSICO

Si la empresa se encuentra en este nivel, significa que acaba de comenzar su camino hacia la protección de los activos de la información y, por tanto, es necesario que se implementen medidas de seguridad informática con la mayor brevedad posible. Con medidas básicas de seguridad, herramientas adecuadas y algo de formación, cualquier organización puede protegerse mejor y reaccionar rápido si algo falla.

La ciberseguridad puede parecer un mundo complejo, especialmente si la PYME no cuenta con un equipo técnico dedicado. Pero proteger la empresa no tiene por qué ser complicado ni costoso. Dado que no siempre está claro por dónde iniciar la ciberseguridad en una organización, a continuación, se presenta una lista de primeros pasos que pueden implementarse de inmediato para proteger el negocio.

CONTENIDOS
NIVEL BÁSICO

1. Instalar y mantener antivirus actualizado en todos los dispositivos

PARA WINDOWS

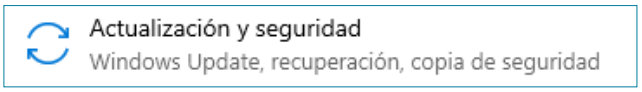
En Windows 10 ya viene un antivirus integrado: **Microsoft Defender Antivirus** (antes Windows Defender). No es necesario descargar nada extra para tener protección básica, pero sí conviene asegurarse de que esté activado, actualizado y bien configurado.

Si ya hay otro antivirus instalado, Microsoft Defender se desactiva automáticamente para evitar conflictos. Esto no significa que el equipo esté desprotegido: el antivirus actual sigue cuidando del equipo.

Si hay activo un antivirus distinto a Microsoft Defender, al ir a **Seguridad de Windows > Protección contra virus y amenazas**, se verá el siguiente mensaje indicando que Defender está desactivado porque otro antivirus se está ejecutando.

Si por el contrario no hay otro antivirus instalado, se debe activar Microsoft Defender:

1. Entrar a Configuración y hacer click en la pestaña opción "**Actualización y Seguridad**"



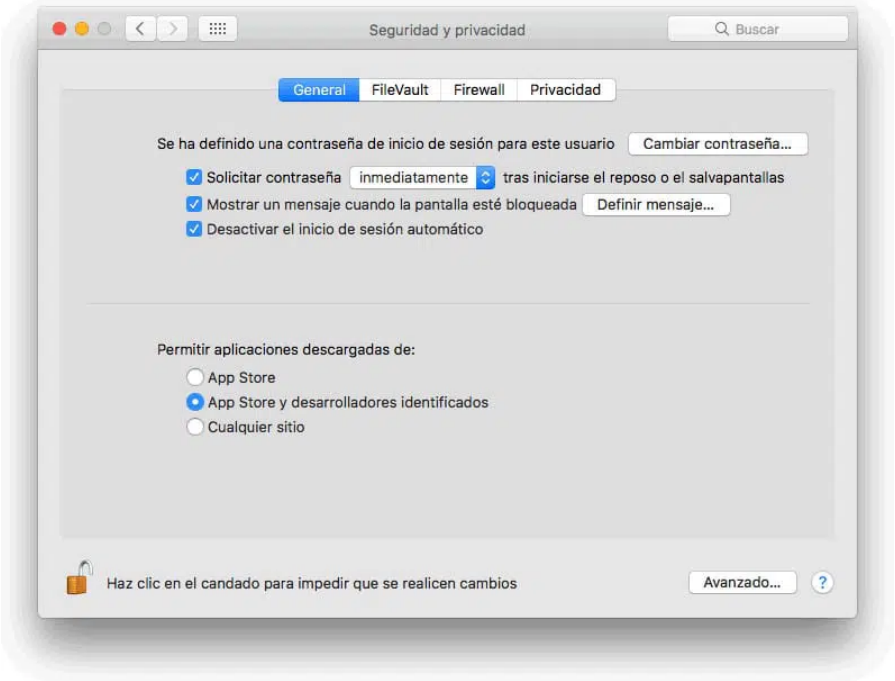
2. A continuación, se verá una nueva ventana donde deberemos seleccionar la opción '**Seguridad de Windows**' en el menú que aparece a la izquierda.

PARA MAC

En el caso de macOS, la clave está en actualizar el sistema operativo siempre que haya una actualización disponible, sin embargo, también existe una herramienta nativa llamada Gatekeeper que protege el equipo frente a software malicioso o no autorizado. Su misión es controlar qué aplicaciones pueden instalarse y ejecutarse en el Mac, bloqueando aquellas que provienen de fuentes desconocidas o que no han sido verificadas por Apple.

Para asegurarte de que Gatekeeper está protegiendo el equipo de forma eficaz:

1. Ir a Configuración del sistema > “Privacidad y seguridad”
2. Buscar la sección > “Permitir apps descargadas de”.
3. Seleccionar la opción App Store o App Store y desarrolladores identificados.



2. Activar actualizaciones automáticas en ordenadores y software crítico

PARA WINDOWS

Las **actualizaciones automáticas** son claves para mantener los equipos protegidos y con un funcionamiento adecuado. Incluyen parches de seguridad, correcciones de errores, mejoras de rendimiento y nuevas funciones que previenen vulnerabilidades y aseguran la estabilidad del sistema. Mantener el sistema operativo actualizado reduce riesgos de ataques y problemas de compatibilidad con programas o dispositivos.
En la mayoría de las versiones recientes de Windows, las actualizaciones automáticas ya vienen activadas. Esto permite que el sistema descargue e instale parches importantes sin que tengamos que intervenir.

Aun así, se puede verificar o ajustar la configuración siguiendo los siguientes pasos:

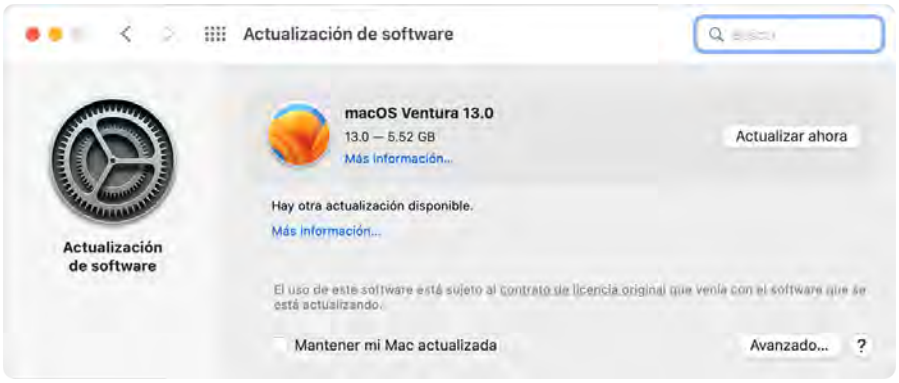
Hacer click en Configuración >Actualización y seguridad > Windows Update, y asegurarse de que la opción “Obtén las últimas actualizaciones en cuanto estén disponible” esté habilitada. Desde aquí también se puede pausar actualizaciones, revisar el historial de parches instalados y programar reinicios para no interrumpir el trabajo.

PARA MAC

Si se usa macOS también es posible actualizar el sistema y asegurarse de que este lo haga de forma automática.

1. Acceder a Configuración del Sistema > General > Actualización de software
2. A continuación, hacer click en la opción > Mantener mi Mac actualizada.

NOTA: Apple lanza parches frecuentes para protegerte frente a malware y vulnerabilidades.



3. Configurar copias de seguridad periódicas

Las copias de seguridad externas son fundamentales para proteger la información frente a fallos de hardware, malware o ransomware. Permiten restaurar archivos eliminados o cifrados, acceder rápidamente a los datos desde otro dispositivo y, en entornos empresariales, cumplir con normativas y auditorías. Aunque plataformas como Google Workspace y Microsoft 365 ofrecen alta disponibilidad y redundancia de datos, **no reemplazan copias externas bajo control de la empresa.** Por ello, se recomienda mantener copias adicionales fuera del servicio principal, ya sea en otra nube o en almacenamiento físico, garantizando así la disponibilidad de los datos, la protección frente a borrados accidentales o ataques de ransomware, y la continuidad operativa en caso de incidencias.

> ***"El cibercrimen evoluciona; tus sistemas también deben hacerlo.***

Recomendaciones según el entorno de trabajo

- **Para empresas que utilizan discos duros de almacenamiento local:** Es recomendable almacenar copias de seguridad en dispositivos externos, como discos duros portátiles o sistemas NAS(*). Esto permite restaurar la información rápidamente ante cualquier incidencia en el sistema principal.
- **Para empresas que utilizan servicios de almacenamiento en la nube:** Es recomendable realizar copias de seguridad adicionales fuera del servicio de nube principal. Esto garantiza la disponibilidad de los datos y asegura la continuidad operativa ante fallos del servicio o incidencias externas.
- **Para empresas que cuentan con servidores propios (on-premise):** Es recomendable diseñar un plan de copias de seguridad periódicas que incluya réplicas en servidores secundarios o en la nube. De este modo se protege la información crítica y se asegura la continuidad del negocio incluso ante fallos físicos o ciberataques en la infraestructura principal.

SIGUE LA REGLA 3-2-1

La estrategia recomendada es la siguiente:

3
Tres copias de los datos

2
Al menos dos soportes distintos

1
Una copia fuera de las instalaciones (nube o disco externo)

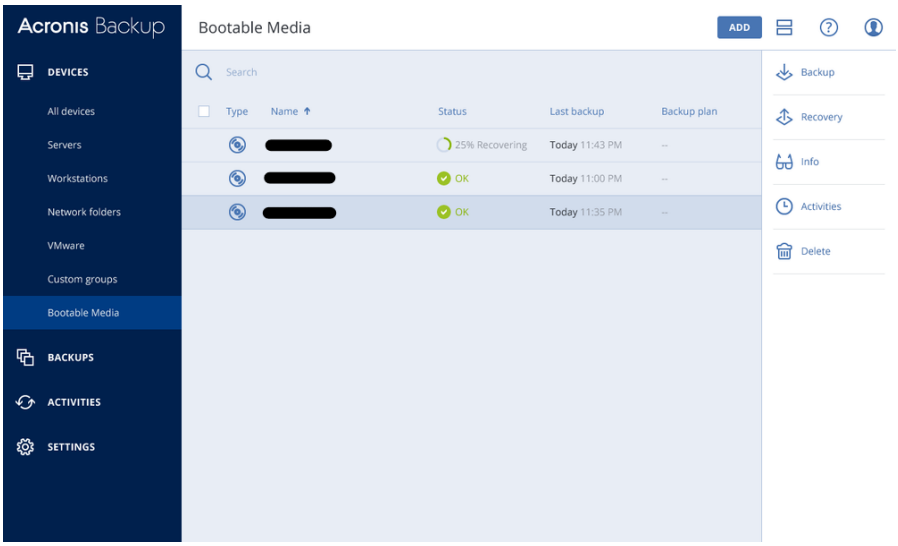
(*) NAS. Por sus siglas en inglés "Network Attached Storage": almacenamiento conectado a la red

Herramienta recomendada

Una opción asequible a nivel económico y ampliamente utilizada por PYMES es **Acronis Cyber Backup**, que permite gestionar copias tanto en local como en la nube. Es fácil de configurar y confiable, ideal para empresas que dependen de sus datos para operar con seguridad y tranquilidad.

Para la implementación de este software se deberá proceder de la siguiente forma:

1. Descargar el programa desde la web oficial de Acronis. (Acronis Cyber Backup 12.5 - Download – Acronis SCS)
2. Instalar primero el servidor principal (donde se controlará todo).
3. Activar la protección en los equipos instalando una aplicación auxiliar en cada máquina.
4. Activar la licencia personal con la cuenta de Acronis pertinente.
5. Elegir dónde guardar las copias: disco externo, un NAS en la oficina o la nube de Acronis.
6. Programar los respaldos (diarios, semanales, etc.).
7. Hacer una prueba: respaldar y restaurar un archivo para comprobar que todo funciona.



Revisar las copias de seguridad al menos una vez al mes para asegurar que funcionan.

No basta con solo configurar backups automáticos: es importante asegurarse de que realmente se están haciendo y que se pueden recuperar los archivos si algo falla. A modo de prueba se puede elegir un documento importante, hacer una restauración de prueba y comprobar que está completo y accesible.

Cada mes, es recomendable revisar los registros del sistema de copias, comprobar el espacio disponible y documentar cualquier fallo. Esta acción genera la garantía de, en casi de incidente, se podrá recuperar el acceso a la información.

4. Usar contraseñas seguras y centralizarlas en un gestor

Las contraseñas son la primera barrera de protección frente a accesos no autorizados a nuestros dispositivos y cuentas. Por ello, resulta esencial crear contraseñas seguras y difíciles de adivinar para mantener a salvo nuestra información.

A continuación, damos varias recomendaciones del INCIBE para generar contraseñas robustas, únicas y fáciles de recordar.

NOTA
Cada cuenta debe tener su contraseña única. Conviene cambiarlas cada 3-6 meses o si se sospecha que han sido comprometidas.

Centralizar contraseñas con un gestor de contraseñas

Es fundamental que las contraseñas sean fuertes, únicas y distintas para cada servicio. También deben guardarse en un entorno seguro.

Una forma fácil de lograrlo es usar un **gestor de contraseñas, como Bitwarden**, un software gratuito (aunque tiene una versión de pago), que es confiable y muy funcional.

Recomendaciones de seguridad

CONTRASEÑAS SEGURAS
Crear contraseñas de al menos 12 caracteres con complejidad suficiente

NO REUTILIZAR
No reutilizar credenciales entre servicios distintos

ALMACENAMIENTO SEGURO
Almacenar las contraseñas en una herramienta segura y cifrada

NOTIFICACIONES
Activar notificaciones ante posibles brechas o accesos no autorizados

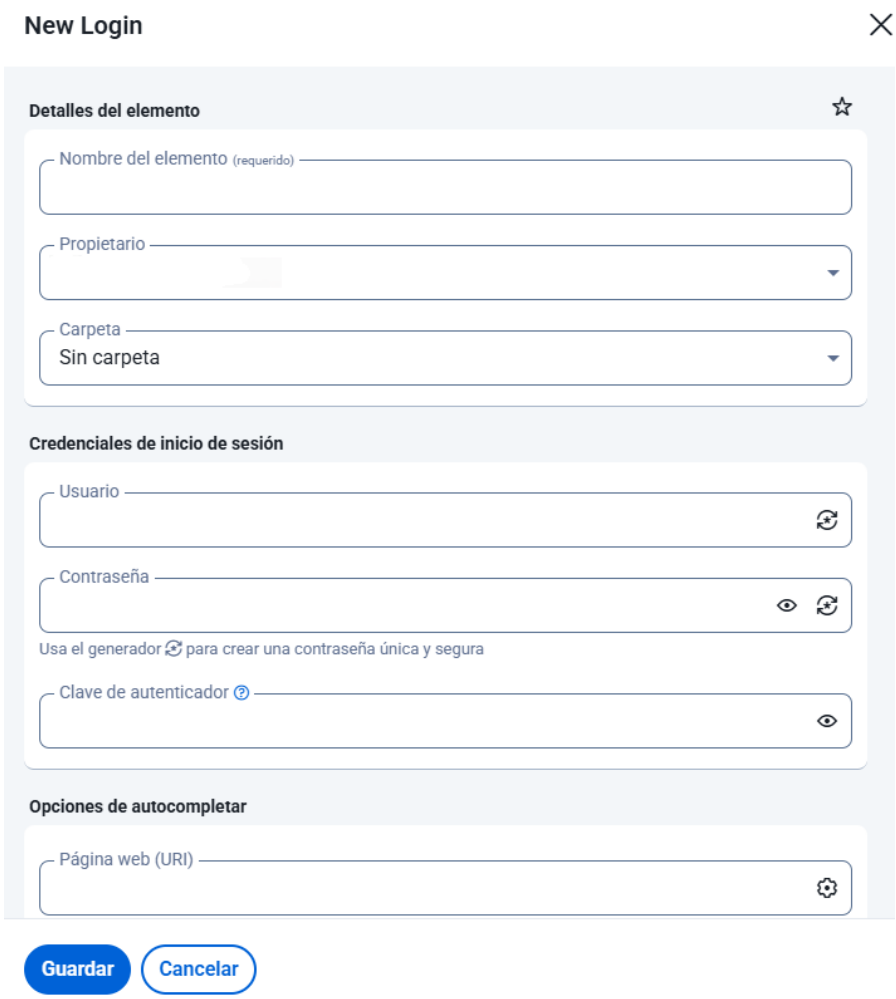
Bitwarden

Con Bitwarden se pueden asociar credenciales a cada página web y generar automáticamente usuarios y contraseñas seguras. Así se evita reutilizar claves, se refuerza la seguridad de las cuentas y se mantiene toda la información protegida en un **almacenamiento cifrado**.

Los pasos para instalar esta herramienta serían los siguientes:

1. Ir la página oficial: https://bitwarden.com/download.
2. Descargar la versión de escritorio para el sistema operativo que se tenga.
3. Ejecutar el instalador y seguir las instrucciones
4. Abrir la aplicación una vez instalada.
5. Crear una cuenta con el correo que corresponda y una contraseña maestra robusta.
6. Iniciar sesión y empezar a guardar las contraseñas.

Bitwarden puede usarse gratis con todas las funciones esenciales, y también ofrece una versión de pago con extras como adjuntos cifrados y autenticación avanzada.



> ***Reutilizar contraseñas es abrir muchas puertas con la misma llave.***

5. Activar autenticación de doble factor (2FA) en correos y servicios críticos

La autenticación de doble factor (conocida como "2FA") es una de las formas más eficaces de proteger las cuentas, sobre todo correo, banca en línea o plataformas profesionales. Añade una capa extra de seguridad, evitando que alguien acceda, aunque tenga la contraseña.

Una herramienta práctica para implementarla es **Google Authenticator, que genera códigos temporales de un solo uso (TOTP)** en el móvil. Solo se necesita vincular las cuentas que se quiera proteger con un código QR, y a partir de ahí siempre se tendrá un código dinámico que refuerza la seguridad frente a accesos no autorizados.

Cómo activarla

Para activar la autenticación en dos pasos (2FA) se deberá:

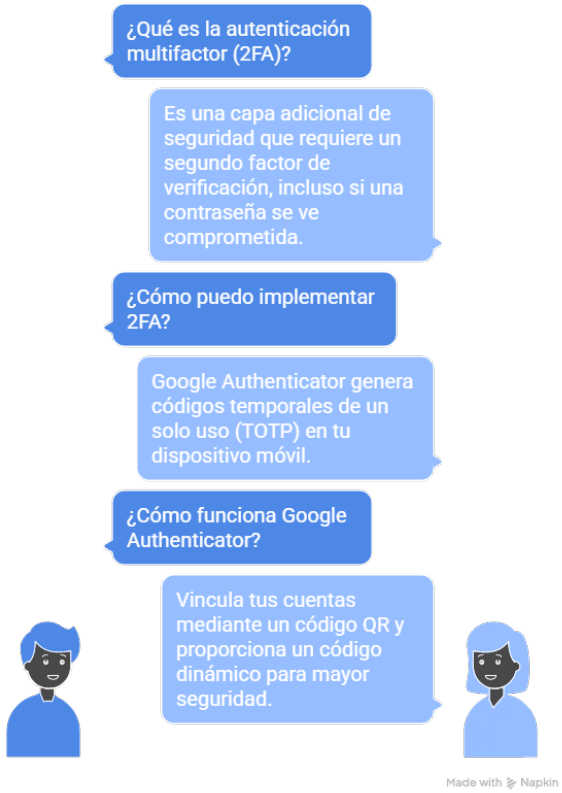
1. **Descargar la aplicación de autenticación** de preferencia (ejemplo: Google Authenticator), en la tienda de aplicaciones del dispositivo.
2. Acceder a la sección de "**Configuración/ Ajustes**" de la aplicación del sistema para la que se desee establecer el doble factor de autenticación.
3. Una vez ahí, seleccionar la opción que habilite la **verificación en dos pasos.**
4. A continuación, se deberá vincular la cuenta mediante **código QR** (opción más rápida) o introduciendo el código manualmente.

A partir de ahí, cada vez que se inicie sesión, además de usuario y contraseña, se deberá introducir el **código temporal** que genera la app. Los códigos se generan de forma periódica cada pocos segundos, garantizando que sean únicos y aumentando la protección frente a accesos no autorizados.

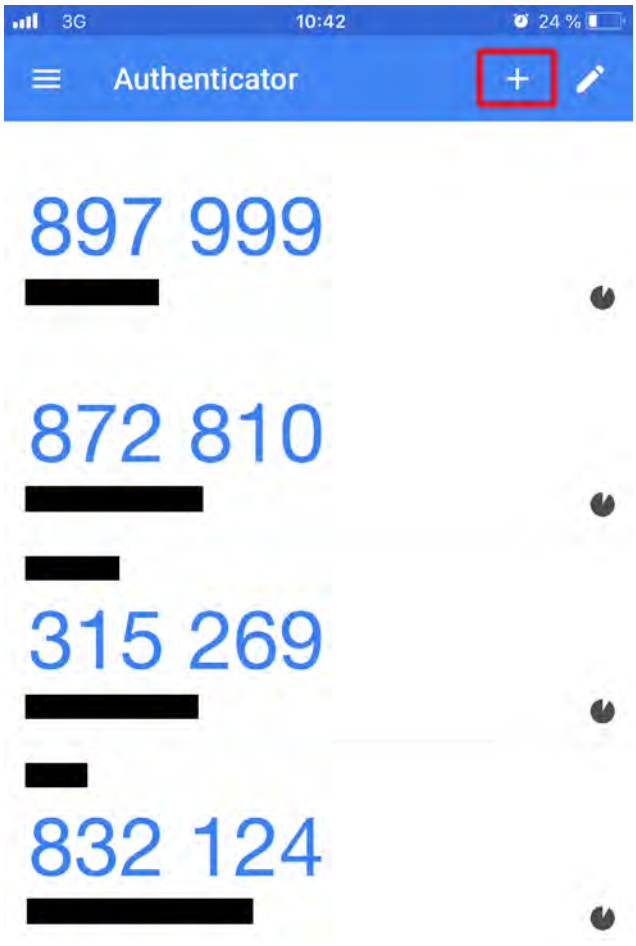
En la captura se ven varios códigos vinculados a cuentas (ocultas en negro) que cambian constantemente. Cada vez que se inicie sesión, será necesario introducir el código, protegiendo así el acceso a información confidencial y servicios sensibles de la empresa.

Así mismo, en el recuadro rojo se muestra cómo añadir una nueva cuenta, vinculándola a la sesión de un sitio específico.

Autenticación Multifactor (2FA) y Google Authenticator



En el recuadro rojo de la imagen inferior, se muestra cómo añadir una nueva cuenta, vinculándola a la sesión de un sitio específico.



6. Aplicar medidas de cortafuegos (firewall)

El cortafuegos es una herramienta fundamental para controlar el tráfico de red y proteger nuestros dispositivos frente a accesos no autorizados o posibles ciberataques. Su función principal es actuar como una "muralla" que filtra y bloquea conexiones sospechosas o no deseadas.

Configurar y mantener activo un firewall, ya sea en el sistema operativo, en el router o mediante soluciones de seguridad adicionales, ayuda a reforzar la protección de nuestra información personal y profesional.

PARA WINDOWS

En Windows ya viene integrado el Firewall de Windows Defender, que protege el equipo filtrando el tráfico de entrada y salida, y bloqueando accesos no autorizados. No es necesario instalar nada adicional, pero sí conviene asegurarse de que esté activado y correctamente configurado. Para comprobar que el firewall está activo, sigue estos pasos:

1. Entrar en Configuración desde el menú Inicio.
2. Hacer clic en la opción Actualización y seguridad.
3. Seleccionar en el menú lateral la pestaña Seguridad de Windows.
4. Entrar en Firewall y protección de red.
5. Verificar que los tres perfiles de red (dominio, privado y público) estén habilitados.

Más información: Firewall y protección de red en la aplicación Seguridad de Windows - Soporte técnico de Microsoft

PARA MAC

En el caso de macOS, también existe un **firewall nativo** que actúa como barrera frente a conexiones externas, permitiendo establecer reglas de acceso y personalizar la seguridad de la red.

Para comprobar que el firewall está activado en macOS:

1. Ir a Preferencias del Sistema desde el menú Apple.
2. Seleccionar la opción Seguridad y privacidad.
3. Hacer clic en la pestaña Firewall.
4. Comprobar que aparezca como "Activado".
5. En caso contrario, pulsar Activar firewall.
6. Opcional: hacer clic en Opciones de firewall para personalizar las conexiones permitidas.

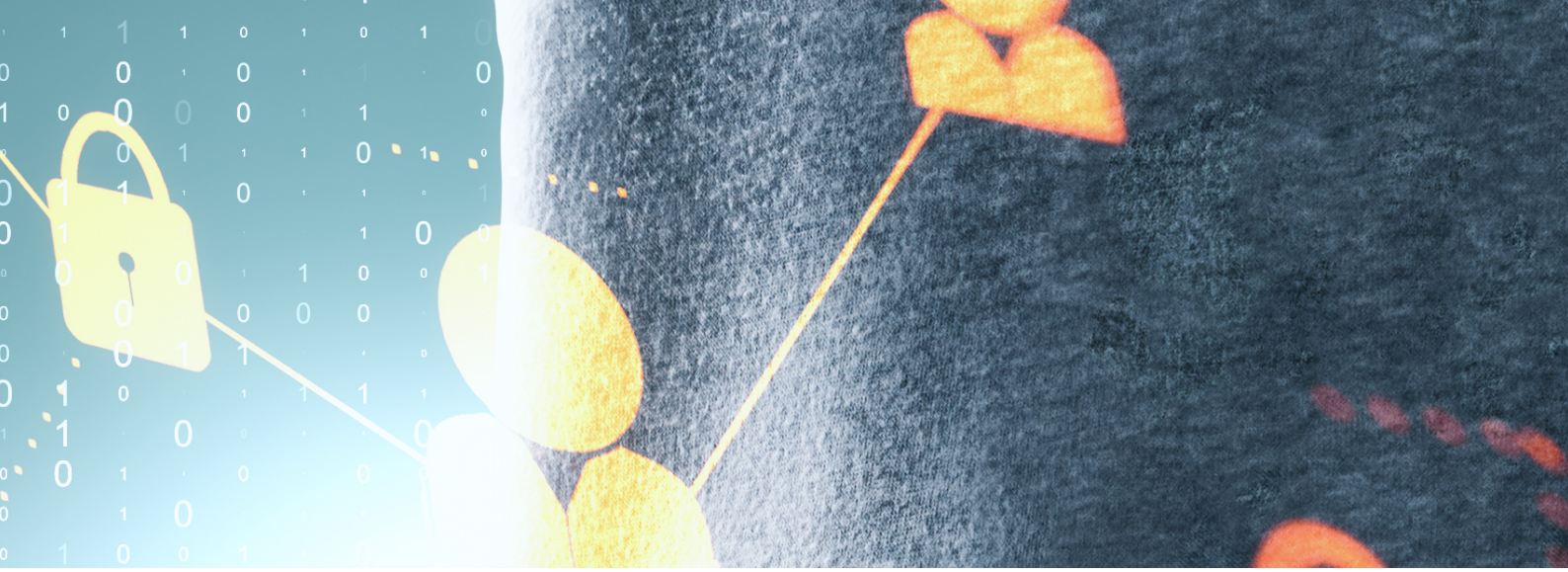
Más información: Bloquea las conexiones hacia tu Mac con un firewall - Soporte técnico de Apple

RECOMENDACIONES

Recomendaciones —basadas en una interpretación práctica de la información del INCIBE— para sacar el máximo provecho al uso del cortafuegos:

- **Mantén el firewall siempre activado en tus dispositivos y redes.**
- **Configura reglas específicas para limitar accesos innecesarios.**
- **Revisa periódicamente los registros de actividad del cortafuegos.**
- **Combínalo con otras medidas de seguridad como antivirus y actualizaciones frecuentes.**

NOTA: El cortafuegos no sustituye al antivirus, pero ambos se complementan para ofrecer una mayor protección frente a amenazas externas.



7. Crear un checklist de seguridad mínimo para comprobar que todos los equipos cumplen con las siguientes medidas de seguridad

A continuación, se facilita uno:

Dispositivos y Software

- ☐ Antivirus instalado y actualizado.
- ☐ Actualizaciones automáticas activadas (sistema operativo y software crítico).
- ☐ Última actualización del sistema realizada en los últimos 7 días.
- ☐ Cortafuegos activado (si aplica).
- ☐ Aplicaciones innecesarias desinstaladas.

Contraseñas y Autenticación

- ☐ Todas las cuentas tienen contraseñas únicas.
- ☐ Las contraseñas cumplen con los requisitos de robustez anteriormente expuestos.
- ☐ Se ha cambiado la contraseña en los últimos 3–6 meses.
- ☐ Autenticación multifactor (2FA) activada en correo, banca online y servicios clave.
- ☐ Gestor de contraseñas implementado y en uso.

Copias de Seguridad

- ☐ Copias de seguridad configuradas (diarias o semanales).
- ☐ Al menos una copia reciente disponible en la nube.
- ☐ Se ha verificado la restauración de archivos en el último mes.
- ☐ Las copias están cifradas y protegidas contra accesos no autorizados.

CONSEJOS BÁSICOS PARA DISPOSITIVOS MÓVILES

Las medidas de ciberseguridad no se limitan únicamente a los dispositivos del puesto de trabajo. Los ciberataques también pueden afectar a dispositivos móviles como teléfonos y tabletas, poniendo en riesgo tanto nuestra información personal como la de la empresa.

Por ello, es fundamental adoptar un enfoque específico para estos dispositivos, aplicando buenas prácticas que protejan los datos y mantengan la seguridad en todo momento. A continuación, compartimos varias medidas de seguridad para tener en cuenta, independientemente de si el dispositivo móvil es personal o corporativo.

Mantener el sistema y las aplicaciones actualizadas

- Instalar las actualizaciones tan pronto como estén disponibles.
- Las actualizaciones corrigen vulnerabilidades que podrían ser explotadas por atacantes.

Activar bloqueo y cifrado del dispositivo

- Utilizar PIN, patrón, contraseña fuerte o huella/detección facial.
- Activar el cifrado completo si el dispositivo lo permite, para proteger los datos en caso de pérdida o robo.

Precaución con redes Wi-Fi públicas

- Evitar realizar compras o acceder a servicios bancarios en redes abiertas.
- En caso de conexión necesaria, utilizar una VPN confiable para cifrar la conexión.

Descargar únicamente aplicaciones de tiendas oficiales

- Evitar la instalación de aplicaciones de fuentes externas.
- Revisar los permisos que solicita cada aplicación y limitar aquellos que sean excesivos.

Utilizar autenticación de dos factores (2FA)

- Activarla en correo electrónico, banca, redes sociales y aplicaciones críticas.
- Proporciona una capa adicional de seguridad, aunque se obtenga la contraseña.

Revisar permisos y seguridad de las aplicaciones regularmente

- Revocar acceso a cámara, micrófono o ubicación si no resulta necesario.
- Desinstalar aplicaciones que no se utilicen o que puedan ser sospechosas.

EJERCICIO PRÁCTICO

¿Cómo actuar antre un posible caso de phishing?

Imagínate que recibes en tu correo corporativo un mensaje con el asunto: ***"Actualización urgente de tu contraseña corporativa".*** El remitente parece legítimo (dominio interno de la organización) y contiene un enlace que imita la intranet.

Primera reacción

- ☐ **Opción A:** Haces clic en el enlace e introduces tus credenciales.
- ☐ **Opción B**: Reenvías el correo a varios compañeros para consultarles si lo han recibido.
- ☐ **Opción C:** Revisas el remitente, sospechas que no es confiable y decides no hacer clic.

Solución. Tercera opción

Segunda acción

- ☐ **Opción A**: Ignoras el correo y lo borras.
- ☐ **Opción B**: Lo reportas inmediatamente al área de TI o al buzón de seguridad (ej. phishing@empresa.com).
- ☐ **Opción C**: Guardas el correo "por si acaso" sin avisar a nadie.

Solución. segunda opción

Resultados posibles PRIMERA REACCIÓN

La acción correcta es la tercera.

Si hiciste clic o reenviaste el correo:

- ◊ El atacante obtiene tus credenciales o más empleados quedan expuestos.
- ◊ Se incrementa el riesgo de robo de información sensible, interrupción de operaciones y sanciones por incumplimiento.
- ◊ Puede producirse una pérdida de confianza de clientes y socios.

Si desconfiaste y no hiciste clic:

- ◊ Evitaste que el atacante accediera a tu cuenta.
- ◊ La amenaza queda contenida.
- ◊ Si en la segunda acción ignoraste o guardaste el correo sin avisar:
- ◊ No proteges a la organización: el correo puede seguir llegando y afectar a otros.
- ◊ Se retrasa la capacidad de respuesta y aumenta la probabilidad de daños.

Resultados posibles SEGUNDA ACCIÓN

La acción correcta es la segunda.

Si en la segunda acción reportaste el correo:

- ◊ El equipo de TI puede bloquear la amenaza y alertar a todos.
- ◊ Se reduce el impacto del ataque.
- ◊ Se fortalece la cultura de seguridad en la empresa.

Evitar ataques de phishing

RECUERDA

Verificar el remitente y la autenticidad del mensaje.

Reportar de inmediato cualquier correo sospechoso al equipo de TI.

No hacer clic en enlaces ni descargar archivos sin estar 100% seguro.

Nunca introducir las credenciales en páginas no verificadas.

No reenviar correos sospechosos a otros compañeros.

HERRAMIENTAS TÉCNICAS
RECOMENDADAS

HERRAMIENTA	FINALIDAD	COSTE	LINK 👆
Windows Update (Microsoft)	Activar actualizaciones automáticas.	NO	Enlace a la herramienta
Microsoft Defender	Instalar y mantener antivirus.	NO	Enlace a la herramienta
Bitwarden	Cambiar contraseñas débiles y usar MFA.	NO (cuenta con un plan opcional de pago)	Enlace a la herramienta
Google Authenticator	Activar autenticación multifactor (2FA) en correos y servicios críticos.	NO	Enlace a la herramienta
Acronis Cyber Backup	Hacer una copia de seguridad externa.	SÍ	Enlace a la herramienta

Enrique Pérez de Tena

Responsable de la Oficina de Relaciones Institucionales del Mando Conjunto del Ciberespacio (MCCE)

Si me definiera la Inteligencia Artificial diria que:

Soy marino por vocación y piloto de helicópteros por pasión. El mundo ciber me llegó cuando ya pensaba en retirarme, y aunque apenas sabía arrancar un ordenador, ahora disfruto cada reto como un niño con un helado.

Es un mundo nuevo que me exige aprender constantemente y me preocupa ver cómo la sociedad asume riesgos digitales innecesarios. Muchas empresas no invierten en ciberseguridad y luego pagan caro por ello.

Para mí, es evidente: es mucho más barato protegerse que sufrir las consecuencias.

AL VUELO

¿Quién es el malo?
Cualquiera que me ataque.

¿Quién es el bueno?
Yo y todos los que defendemos nuestro modelo de vida y social.

Un sueño recurrente
Encontrar la herramienta definitiva de ciberseguridad que garantice al 100 % que un sistema no está comprometido. No existe.

Recomendación para amigos en una cena
Leer siempre los términos y condiciones; si no, vendes tu alma al diablo digital.

¿En qué país se navega mejor en el mundo ciber?
No lo sé, pero España es respetada por su modelo de gobernanza y activos.

¿Naufragamos?
Sí, si no podemos restaurar sistemas y servicios tras un ataque.

Nunca subestimes...
Cualquiera que no sepa informática puede causar un gran daño usando IA.

¿Cuál es el propósito del Mando Conjunto del Ciberespacio?

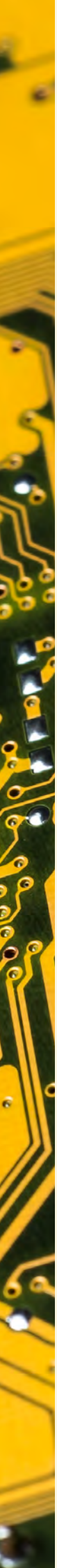
Para comprender bien nuestro trabajo, conviene hacer un poco de historia. A principios de la década de 2010, las Fuerzas Armadas se dieron cuenta de que el entorno digital se estaba convirtiendo en un nuevo campo de operaciones clave. Era evidente que el futuro de la seguridad nacional no solo se jugaba en tierra, mar o aire, sino también en las redes, los sistemas de información, las comunicaciones y todo lo que circula por el ciberespacio. En 2013 se crea el Mando Conjunto de Ciberdefensa, un pequeño equipo pionero de apenas 20 personas, que empezó con escasos medios, pero con una gran determinación. Pese a las limitaciones, desarrollaron capacidades desde cero, demostrando que España podía avanzar en este terreno estratégico.

Con el tiempo, se vio que había que ir más allá de la simple ciberdefensa. Era necesario integrar otras capacidades: guerra electrónica, ciberinteligencia, seguridad en telecomunicaciones (CIS), uso seguro del espectro electromagnético, sistemas satelitales, comunicaciones cifradas... El entorno digital es mucho más complejo de lo que parece. Así, en 2020, el antiguo Mando de Ciberdefensa evolucionó al actual Mando Conjunto del Ciberespacio, que abarca un espectro mucho más amplio.

Nuestro objetivo principal es que las Fuerzas Armadas puedan operar con seguridad en todos los escenarios donde haya tecnología: un barco, un avión, una base militar, un centro logístico o incluso una operación en el extranjero.

Aseguramos que sus sistemas funcionen correctamente, que no sean vulnerables a interferencias o ataques, y que la información fluya de manera segura. Somos el escudo invisible que garantiza que todo lo demás funcione cuando hace falta.

> ***"El ciberespacio es el quinto dominio de las operaciones militares.***



¿Cuántos efectivos sois actualmente?

En 2021, cuando me incorporé, éramos unas 250 personas. Hoy, apenas cuatro años después, ya hemos superado los 500. Y la previsión es que, en un plazo de cinco años, lleguemos a estar entre 1.300 y 1.400. Es un crecimiento muy notable, pero absolutamente necesario.

Este aumento responde no solo al volumen creciente de amenazas, sino a la necesidad de tener equipos más especializados. Necesitamos perfiles muy diversos: desde ingenieros en ciberseguridad, expertos en guerra electrónica, criptógrafos, analistas forenses, hasta operadores de sistemas satelitales. Además, debemos estar disponibles 24/7, con turnos rotativos y equipos de reacción inmediata. El crecimiento también significa que estamos incorporando más talento joven y civil, lo que nos da una visión más amplia y nos permite mantenernos al día frente a un adversario que no descansa.

¿En vuestro ámbito también se está notando el aumento del presupuesto en defensa?

Sí, aunque siempre se puede hacer más. El aumento del presupuesto en defensa se nota, pero en nuestro caso, el ciberespacio tiene una característica particular: permite mucho con poco. Un entorno de operaciones clásico como el marítimo o el aéreo requiere inversiones gigantescas —fragatas, cazas, misiles, mantenimiento...—. En cambio, nosotros, con una fracción mínima de ese presupuesto, podemos desplegar herramientas muy eficaces.

> ***"Somos el escudo invisible que garantiza que todo lo demás funcione cuando hace falta.***

Pero también hay una trampa: esa facilidad de entrada al entorno cibernético significa que los adversarios también lo tienen fácil. Un grupo hostil, con pocos recursos, puede atacar redes críticas o desinformar a la población usando herramientas gratuitas y conocimientos técnicos. Es decir, la amenaza está al alcance de cualquiera, desde un Estado hasta un actor no estatal o incluso individuos con motivaciones ideológicas, políticas o económicas.

Por eso, cada euro invertido en ciberdefensa tiene un retorno altísimo. Pero necesitamos que esas inversiones sean sostenidas y estén bien dirigidas, no solo en herramientas tecnológicas, sino también en formación, retención del talento y cultura de ciberseguridad.

¿La gente joven quiere trabajar en ciberdefensa? ¿Hay vocaciones?

Cada vez más, sí, pero hay que saber atraerles. El entorno militar no siempre es el más natural para un perfil técnico joven. Pero cuando se les muestra lo que hacemos, cómo trabajamos, y lo estratégico que es nuestro papel, muchos se sienten atraídos. Y lo que es más importante: se quedan. Porque aquí encuentran un entorno de misión, de propósito, donde su trabajo tiene un impacto real en la seguridad del país.

Además, estamos adaptando los recorridos profesionales: jóvenes con grados en Ingeniería Informática, Telecomunicaciones o incluso Formación Profesional pueden acceder a puestos técnicos desde el inicio. Eso elimina las barreras tradicionales de acceso y acelera la incorporación de talento útil.

También trabajamos con universidades, institutos y empresas tecnológicas para crear sinergias. No queremos ser una burbuja militar cerrada, sino una estructura abierta que dialogue con el entorno civil y tecnológico del país.

¿El ciberespacio funciona como un "cuarto ejército"?

No exactamente. Más bien hablamos del ciberespacio como el "quinto dominio" de operaciones. Según la OTAN, los cinco dominios son: tierra, mar, aire, espacio y ciberespacio. Este último es transversal: no es un ejército autónomo, sino un entorno en el que todos los demás operan.

Por ejemplo, un buque de guerra depende de sistemas digitales para navegar, comunicarse y combatir. Si esos sistemas son vulnerables, el barco entero

queda comprometido. Lo mismo ocurre con un avión, una base militar o una unidad desplegada. El ciberespacio es el tejido invisible que une todo: comunicaciones, inteligencia, logística, operaciones. Por eso no hay una "guerra cibernética" aislada: hay guerras que siempre tienen un componente cibernético cada vez más importante.

¿También protegéis infraestructuras sensibles como centrales eléctricas?

No directamente, pero estamos integrados en la red nacional de respuesta ante incidentes graves. En España existen tres grandes CERT (Computer Emergency Response Team). Uno es el de INCIBE, orientado a empresas y ciudadanos; otro es el del CCN-CERT, centrado en administraciones públicas y vinculado al CNI; y el tercero es el nuestro, el Spanish Defence CERT, que da cobertura al Ministerio de Defensa y las Fuerzas Armadas.
Cuando hay una amenaza o un ataque serio —por ejemplo, contra una central eléctrica o un hospital—, trabajamos de forma coordinada. Compartimos inteligencia, activamos protocolos comunes y, si hace falta, actuamos de manera conjunta. Además, en casos de especial gravedad, todos los CERT colaboramos bajo la dirección del Departamento de Seguridad Nacional. Nuestro papel es esencial en todo el ecosistema de ciberseguridad nacional.

¿La próxima guerra será cibernética?

No necesariamente será solo cibernética, pero lo cibernético será protagonista, sin duda.
Ya lo estamos viendo. En conflictos como el de Ucrania, el uso de drones, ciberataques, desinformación y guerra electrónica está completamente integrado en las operaciones militares. Y en muchos casos, los efectos de un ataque digital son incluso más impactantes que un bombardeo físico, porque pueden paralizar infraestructuras críticas sin necesidad de disparar un solo tiro.

Además, el ciberespacio tiene una ventaja para los agresores: permite operar con ambigüedad. No siempre se puede atribuir con claridad quién está detrás de un ciberataque. Eso complica la respuesta diplomática o militar. Pero no podemos ignorar que hoy, colapsar una red eléctrica, interrumpir el suministro de agua o inutilizar un sistema de defensa se puede hacer desde miles de kilómetros, sin necesidad de tropas ni misiles. Eso es un cambio radical en la forma de pensar la guerra.

> ***La mayoría de los ciberataques exitosos no se deben a fallos técnicos, sino a errores humanos.***

¿Estáis preparados también para la ofensiva, no solo para defender?

Sí. No tendría sentido limitarse solo a defender. En cualquier entorno operativo —marítimo, terrestre, aéreo o cibernético—, la capacidad ofensiva es esencial. No solo como disuasión, sino para neutralizar amenazas antes de que se materialicen, o para responder proporcionalmente si se produce una agresión.

Obviamente, esto está regulado por una normativa muy estricta, tanto nacional como internacional. No se actúa de forma arbitraria. Pero tenemos las capacidades, los procedimientos y el marco legal para hacerlo si fuera necesario. Lo que está claro es que la mejor defensa, muchas veces, es que el adversario sepa que también puedes responder.

Dices habitualmente que "todos los días hay guerra", aunque no lo veamos. ¿Qué significa eso exactamente?

Significa que estamos en una situación de confrontación permanente. Todos los días recibimos entre 1.500 y 2.000 intentos de acceso, escaneos de vulnerabilidades, campañas de phishing, malware o ingeniería social. Muchos de estos ataques son automatizados, pero otros son muy específicos, dirigidos contra objetivos concretos. Y no paran. Ni los fines de semana, ni en verano, ni de madrugada.

En 2024, gestionamos más de 1.000 incidentes reales. Algunos de ellos tuvieron un nivel de riesgo muy alto. Pero lo más preocupante es cómo ha cambiado el perfil del atacante. Ya no hablamos de aficionados o "hackers" solitarios. Hoy enfrentamos estructuras criminales organizadas, con jerarquías, departamentos y objetivos económicos o políticos. Algunas incluso ofrecen sus servicios como empresas: tú contratas un ataque, eliges el objetivo, pagas, y ellos lo ejecutan.

Muchos de estos grupos están patrocinados, directa o indirectamente, por Estados. Eso hace que el nivel de sofisticación aumente, y que sea mucho más difícil atribuir los ataques o frenarlos a tiempo. La guerra cibernética ya no es ciencia ficción: es una realidad diaria, aunque la sociedad no siempre lo perciba.

¿Consideras que se está haciendo suficiente para concienciar a la ciudadanía sobre estos riesgos?

Se está haciendo mucho más que antes, pero aún no es suficiente. Desde el Mando Conjunto del Ciberespacio realizamos numerosas acciones de divulgación, colaboramos con centros educativos, universidades, empresas y organismos públicos. Intentamos explicar de forma clara cómo protegerse, qué hábitos adoptar, qué señales de alarma tener en cuenta.

Pero aún falta una verdadera cultura digital. La mayoría de los ciberataques exitosos no se deben a fallos técnicos, sino a errores humanos. Alguien que abre un correo que no debía, que comparte su contraseña, que descarga un archivo infectado. La tecnología puede ser muy segura, pero si el usuario no está bien formado, el sistema entero se vuelve vulnerable.

Necesitamos una ciudadanía crítica, informada, capaz de gestionar su identidad digital con responsabilidad. Porque la ciberseguridad no es solo cosa del Estado, del ejército o de las empresas. Es una responsabilidad colectiva. Y cada clic cuenta.

> ***La guerra cibernética ya no es ciencia ficción: es una realidad diaria, aunque la sociedad no siempre lo perciba.***


NIVEL
INTERMEDIO

NIVEL INTERMEDIO

Si la PYME se encuentra en este nivel de madurez, conviene centrarse en reforzar la seguridad a nivel organizativo de la empresa y aplicar controles (tecnológicos, organizativos, de personal y de accesos físicos), lo que permitirá proteger la información crítica. Así se consolidará lo logrado y se reducirán riesgos frente a amenazas más sofisticadas.

CONTENIDOS
NIVEL INTERMEDIO

Responsable de seguridad
Política de seguridad
Formación
Firmar acuerdos
Requisitos de seguridad en contratos tecnológicos
Plan de respuesta a incidentes
Medidas de segmentación
Auditorías y revisiones

ESTRATEGIAS DE GESTIÓN Y ORGANIZACIÓN

1. Nombrar a un responsable de seguridad

Es recomendable que en la empresa haya alguien encargado de la gestión de los activos de información y de la seguridad digital.

No es necesario, especialmente en una PYME, contar con un CISO con formación universitaria o una larga trayectoria profesional. Puede ser alguien del propio equipo de TI, o incluso un responsable de sistemas con interés y conocimientos en ciberseguridad que:

- Coordine esfuerzos;
- Asegure el cumplimiento de políticas básicas
- Actúe como referencia ante incidentes

Lo importante es que exista una persona que supervise la protección de la información, fomente buenas prácticas y garantice que la empresa pueda reaccionar de manera organizada frente a cualquier riesgo digital.

- Permite al CISO tener visibilidad real de los riesgos técnicos
- Facilita el Gap Analysis contra normas como ISO 27001
- Transforma hallazgos técnicos en decisiones para la alta dirección

2. Redactar una política de seguridad

Es necesario aplicar formalmente una política de seguridad. Podrá ser sencilla pero tiene que ser clara y contener:

- Reglas sobre uso de equipos y redes;
- Contraseñas;
- Condiciones de manejo de datos sensibles
- Plan de actuación ante incidentes.

Con este documento se fomentan buenas prácticas entre todo el personal.

En la sección "Recursos útiles" que ponemos a su disposición al final de esta guía, encontrarás políticas en versiones editables totalmente adaptables a tu empresa, creados por el INCIBE. Cada una de ellas contiene una lista de chequeo de las acciones que debe tomar en cuenta el empresario, el equipo técnico y los empleados.

3. Formar al equipo

Muchos incidentes ocurren por errores humanos: contraseñas débiles, clics en enlaces fraudulentos o mal manejo de archivos. La realización de sesiones periódicas de concienciación del personal, al menos una vez al año; sobre las medidas de seguridad y su importancia para la empresa, así como realizar ejercicios prácticos que impliquen al personal en función de sus responsabilidades, mantienen a todos alerta.

El equipo puede formarse de manera continua utilizando recursos gratuitos a través de las plataformas especializadas como CCN-CERT. La empresa puede promover cursos y talleres internos basados en estos contenidos, o los empleados pueden acceder de forma autónoma a la formación online que ofrece la plataforma, reforzando sus conocimientos sobre ciberseguridad, buenas prácticas y prevención de incidentes, lo que contribuye a crear una cultura de seguridad más sólida dentro de la organización.

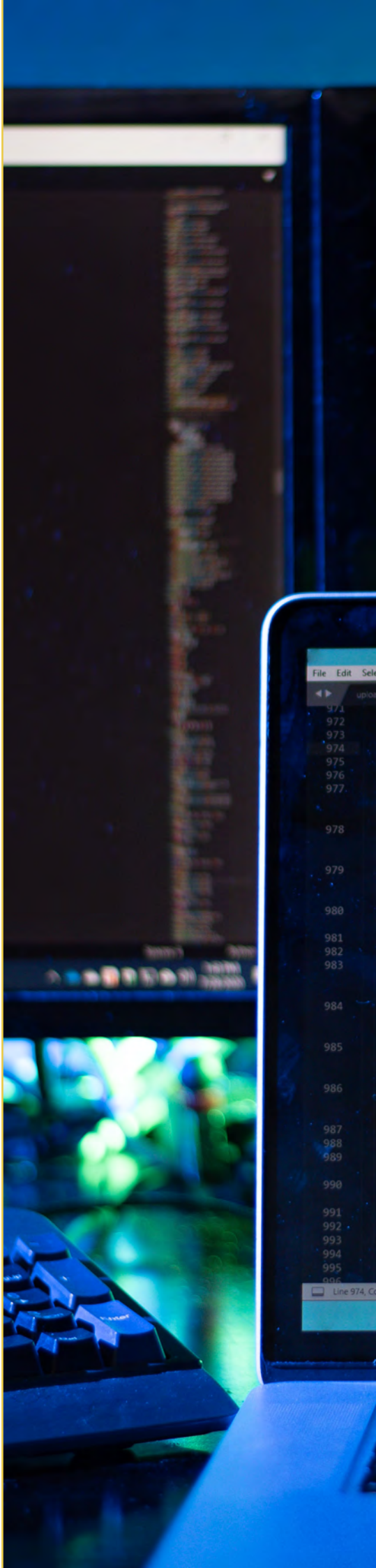
Accede aquí a los cursos online gratuitos de formación del CCN-CERT

4. Firmar acuerdos de confidencialidad con empleados y proveedores

Los acuerdos de confidencialidad (NDA) permiten a una PYME proteger su información sensible frente a empleados y proveedores, asegurando su reserva incluso después de terminar la relación laboral o contractual. Para que sean efectivos, conviene incluir cláusulas que definan qué información es confidencial, cómo debe manejarse y durante cuánto tiempo se mantiene la obligación de secreto.
Un ejemplo de cláusulas esenciales en un NDA sería:

1. **Definición de información confidencial** – Qué se protege
2. **Obligaciones de confidencialidad** – No divulgar ni usar la información fuera del acuerdo.
3. **Excepciones** – Información pública, conocida previamente o requerida por ley.
4. **Duración** – Tiempo que dura la confidencialidad.
5. **Devolución o destrucción** – Qué hacer con la información al terminar la relación.
6. **No concesión de derechos** – No se otorgan derechos de propiedad intelectual.
7. **Consecuencias de incumplimiento** – Sanciones o indemnizaciones.

Con estas condiciones claras, un NDA (*) se convierte en una herramienta eficaz para reducir riesgos, proteger activos estratégicos y reforzar la confianza con terceros.



(*) NDA. Por sus siglas en inglés "Non-Disclosure Agreement": acuerdo de confidencialidad

5. Incluir requisitos mínimos de seguridad en los contratos tecnológicos

Al trabajar con proveedores tecnológicos, una PYME debe asegurarse de que los contratos incluyan requisitos mínimos de seguridad que protejan tanto la información propia como la de sus clientes. Esto evita ambigüedades, fortalece la relación con terceros y ayuda a cumplir con la normativa en materia de protección de datos. Un contrato sin estas garantías deja a la organización expuesta a riesgos importantes en caso de incidentes o fugas de información.

Entre los aspectos esenciales a exigir se encuentran:

1. El compromiso de confidencialidad y el uso adecuado de los datos;
2. La aplicación de medidas técnicas básicas como cifrado, copias de seguridad y control de accesos;
3. La obligación de notificar de manera rápida cualquier incidente de seguridad
4. La existencia de planes de continuidad y recuperación ante fallos.

Además, es recomendable incluir el derecho de la empresa a solicitar evidencias de seguridad, como certificaciones o auditorías, y definir claramente las consecuencias de un posible incumplimiento.

De esta manera, los contratos tecnológicos dejan de ser un simple trámite legal para convertirse en una herramienta de protección activa frente a ciberamenazas. Exigir estas condiciones no solo eleva el nivel de seguridad de la PYME, sino que también transmite confianza a socios y clientes, reforzando la imagen de la empresa como una organización responsable y comprometida con la seguridad digital.

> ***"Cada decisión digital tiene un impacto en la seguridad.***

6. Definir un plan de respuesta a incidentes

En relación con la política de continuidad de negocio (BCP, por sus siglas en inglés), INCIBE señala que deben establecerse de forma expresa varios aspectos esenciales. Entre ellos destacan: concretar el flujo de responsabilidades, definir la política de comunicación y aviso a entidades externas, así como diseñar actividades para verificar, revisar y evaluar periódicamente el plan de continuidad.

Por su parte, el plan de respuesta ante incidentes (IRP, Incident Response Protocol) constituye un pilar fundamental que alimenta directamente al BCP. En el ámbito de la ciberseguridad, una de las prioridades es gestionar adecuadamente los incidentes para evitar o, al menos, minimizar la interrupción de los procesos críticos. Por ello, centraremos la atención en este plan.

Recomendamos tener en cuenta los siguientes 8 puntos clave

1. **Equipo responsable**: Se designará un equipo encargado de gestionar los incidentes de ciberseguridad, incluyendo personal técnico y de dirección que deba estar informado del estado del incidente.
2. **Mejora continua:** Se aprovechará la información de la gestión de incidentes para evaluar y ajustar procedimientos, incorporar mejoras y controles, y realizar acciones preventivas que entrenen al personal frente a posibles incidentes.
3. **Caducidad del plan de gestión:** Se establecerá la frecuencia de revisión y actualización del plan, así como la necesidad de modificarlo tras cambios importantes en los sistemas.
4. **Detección del incidente:** Se definirán las situaciones consideradas incidentes y se implementarán herramientas automáticas de detección, junto con un sistema de alertas que informe en tiempo real.
5. **Evaluación del incidente:** Tras la detección, se categorizará el incidente, determinando su gravedad y priorizando su tratamiento.
6. **Notificación del incidente:** Se creará un punto de contacto único para reportar incidentes o vulnerabilidades, indicando la información a recopilar y las acciones inmediatas, con un listado de contactos para actuar rápidamente.
7. **Resolución de incidentes:** Se desarrollarán procedimientos documentados de respuesta según el tipo de incidente, prestando especial atención a los más comunes y críticos. Esto incluye:
    - ◊ Recoger evidencias manteniendo la cadena de custodia e integridad
    - ◊ Estimar el tiempo de resolución.
    - ◊ Realizar análisis forense cuando sea necesario.
    - ◊ Escalar el incidente si no puede resolverse.
    - ◊ Ejecutar acciones para reparar, mitigar o contener los daños.
8. **Tratamiento del registro del incidente:** Se registrará toda la información relevante del incidente, incluyendo fecha y hora, tipo y gravedad, recursos afectados, posibles orígenes, estado, acciones realizadas, responsables y fecha de resolución y cierre.

¿Qué beneficios trae tener implementado un plan de respuesta a incidentes?

Por ejemplo: si tu empresa enfrenta un ataque de ransomware, el IRP (*) se activa para contener y recuperar los sistemas; esto permite que los procesos críticos definidos en el BCP (*) no se detengan por mucho tiempo.

NOTA: Si hay datos personales involucrados, es imperativo cumplir con el RGPD(*) **: se ha de notificar a la AEPD**(*) **dentro de las 72 horas posteriores al incidente, y a los afectados si el riesgo es relevante.** Adoptar esta estrategia refuerza la seguridad, profesionalidad y la confianza de clientes y socios.

BENEFICIOS CLAVE DE CONTRATAR CON UN IRP EN CIBERSEGURIDAD

Mayor confianza organizacional

Reducción de costes ocultos

Mejor relación con socios y proveedores

Reputación fortalecida

Facilita auditorías y certificaciones

Capacidad de aprendizaje organizativo

Mayor resiliencia estratégica

(*) IRP. Por sus siglas en inglés "Incident Response Plan": Plan de Respuesta a Incidentes. / BCP. Por sus siglas en inglés: "Business Continuity Plan": Plan de Continuidad de Negocio / RGPD "Reglamento General de Protección de Datos " AEPD "Agencia Española de Protección de Datos "

7. Aplicar medidas de segmentación de red y accesos mínimos necesarios

La **segmentación de red** consiste en dividir la infraestructura en zonas según la criticidad de los sistemas, aislando servidores críticos de los menos sensibles. Esto permite que un fallo o ataque en una zona no afecte a toda la red, mejora el control y facilita la detección de incidentes. Se puede implementar mediante **VLANs***(*)*, subredes y **firewalls internos** que controlen estrictamente el tráfico entre zonas. Por ejemplo, una zona crítica con bases de datos solo accesible desde la zona de aplicaciones, mientras que los servidores web públicos están separados en otra zona.

El **principio de acceso mínimo necesario** asegura que cada usuario o sistema tenga únicamente los permisos esenciales para su función, reduciendo riesgos de errores o abusos. Por ejemplo, un empleado de contabilidad solo puede acceder a sistemas financieros, y un equipo de soporte puede reiniciar servicios internos sin modificar bases de datos críticas.

Ambas medidas se complementan usando **control de privilegios**, autenticación multifactor y monitoreo constante.

> ***"Compartir menos información reduce los riesgos.***

8. Realizar auditorías y revisiones regulares

Una estrategia clave para la optimización de las medidas anteriormente propuestas, consiste en la realización de auditorías de sistemas, políticas y procedimientos. Esto asegura que la estrategia de ciberseguridad siga siendo eficaz, que se detecten vulnerabilidades correctamente y que se garantice el cumplimiento de estándares y regulaciones aplicables.

A los efectos de esta guía, se distinguen en dos tipos: las auditorías internas y las auditorías externa. Cada una tiene sus beneficios y momentos de aplicación.

(*) VLAN. Virtual Local Area Network (Red de Área Local Virtual)

CASO: TIENDA DE ROPA

(Ventas físicas + online)

AUDITORÍA INTERNA

- Revisión de sistemas y base de datos
- Problemas detectados: contraseñas compartidas, equipos sin actualizar, copias de seguridad no probadas
- Soluciones: contraseñas individuales, actualizaciones, pruebas semanales de copias...
- Beneficio: menos riesgos internos, menos errores y mayor conciencia del personal.

AUDITORÍA EXTERNA

- Empresa especializada revisa seguridad y cumplimiento
- Riesgos hallados: tienda online mal configurada, pagos sin cifrado seguro
- Medidas: cifrado en tránsito, revisión de contratos y procesos de actualización.
- Beneficio: cumplimiento legal, confianza de clientes/proveedores, preparación para inspecciones.

RESULTADO GLOBAL

- Datos sensibles protegidos
- Ventas y stock más seguros.
- Empleados con mejores prácticas
- Mayor confianza de clientes y socios

Auditorías internas

Las auditorías internas son realizadas por el personal propio de la empresa o bien a través de consultores que actúan como equipo interno. Sus principales beneficios son:

- Permitir un monitoreo continuo de los sistemas y facilitar la detección temprana de vulnerabilidades;
- Fomentar la mejora constante de procesos y controles internos;
- Ayudar a consolidar una cultura de ciberseguridad dentro de la organización.

Son especialmente útiles para revisiones periódicas, cuando se busca mantener un control constante y cuando la empresa ya cuenta con un nivel intermedio de seguridad.

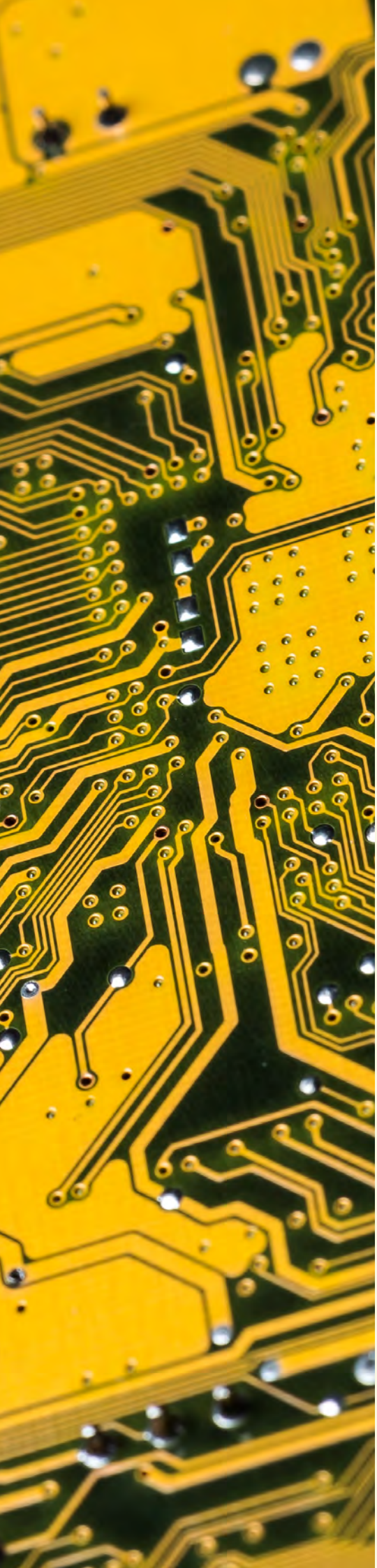
Auditorías externas

Las auditorías externas son ejecutadas por terceros independientes, como consultores especializados o firmas certificadoras. Sus ventajas principales son:

- Ofrecer una visión objetiva e imparcial, identificar riesgos que podrían pasar desapercibidos internamente;
- Garantizar el cumplimiento de regulaciones y estándares internacionales;
- Aportar confianza ante clientes, socios y autoridades.

Son recomendables antes de certificaciones oficiales, auditorías regulatorias o cuando se busca validar los procesos desde una perspectiva externa.

En la práctica, la combinación de ambas auditorías suele ser la estrategia más efectiva: las internas permiten un control y mejora continua, mientras que las externas aportan objetividad, cumplimiento y credibilidad frente a terceros.



Santos González

Catedrático Emérito de Álgebra de la Universidad de Oviedo

Si me definiera la Inteligencia Artificial diria que:

Soy un enamorado de la educación y del trabajo con los jóvenes; ese será mi epitafio. Empecé a dar clases en mi pueblo gracias a un maestro ejemplar y al apoyo de mis padres. Desde entonces he dedicado mi vida a la enseñanza, y seguiré haciéndolo hasta el final.

Creo firmemente que la educación es la herramienta que iguala a los seres humanos y la mayor responsabilidad de un educador. He tenido la suerte de vivir de lo que me apasiona, y me considero un afortunado.

AL VUELO

¿Qué regalarías a un amigo que acaba de abrir su empresa?
Un taller gratuito de ciberseguridad.

Nunca te acuestas sin antes...
Leer sobre matemáticas y ciberseguridad.

¿Qué consejo darías a un joven con su primer móvil?
Que aprenda a manejar bien las contraseñas.

¿La estafa más lucrativa de un ciberdelincuente?
Robar datos y pedir rescate por ellos.

El último grito en ciberseguridad.
La criptografía cuántica.

¿El riesgo más inofensivo?
La confianza.

¿La Tercera Guerra Mundial será matemática?
Ya lo es: se libra en la ciberseguridad.

La Cátedra Castroalonso de Ciberseguridad y Entorno digital contribuyó durante los últimos 4 años a la vanguardia y estudio de los retos en esta materia. ¿Qué retos tuvo ante sí?

Castroalonso es una PYME asturiana especializada en ciberseguridad. Fueron ellos quienes propusieron al rector de la Universidad de Oviedo la creación de esta cátedra y solicitaron expresamente que yo la dirigiera. Para mí fue un honor colaborar con empresas del ámbito tecnológico, y más aún con una tan implicada en este campo.

La ciberseguridad es una pieza clave de la I+D, no solo en Asturias, sino a nivel nacional e internacional. Sostiene sectores fundamentales como la sanidad, la economía o las comunicaciones. Desde

"La computación cuántica es el gran reto que amenaza la seguridad digital.

las matemáticas, que es mi área como catedrático de Álgebra, llevamos años trabajando en este campo, abordando temas como la computación cuántica, la Inteligencia Artificial o el blockchain. Nuestro objetivo en la cátedra fue contribuir al desarrollo tecnológico y, sobre todo, a la formación de jóvenes en áreas con salidas profesionales reales.

¿Qué líneas de investigación desarrollasteis en este tiempo?

Trabajamos principalmente desde una perspectiva matemática. Todo en ciberseguridad, en realidad, se basa en números. Incluso una entrevista como esta entrevista, si se transmite digitalmente, está protegida por claves numéricas. Nos centramos, por ejemplo, en la factorización de números primos, que es la base de la criptografía actual. El reto inmediato es la computación cuántica, que amenaza con romper los sistemas de seguridad basados en esa factorización. Si eso ocurre, se pondrían en riesgo las comunicaciones digitales más sensibles, como las de líderes internacionales o sistemas financieros.

Por eso estuvimos desarrollando nuevos algoritmos que pudieran mantener la seguridad en ese nuevo escenario. Utilizamos herramientas como la teoría de grupos, una rama de las matemáticas con aplicaciones directas en criptografía. También trabajamos con Inteligencia Artificial, que al final no es más que una serie de algoritmos matemáticos.

La cátedra se diseñó para promover la colaboración público-privada. ¿Qué aporta cada parte?

La colaboración entre lo público y lo privado es esencial. En Asturias, este modelo está ganando fuerza y creo que es el camino correcto. La universidad pública debe competir, mejorar y colaborar con las empresas privadas, que tienen otros objetivos pero también mucha capacidad de acción.

Un buen ejemplo es el proyecto que tenemos junto a la Universidad Alfonso X el Sabio. Lo lidera la Universidad de Oviedo y cuenta con financiación del INCIBE y fondos europeos. A través de este programa llevamos formación en ciberseguridad a colegios, empresas y diferentes colectivos.

¿Ese proyecto conjunto se centra únicamente en ciberseguridad?

Sí, al menos en nuestra parte. Trabajamos en tres líneas principales: formación en colegios, asesoramiento a pequeñas empresas y análisis del estado actual de la ciberseguridad.

En los colegios impartimos talleres para formar a los más jóvenes en el uso seguro de la tecnología. En el ámbito empresarial, ayudamos especialmente a las PYMES, que suelen ser más vulnerables. Y además participamos en encuentros nacionales con expertos para debatir sobre las amenazas y soluciones actuales.

> ***El riesgo más inofensivo: la confianza.***

¿En qué punto se encuentra Asturias respecto al desarrollo de un ecosistema de innovación en ciberseguridad?

Aún no estamos donde deberíamos, pero al menos hay conciencia del reto. Se están promoviendo microcredenciales (talleres de pocos créditos que ofrece la Universidad conjuntamente con empresas e instituciones) y proyectos formativos desde la Universidad y la Consejería de Ciencia. Además, la Cámara de Comercio también está implicada.

Lo ideal sería contar con un centro propio de ciberseguridad en Asturias o, si no es posible, mantener una colaboración fuerte con el INCIBE. Llevo colaborando con ellos desde su origen como INTECO, hace más de 20 años, y es sin duda uno de los mejores proyectos que se han impulsado en este campo desde España.

Ahora mismo hay un debate abierto sobre la creación de un Centro Nacional de Ciberseguridad. Se baraja las opciones de instarlo en León, Madrid o Málaga. Asturias no puede quedarse al margen de proyectos de esta envergadura. Es fundamental tener una estrategia cohesionada.

En tu faceta como divulgador, ¿cómo crees que influye la historia de la matemática en la tecnología actual?

La sociedad digital actual se basa en la lógica booleana, en ceros y unos. George Boole, creador de esa lógica hace 150 años, es una figura esencial. Curiosamente, su tataranieto es uno de los impulsores de la Inteligencia Artificial moderna y ha sido galardonado recientemente con el Premio Nobel de Física. Es importante explicar estas conexiones para que la ciudadanía entienda que detrás de cada avance hay una historia científica y humana.

¿Cómo ves la relación de los jóvenes universitarios con la ciberseguridad?

Todavía están lejos del nivel que deberían tener, aunque poco a poco va mejorando. Nosotros impartimos seminarios y formamos a nuestros alumnos en estos temas. También se están promoviendo microcredenciales que ayudan a reforzar su perfil profesional.

El INCIBE calcula que en los próximos dos años habrá 90.000 empleos vinculados a la ciberseguridad. Es un sector en auge, transversal y multidisciplinar. No solo los matemáticos tienen cabida: también economistas, psicólogos, ingenieros... En nuestro equipo, por ejemplo, tenemos una matemática que estudió psicología para trabajar en el análisis de redes sociales desde esa perspectiva.

> ***¿La Tercera Guerra Mundial será matemática? Ya lo es: se libra en la ciberseguridad.***


NIVEL
AVANZADO

NIVEL AVANZADO

Si la PYME se encuentra en este nivel, significa que ya dispone de un conjunto sólido de medidas de seguridad, diseñadas para garantizar la protección integral de los activos de información frente a accesos no autorizados y otras amenazas que puedan comprometer la confidencialidad, integridad o disponibilidad.

No obstante, incluso en este nivel la empresa sigue siendo vulnerable a incidentes de seguridad, que pueden ir desde ataques informáticos hasta la pérdida de dispositivos con información sensible. Por ello, resulta esencial contar con mecanismos de mejora continua que permitan evaluar la efectividad de los controles implantados y adaptarlos a nuevas amenazas.

La ciberseguridad es un proceso dinámico: exige revisar periódicamente las medidas existentes, actualizar el inventario de dispositivos y sistemas, y realizar pruebas o simulacros que ayuden a detectar fallos antes de que se conviertan en incidentes reales.

En esta sección, te recomendamos un conjunto de estrategias que se pueden aplicar para ayudar al negocio a fortalecer su seguridad y garantizar que las medidas y los controles que ya han sido implementados continúen siendo efectivos.

CONTENIDOS

NIVEL AVANZADO

ESTRATEGIAS AVANZADAS

1. Obtener una certificación (ISO 27001, ENS-Medio/Alto)

Contar con una certificación reconocida, como la **ISO 27001** o el **Esquema Nacional de Seguridad (ENS)** en nivel Medio o Alto, aporta un **valor diferencial** a la empresa frente a clientes y en procesos de licitación. Estas certificaciones acreditan contar con un sólido sistema de gestión de seguridad de la información; reflejando profesionalidad, y por tanto, generando confianza tanto en socios como en usuarios.

No obstante, es importante tener en cuenta que la obtención de una certificación puede implicar una **inversión significativa** para una PYME, por lo que su implementación se plantea como una **recomendación estratégica**, a valorar según los recursos y prioridades de la organización.

Pasos recomendados para la PYME:

1. **Definir el objetivo.** Definir si la empresa aspira a obtener una certificación en ISO 27001, en el Esquema Nacional de Seguridad (ENS) u otro marco de referencia, en función del sector y del perfil de sus clientes; o bien optar únicamente por alinearse con dicho marco y establecer un Sistema de Gestión de Seguridad de la Información (SGSI) sin buscar la certificación.
2. **Nombrar un responsable interno.** Designar una persona o equipo que lidere el proceso de certificación y coordine con consultores externos si fuera necesario.
3. **Diagnóstico inicial.** Realizar un análisis de la situación actual (brecha entre lo que exige la norma y lo que la empresa ya cumple).
4. **Plan de acción.** Elaborar un plan con las medidas a implementar: políticas, controles, formación del personal, gestión de riesgos, etc.
5. **Implantación de medidas.** Ejecutar los cambios necesarios (ejemplo: clasificación de la información, control de accesos, procedimientos de backup, gestión de incidentes).
6. **Auditoría interna.** Revisar que todo lo implantado funciona correctamente antes de la auditoría oficial.
7. **Certificación (si procede) .** Contratar una entidad certificadora acreditada que evalúe a la empresa y emita la certificación oficial.

2. Implantar un ciclo de mejora continua

La mejora continua debe consolidarse como un principio central en la estrategia de ciberseguridad. Para lograrlo, la empresa puede seguir estos pasos:

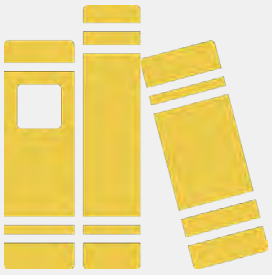
1. **Realizar auditorías periódicas** (internas y/o externas) para evaluar el estado de la seguridad.
2. **Revisar indicadores clave** que midan el desempeño de los controles y la gestión de incidentes.
3. **Definir y actualizar un roadmap de seguridad** con prioridades claras y plazos realistas.
4. **Introducir mejoras de forma constante**, ajustando políticas, procedimientos y controles según los hallazgos.

3. Dar un paso más: aplicar modelos de madurez

Una vez consolidada la mejora continua, el siguiente paso es apoyarse en modelos de madurez reconocidos, como el NIST CSF (*) o el CMMI (*), que ayudan a estructurar ese proceso.

Para aplicarlos, la empresa puede avanzar de la siguiente manera:

1. **Planificar (Plan):** establecer objetivos claros y evaluar riesgos y controles existentes.
2. **Hacer (Do):** implementar las medidas de seguridad definidas (técnicas y organizativas).
3. **Verificar (Check):** medir la efectividad de las acciones mediante métricas y auditorías.
4. **Actuar (Act):** ajustar procesos, reforzar controles y perfeccionar las prácticas en función de los resultados.



RECURSOS ÚTILES

En el ámbito de la ciberseguridad y la protección de la información, es esencial que las organizaciones, en especial las PYMES, dispongan de fuentes fiables de consulta y apoyo que les permitan mantenerse actualizadas e incorporar buenas prácticas. Con el fin de facilitar este proceso, se presentan a continuación diversos recursos de referencia a nivel nacional y europeo, que han servido de guía, herramienta y orientación práctica para la elaboración de este documento. Su propósito es reforzar la seguridad digital en el entorno empresarial.

De manera enunciativa, aunque no exhaustiva, se sugieren:

- ☐ **INCIBE.** Oficina de Seguridad del Internauta. Enlace directo 👆
- ☐ **INCIBE.** Políticas de seguridad para la PYME. Enlace directo 👆
- ☐ **INCIBE.** Cursos de ciberseguridad para PYMES. Enlace directo 👆
- ☐ **INCIBE**. El cortafuegos. Enlace directo 👆
- ☐ **CCN-CERT** – Gobernanza de la Ciberseguridad Nacional. Enlace directo 👆
- ☐ **CCN-CERT** – Herramientas y soluciones de ciberseguridad. Enlace directo 👆
- ☐ **CCN-CERT** - Guías para PYMES:. Enlace directo 👆
- ☐ **ENISA** – Agencia de la Unión Europea para la Ciberseguridad. Enlace directo 👆
- ☐ **EEPD**. Agencia Española de Protección de Datos. Enlace directo 👆

(*) NIST CSF.National Institute of Standards and Technology Cybersecurity Framework (Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología de EE. UU.)./ CMMI: Capability Maturity Model Integration (Modelo Integrado de Madurez de Capacidades)

Cristina Fernández Caldueño

Directora de Operaciones de Castroalonso

Si me definiera la Inteligencia Artificial diria que:

Soy tecnohumanista y periodista de formación, aunque dejé la profesión en los noventa. Dirijo operaciones en Castroalonso, coordinando equipos y proyectos, representando a la organización.

Mi labor busca unir perfiles técnicos y no técnicos, creando un entorno en el que todos se entiendan y se sientan cómodos. Creo en situar a las personas por encima de la tecnología, sin perder de vista su papel imprescindible en nuestro avance.

AL VUELO

¿A qué temes más en ciberseguridad?
A un ataque global, una guerra digital.

¿Un día en el que pareciera que los malos ganaban?
Ninguno.

¿A quién pondrías a formarse en ciberseguridad?
A cualquier político con responsabilidades.

Un uso indispensable de la Inteligencia Artificial.
La lectura de una licitación.

¿A quién animarías o reanimarías con Inteligencia Artificial?
A todo el mundo, es imprescindible.

¿A quién darías el premio Ciberseguro?
A cualquier PYME que, con esfuerzo, invierte en ciberseguridad.

¿Y el premio Ciberinseguro?
A los eslabones más débiles: autónomos, PYMES, departamentos de RR. HH., administración y trabajadores poco formados.

¿En qué consiste vuestra labor al frente de los servicios de ciberseguridad en Castroalonso?

En Castroalonso trabajamos desde la consultoría en tres grandes áreas: Ciberseguridad, Derecho Digital y Ética Digital, prestando además servicios de peritaciones informáticas, auditorías de seguridad y acciones de sensibilización y formación. Uno de nuestros objetivos primordiales es acercar la ciberseguridad a las PYMES, que suelen ser las más expuestas a los riesgos digitales.

Además de intervenir frente a incidentes —cuando, en muchos casos, ya es tarde y apenas queda desconectar sistemas o reparar con recursos limitados—, priorizamos la prevención a través de la formación, la concienciación y las auditorías proactivas. Apoyamos a las empresas en su camino a la implantación de controles de seguridad conforme a normas como la ISO 27001 o el Esquema Nacional de Seguridad, requisitos que muchas compañías deben cumplir para poder licitar con el sector público, aunque no siempre comprendan su verdadera relevancia.

> ***El principal obstáculo es económico: la ciberseguridad es intangible y cuesta percibirla como inversión.***

Desde la pandemia, y gracias también al impulso de iniciativas como la Cátedra Universitaria, hemos reforzado esta labor esencial de sensibilización, demostrando que la ciberseguridad no es un lujo, sino una necesidad creciente para la sostenibilidad y resiliencia de cualquier organización.

¿Habéis notado un cambio en la sensibilización y la conciencia del peligro en estos últimos años?

Sí, claramente. Desde que empezamos en 2018, justo antes de la pandemia, hasta hoy, la evolución ha sido notable. Los fondos europeos y programas de INCIBE han sido fundamentales para que el mensaje llegue, a través de cátedras y otras iniciativas educativas. También los medios de comunicación han jugado un papel esencial: antes apenas había noticias de ciberataques, ahora es habitual ver titulares sobre brechas de datos masivas o ataques a empresas. Esto ha hecho que tanto las compañías como la sociedad en general estén mucho más concienciadas. Lo que antes parecía lejano, exclusivo de grandes corporaciones, hoy afecta a todos.

Aunque el avance es evidente, aún queda camino por recorrer, sobre todo en la formación básica para identificar amenazas en móviles o correos electrónicos.

¿A qué tipo de empresas les cuesta más convencer de la necesidad de dar ese salto en seguridad?

Principalmente a las PYMES más pequeñas. El principal obstáculo es económico: la ciberseguridad es intangible y cuesta percibirla como inversión. A diferencia de adquirir un equipo físico, no se ve

> ***La ciberseguridad no es un lujo, sino una necesidad creciente.***

ni se toca. Por eso recurrimos a simulaciones de ataques —cajas negras y blancas— para mostrar vulnerabilidades reales.
Otro reto es que muchos informáticos internos creen tenerlo todo controlado, sin aceptar que la ciberseguridad va mucho más allá de antivirus o firewalls.

Convencer es difícil porque los recursos son limitados y el coste de estos servicios pesa en sus presupuestos. Además, aportamos también desde lo jurídico, con asesoría en protección de datos o peritaciones judiciales, lo que añade valor, pero también complejidad.

¿Crees que la sensibilización ya ha llegado a la mayoría de las PYMES o todavía queda mucho por hacer?

Hace unos tres años empezamos a ver un cambio claro: las PYMES ya no perciben la ciberseguridad como algo lejano o exclusivo de grandes organizaciones.
Hoy entienden que les afecta directamente, aunque existe un desfase entre la concienciación y la capacidad real de inversión. Muchas reconocen su importancia, pero no tienen recursos para aplicar medidas adecuadas.
A menudo se piensa que la ciberseguridad es solo técnica, cuando en realidad incluye formación, procesos y protocolos que afectan a toda la organización. Algunas ya solicitan auditorías para conocer su situación, pero sin el apoyo de las administraciones y de programas europeos, será difícil que den el salto definitivo.

¿Qué más se podría hacer para facilitar que las empresas avancen en su seguridad?

El gran reto es el acceso a recursos y formación de calidad. Los informáticos de las PYMES deben ampliar su visión, entendiendo que la ciberseguridad no es solo técnica, sino que implica también aspectos jurídicos, de sensibilización y gestión del riesgo.

Es fundamental impulsar formación práctica y asequible, ya que los cursos avanzados suelen ser caros, muy técnicos y orientados a grandes corporaciones.

Proyectos europeos y el INCIBE ya están abriendo camino, pero falta un mayor compromiso de las administraciones para destinar más recursos. También es clave reforzar la formación del sector público, que maneja infraestructuras críticas y que muchas veces no dispone de preparación suficiente.

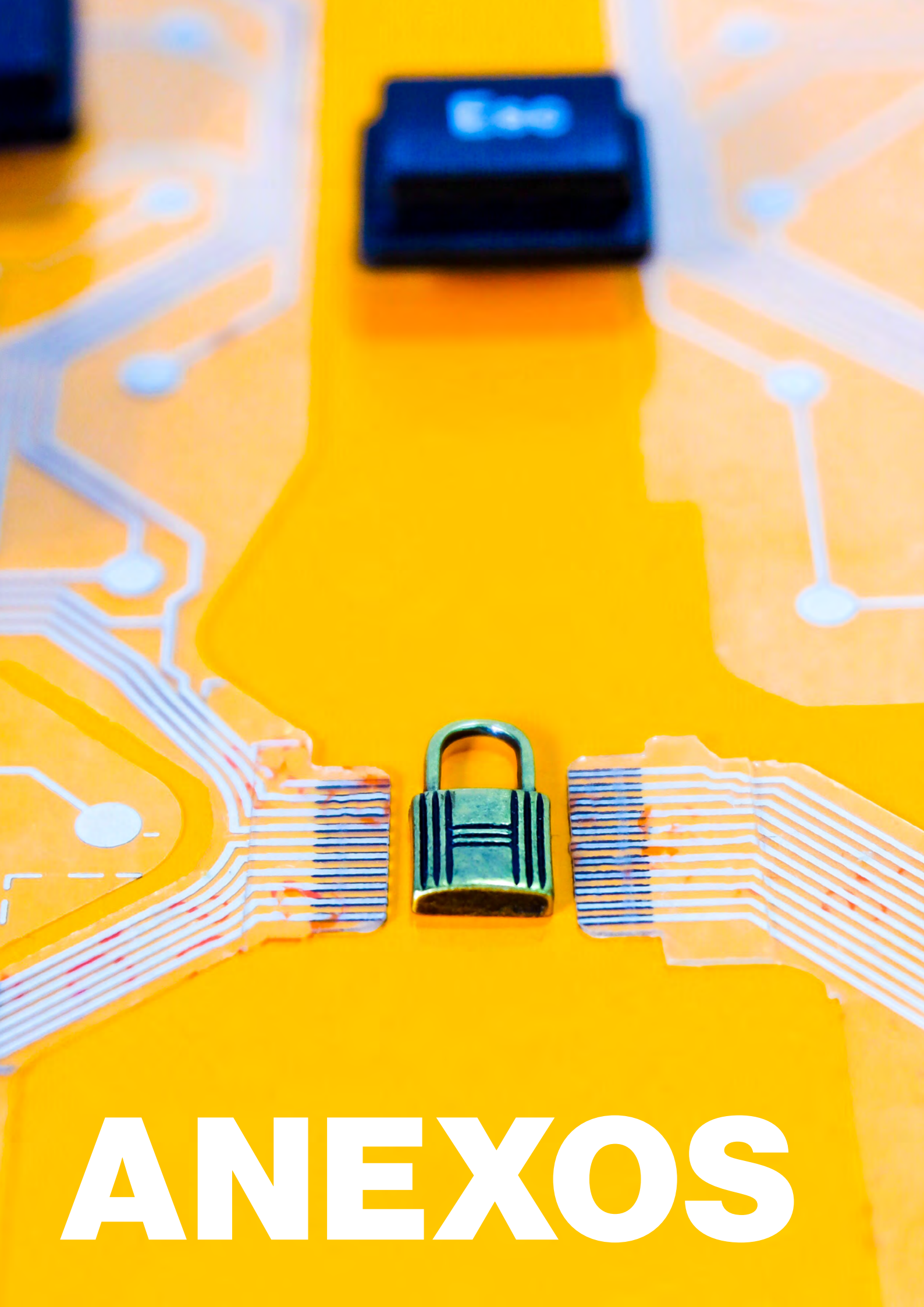
Foto: Marta Martín

¿Cuál es para ti la clave en tu trabajo en ciberseguridad?

La ciberseguridad ya no es solo un tema técnico, sino un riesgo empresarial más, al nivel de incendios o catástrofes naturales. Sin embargo, no todos los responsables de empresas ni empleados entienden aún la magnitud de este riesgo ni cómo mitigarlo. Esto es especialmente crítico en sectores sensibles como energía, agua o sanidad, donde un fallo podría tener consecuencias graves. Además, la digitalización masiva y la Inteligencia Artificial amplían el campo de amenazas, lo que obliga a una actualización constante.

En definitiva, aunque se ha avanzado mucho, la colaboración público-privada y una visión integral serán claves para que las PYMES puedan protegerse ante los retos crecientes del mundo digital.

> ***"Las PYMES ya son más conscientes del riesgo, pero aún falta formación y recursos.***



ANEXOS

ANEXO I

LOS 10 MANDAMIENTOS DE LA CIBERSEGURIDAD

1. **Protege tus contraseñas y no las compartas.** Usa contraseñas fuertes, únicas para cada cuenta, y considera un gestor de contraseñas.

2. **Activa la autenticación en dos pasos siempre que sea posible.** La doble verificación añade una capa extra de seguridad ante accesos no autorizados.

3. **Mantén tus dispositivos y software actualizados.** Aplica parches y actualizaciones de sistemas operativos, aplicaciones y antivirus.

4. **No abras enlaces ni archivos sospechosos.** Evita correos de phishing, mensajes desconocidos y descargas de fuentes no confiables.

5. **Haz copias de seguridad regularmente.** Protege tus datos críticos con backups automáticos y verifica que puedas restaurarlos.

6. **Usa soluciones de seguridad confiables.** Antivirus, firewalls y herramientas de protección deben estar activas y configuradas correctamente.

7. **Protege tu red y dispositivos móviles.** Configura correctamente tu Wi-Fi, usa VPN en redes públicas y activa el cifrado de dispositivos.

8. **Limita los permisos y accesos según la necesidad.** Solo da acceso a datos y sistemas a quienes realmente lo necesiten, evitando privilegios innecesarios.

9. **Conciencia y formación continua.** Aprende sobre riesgos digitales y participa en sesiones de formación para ti y tu equipo.

10. **Planifica y prepara tu respuesta ante incidentes.** Ten un plan de acción en caso de ciberataques, pérdida de datos o intrusiones, y ensáyalo regularmente.

ANEXO II

RECOMENDACIONES GENERALES PARA EL TELETRABAJO

En los últimos años, y especialmente durante y tras la pandemia, muchas empresas han adoptado modalidades de teletrabajo o trabajo híbrido. Este tipo de prácticas requieren recomendaciones específicas, ya que, al no encontrarse el trabajador en el espacio de trabajo u oficina, el uso de los dispositivos debe cumplir con restricciones y precauciones particulares.

Para garantizar un uso seguro de los activos de información y mantener la ciberseguridad en esta modalidad de trabajo, es necesario tener en cuenta las siguientes medidas:

- **Evitar el uso de dispositivos personales para trabajar**
  - Siempre que sea posible, utilizar equipos proporcionados por la empresa.
  - Los dispositivos corporativos cuentan con configuraciones y protecciones específicas que los personales no tienen.
- **Conexión segura a la red corporativa**
  - Usar VPN corporativa para cifrar la conexión y proteger la información transmitida.
  - Evitar redes Wi-Fi públicas para acceder a sistemas de la empresa.
- **Activar firewalls y configuraciones de seguridad**
  - Mantener activado el firewall del sistema operativo y de la VPN.
  - Configurar correctamente reglas de acceso a recursos corporativos desde casa.
- **Separación de entornos personales y profesionales**
  - No mezclar cuentas de correo o aplicaciones personales con las corporativas.
  - Utilizar perfiles o sesiones distintas si se trabaja desde un mismo equipo.
- **Protección física y bloqueo de dispositivos**
  - Bloquear la pantalla cuando no se utilice el ordenador.
  - Evitar dejar dispositivos corporativos desatendidos en lugares accesibles.
- **Conciencia sobre seguridad digital**
  - No abrir enlaces o archivos sospechosos en correos electrónicos.
  - Reportar cualquier intento de phishing o incidente de seguridad al departamento de IT.
- **Copias de seguridad y almacenamiento seguro**
  - Guardar la información laboral únicamente en repositorios corporativos.
  - Evitar almacenar documentos sensibles en dispositivos locales personales.

ANEXO III
INFORMACIÓN ESENCIAL
APLICACIONES GRATUITAS

El uso de aplicaciones gratuitas (como servicios de almacenamiento en la nube, mensajería instantánea o herramientas online de edición/IA) puede implicar riesgos significativos para la **seguridad y privacidad de la información**.

Ejemplos de estos riesgos son:

- **Menor nivel de protección:** no suelen ofrecer las mismas garantías que sus versiones de pago o soluciones corporativas.
- **Uso inadecuado en entornos profesionales:** por ejemplo, compartir documentos sensibles en WhatsApp o almacenar información corporativa en un "drive gratuito".
- **Riesgo de fuga de datos:** herramientas online gratuitas (como convertidores de documentos, chatbots o editores en la nube) pueden recopilar o exponer información sin que el usuario sea consciente.

Siempre que se manejen **datos corporativos o sensibles**, se recomienda utilizar soluciones validadas por la organización, con **licencias profesionales** y políticas claras de privacidad.

> ***Evita usar Wi-Fi públicas para operaciones críticas***

ANEXO IV
HERRAMIENTAS TÉCNICAS

Este anexo presenta **medidas técnicas de seguridad** para pequeñas y medianas empresas con infraestructuras locales, servicios en Internet y entornos en la nube. Su objetivo es que el equipo técnico aplique controles que reduzcan riesgos, protejan la información crítica y fortalezcan la resiliencia de tus sistemas.

A diferencia de consejos generales (copias de seguridad, contraseñas o antivirus), aquí se detallan **mecanismos específicos**: protección de accesos, control de dispositivos, seguridad en redes y correo, y respuesta ante incidentes.

No es una lista completa, pero establece un **marco mínimo de medidas** que, combinadas, elevan de manera significativa la seguridad de tu empresa. Además, estos productos han sido aprobados por el CCN-CERT para su uso en entornos que manejan información sensible o clasificada, y cumplen con los requisitos establecidos en el Esquema Nacional de Seguridad (ENS). Más información, aquí.

CUADRO DE
HERRAMIENTAS TÉCNICAS

CATEGORÍA	FINALIDAD	LINK
Seguridad en Correo y Navegación	Sistema de seguridad para correo electrónico que ofrece protección contra spam, virus y otras amenazas.	Fortinet SSO
Seguridad en Correo y Navegación	Filtra spam, malware y ataques de phishing en correo electrónico corporativo, proporcionando seguridad avanzada para los servidores de correo.	Software Download - Cisco Systems
Dispositivos y Puestos de Trabajo	Agente de seguridad para endpoints que proporciona protección contra malware y otras amenazas.	Fortinet SSO
Dispositivos y Puestos de Trabajo	Proporciona protección avanzada para endpoints(*), combinando detección y respuesta ante amenazas (EDR), prevención de malware, y análisis en tiempo real mediante Inteligencia Artificial.	CrowdStrike: Detenemos las brechas con ciberseguridad basada en IA nativa
Red y Comunicaciones	Dispositivo de seguridad de red que ofrece funcionalidades de firewall, VPN y filtrado web.	Fortinet SSO
Red y Comunicaciones	Garantizar la confidencialidad, integridad y autenticidad de la comunicación remota, permitiendo a los usuarios acceder a recursos internos de forma segura desde ubicaciones externas.	Emma VPN
Aplicaciones y Desarrollo Interno	Plataforma de análisis de seguridad de aplicaciones que ayuda a identificar y corregir vulnerabilidades en el código.	Fortify Software Security Center - Documentation | Micro Focus
Aplicaciones y Desarrollo Interno	Genera números aleatorios físicamente imposibles de predecir, usados para claves criptográficas y operaciones de cifrado de alta seguridad.	TRNG True Random Number Generators
Respuesta y Continuidad	Monitorea, captura y analiza tráfico de red y eventos de seguridad para detectar amenazas avanzadas y proporcionar visibilidad completa de la seguridad de la red.	NetWitness Downloads
Respuesta y Continuidad	Sistema de monitorización de seguridad para gestión de incidentes y análisis de eventos en entornos corporativos o críticos.	MONSE

(*)Endpoint: Dispositivo conectado a la red, como ordenador, móvil o tableta, que puede ser objetivo de protección y gestión en ciberseguridad.

DICCIONARIO

OFICIAL DE LA CIBERSEGURIDAD

2FA (Autenticación en Dos Factores)
Variante de MFA que utiliza exactamente dos factores de autenticación distintos.

Activo Comprometido
Dispositivo, sistema, cuenta o recurso afectado por un incidente de seguridad.

Adware
Software que muestra publicidad no deseada y puede recopilar datos de navegación.

AES (Advanced Encryption Standard)
Algoritmo de cifrado simétrico seguro y eficiente, estándar en la industria.

Antivirus
Software que detecta, bloquea y elimina malware.

Anti-spoofing
Técnicas para evitar la falsificación de IPs o remitentes.

APT (Amenaza Persistente Avanzada)
Ataque sofisticado y prolongado con fines de espionaje o robo.

Ataque de Denegación de Servicio (DoS/DDoS)
Saturación de un sistema con tráfico malicioso.

Backup (Copia de seguridad)
Duplicación de datos en un soporte seguro.

Backdoor (Puerta trasera)
Acceso oculto a un sistema fuera de la autenticación estándar.

Bastionado (Hardening)
Proceso de reforzar un sistema eliminando servicios innecesarios y aplicando configuraciones seguras.

Botnet
Red de dispositivos infectados controlados remotamente.

Ciberataque
Acción en el ciberespacio para interrumpir, robar o destruir información.

Ciberincidente
Suceso que compromete la seguridad de la información.

Cifrado (Encryption)
Transformación de datos en un formato ilegible sin clave.

Cloud Security (Seguridad en la nube)
Controles para proteger datos y aplicaciones en servicios cloud.

Credenciales
Conjunto de usuario y contraseña u otros métodos de autenticación.

CSRF (Cross-Site Request Forgery)
Vulnerabilidad web que induce a usuarios a ejecutar acciones no deseadas.

Cuarentena
Aislamiento de archivos o dispositivos sospechosos.

Data Loss Prevention (DLP)
Tecnología para evitar fugas de información sensible.

Dropper
Malware que instala otros programas maliciosos en el sistema.

Filtrado DNS seguro
Bloqueo de acceso a dominios maliciosos conocidos.

Fingerprinting
Identificación de características de sistemas o aplicaciones.

Firewall
Sistema que filtra tráfico de red según reglas.

Forense Digital
Análisis de evidencias electrónicas tras un incidente.

Honeypot
Sistema falso para atraer y estudiar ataques.

Ingeniería Social
Manipulación psicológica para engañar a usuarios.

Inventario automatizado de activos
Registro continuo de hardware y software en la empresa.

Lista blanca
Recursos o aplicaciones explícitamente autorizados.

Lista negra
Recursos o aplicaciones bloqueados por seguridad.

Malware
Software malicioso como virus, troyanos o ransomware.

MDM (Mobile Device Management)
Gestión centralizada de dispositivos móviles corporativos.

MFA (Autenticación Multifactor)
Método de verificación que requiere dos o más factores (como contraseña + código SMS) para acceder a un sistema.

NAC (Network Access Control)
Controla qué dispositivos pueden conectarse a la red.

NIST (National Institute of Standards and Technology)
Organismo estadounidense que desarrolla estándares y guías de referencia en ciberseguridad y tecnología.

Patch Management (Gestión de parches)
Proceso de actualizar sistemas y aplicaciones.

Phishing
Engaño para obtener credenciales mediante correos o webs falsas.

Playbooks de ciberseguridad
Guías de actuación frente a incidentes comunes.

Política de mínimo privilegio
Otorgar a cada usuario solo los permisos necesarios.

Ransomware
Malware que cifra archivos y pide rescate.

Rogue Access Point
Punto de acceso no autorizado conectado a la red.

Shadow IT
Uso de software o servicios no autorizados por TI.

SIEM (Security Information and Event Management)
Plataforma que centraliza y correlaciona logs de seguridad.

SOC (Security Operations Center)
Centro que monitoriza y responde a incidentes 24/7.

Solución EDR (Endpoint Detection & Response)
Monitoriza dispositivos en busca de comportamientos anómalos.

Spearfishing
Phishing dirigido a objetivos concretos con correos personalizados.

Spyware
Software que recopila información sin consentimiento.

Threat Intelligence (Inteligencia de amenazas)
Información procesada sobre tácticas y técnicas de atacantes.

Troyano
Malware que se oculta como software legítimo.

VLANs (Virtual Local Area Networks)
Segmentación de red en redes lógicas separadas.

VPN (Virtual Private Network)
Canal cifrado para transmitir datos en redes inseguras.

Vulnerabilidad
Debilidad en software, hardware o procesos

Watering Hole
Ataque que infecta sitios web visitados por objetivos específicos

Zero Trust
Modelo de seguridad basado en "nunca confiar, siempre verificar.

RECUERDA...

La ciberseguridad es un proceso continuo y una responsabilidad compartida que afecta a todas las PYMES, sin importar su tamaño o sector.

Proteger la información, la confianza de los clientes y la continuidad del negocio no requiere grandes inversiones, sino constancia, formación y la aplicación de medidas adaptadas a cada realidad.

Esta guía te acompaña desde los primeros pasos hasta estrategias avanzadas, ayudándote a identificar tu nivel de madurez, reforzar áreas débiles y anticiparte a los riesgos.

Implementar buenas prácticas, revisar proveedores, formar al equipo y tener un plan de respuesta ante incidentes son claves para fortalecer la resiliencia y la competitividad.

La mejor ventaja en el mundo digital es estar prevenidos y preparados para afrontar cualquier desafío.

Avanza con decisión: cada medida que adoptes te acerca a una PYME más segura, más fuerte y más confiada en el futuro.

SOBRE LOS AUTORES

El Club de Calidad es una asociación empresarial que promueve la mejora de la gestión, la mejora continua y la transformación digital en Asturias. Reúne a más de 240 organizaciones de todos los sectores y destaca por su capacidad de generar sinergias e intercambio de experiencias entre sus socios.

Una de sus actividades destacadas son los **grupos de trabajo, espacios de colaboración** donde profesionales de diferentes empresas se reúnen para compartir experiencias, analizar tendencias y desarrollar proyectos sobre temas clave como sostenibilidad, economía circular, liderazgo o transformación interna. Entre estos, destaca el grupo de CIOs, formado por responsables de tecnología y sistemas de información, y cuyos miembros impulsaron la necesidad de elaborar esta guía práctica sobre ciberseguridad.

El Club desarrolla iniciativas orientadas a visibilizar casos de éxito y difundir tendencias, organizando jornadas, talleres y foros que facilitan el intercambio de experiencias y la transferencia de conocimiento entre sus socios, contribuyendo activamente a la modernización y competitividad del tejido empresarial asturiano.

Con sede en el Parque Científico y Tecnológico de Gijón, Castroalonso se ha consolidado como referente en Derecho Digital, Ciberseguridad y Ética digital, ofreciendo acompañamiento a entidades públicas y privadas en su transformación digital segura y sostenible y cuyo nicho de trabajo ha sido Asturias.

La organización cuenta con un equipo multidisciplinar que integra perfiles jurídicos, técnicos y **humanísticos**, lo que le permite abordar la ciberseguridad desde una perspectiva integral: cumplimiento normativo, protección de datos, implementación de estándares de seguridad (ISO/IEC 27001, Esquema Nacional de Seguridad), auditorías, formación y cultura corporativa.

A lo largo de los últimos años, Castroalonso ha impulsado iniciativas de referencia como la Cátedra Castroalonso de Ciberseguridad y Entorno Digital (Universidad de Oviedo), las jornadas #Ciberseguridad al Descubierto, cuya séptima edición tendrá lugar este año, y la plataforma Arco Atlántico, centradas en la divulgación y la creación de ecosistemas de innovación en el ámbito digital. Además, **forma parte de la Red Nacional de SOCs en categoría oro** y participa activamente en proyectos europeos de I+D+i, colaborando en áreas como la ética digital aplicada a la Inteligencia Artificial, la gobernanza de datos, y, en general, contribuyendo a la adaptabilidad empresarial en el ámbito tecnológico.

GUÍA PRÁCTICA DE CIBERSEGURIDAD

PARA PYMES

Noviembre 2025