Junta de Andalucía
Consejería de Empleo, Empresa y Trabajo Autónomo

Dirección General de Comercio

Versión 14/10/2025

Asistencia Técnica

saet consultores

www.saetconsultores.es
Servicio de Análisis en Economía y Estrategia Territorial

Guía sobre ciberseguridad en el comercio andaluz

Edita:

Consejería de Empleo, Empresa y Trabajo Autónomo

Coordinación de la edición:

Dirección General de Comercio

Documento elaborado por:

Servicio de Análisis en Economía y Estrategia Territorial S.L.

ÍNDICE

1. Preámbulo

El compromiso de la Junta de Andalucía con la **digitalización segura del sector comercial** se refleja de forma clara y operativa en el **VII Plan Integral de Fomento del Comercio Interior de Andalucía** (en adelante, VII Plan), aprobado por la **Consejería de Empleo, Empresa y Trabajo Autónomo** el 27 de noviembre de 2023. Este plan, concebido como instrumento estratégico para el impulso y la modernización del comercio andaluz, aborda diferentes dimensiones: desde la competitividad y la sostenibilidad, hasta la transformación digital y la formación del capital humano.

El diagnóstico sectorial desarrollado en el VII Plan pone de manifiesto que muchos pequeños comercios y negocios de proximidad se enfrentan a amenazas digitales sin disponer de los recursos, conocimientos o herramientas necesarios para prevenir o responder ante un incidente. A partir de esta debilidad identificada, el Plan incorpora **la actuación 2.1.2.4, "Ciberseguridad en el sector comercio",** mediante la cual se impulsa un conjunto de acciones orientadas a concienciar, capacitar y acompañar a los comercios en su avance hacia una mayor madurez en materia de ciberseguridad.

En este contexto, la *Guía sobre ciberseguridad en el comercio andaluz*, impulsada por la Dirección General de Comercio y elaborada por saet consultores, responde a dicho planteamiento con un objetivo claro: **fomentar la sensibilización del sector comercial** ante los riesgos asociados a la seguridad digital y difundir medidas preventivas y herramientas que contribuyan a evitar vulneraciones y reducir sus posibles consecuencias.

El contenido del documento, de carácter eminentemente práctico, no pretende convertir a los comerciantes en expertos en seguridad digital, sino proporcionarles los recursos necesarios para identificar riesgos, proteger sus activos esenciales y saber cómo actuar y a quién acudir en caso de incidente. En otras palabras, se trata de **promover una cultura empresarial en la que la ciberseguridad forme parte de las decisiones cotidianas de los comercios andaluces**.

Asimismo, la guía se **alinea con las políticas de digitalización impulsadas por la Junta de Andalucía** y se conecta con los instrumentos de apoyo financiados por la Unión Europea y la propia Administración regional, destinados, entre otros ámbitos, a facilitar la adopción de soluciones tecnológicas seguras en las actividades comerciales.

La **Guía sobre ciberseguridad en el comercio andaluz** se organiza en **bloques complementarios** que combinan contenidos conceptuales y recomendaciones operativas. Tras una **contextualización institucional** que sitúa la ciberseguridad en el marco europeo, nacional y autonómico, el documento ofrece una **exposición didáctica de las principales ciberamenazas**, describiendo su naturaleza, mecanismos de acción y razones por las que afectan especialmente al sector comercial. A continuación, se abordan las **medidas de protección más relevantes**, junto con un **catálogo de buenas prácticas** que traduce los principios de ciberseguridad en actuaciones concretas y asequibles para los negocios.

Finalmente, el **anexo de la guía**, que incluye un glosario de términos utilizados, incorpora un **ejercicio introductorio de evaluación de riesgos** en materia de seguridad digital, cuya aplicación

resulta recomendable para cualquier comercio, independientemente de su tamaño o nivel de digitalización.

2. Contextualización institucional de la ciberseguridad

La transformación digital, cada vez más relevante en todos los ámbitos de la sociedad y la economía, ha convertido a la ciberseguridad en una prioridad estratégica para las instituciones públicas. Garantizar un entorno digital confiable no solo implica proteger infraestructuras críticas, sino también fomentar una cultura preventiva entre la ciudadanía y, especialmente, entre las empresas, cuya exposición a las ciberamenazas es cada vez mayor.

Las amenazas digitales han dejado de ser fenómenos aislados o exclusivos de grandes corporaciones. En la actualidad afectan de manera directa a las pymes de todos los sectores, incluyendo las actividades comerciales, tanto minoristas como mayoristas. Estas pueden ser objeto de ciberataques con consecuencias económicas y reputacionales significativas que podrían afectar a su día a día.

Ante esta realidad, la respuesta institucional se despliega en distintos niveles, desde el marco estratégico de la Comisión Europea hasta las medidas impulsadas por el Gobierno de España y la Junta de Andalucía.

La presente sección ofrece una panorámica estructurada del compromiso de las Administraciones Públicas en materia de ciberseguridad, destacando sus esfuerzos en sensibilización y apoyo al tejido empresarial. El análisis contextual que se presenta a continuación muestra un resumen sintético sobre las estrategias y directivas relevantes en materia de ciberseguridad así como el impacto general que se persigue sobre diferentes sectores económicos, con especial atención al comercio.

2.1. Marco Europeo: Una ciberseguridad común para la Década Digital

La Unión Europea ha situado la ciberseguridad como una prioridad estratégica dentro del proceso de transformación digital. La Decisión (UE) 2022/2481 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, establece en su artículo 3 los objetivos generales del **Programa Estratégico para la Década Digital de 2030**. Esta estrategia digital ofrece una visión integral orientada a garantizar un entorno digital seguro y resiliente, apostando por la consolidación de capacidades comunes, la mejora de los mecanismos de **respuesta ante incidentes y la promoción de una cultura de ciberseguridad** compartida entre ciudadanos, empresas e instituciones.

Las regulaciones europeas en esta materia no se limitan a formular principios generales, sino que establecen **obligaciones específicas y definen estándares comunes que deben aplicarse en todos los Estados miembros**. Entre las regulaciones más significativas destacan:

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016[1], conocido como Reglamento General de Protección de Datos (RGPD), que garantiza la protección de los derechos fundamentales vinculados a la privacidad y al tratamiento de los datos personales.

- Es aplicable a cualquier entidad que gestione datos personales en el marco de actividades comerciales.
- Los artículos 5 y 6 establecen los principios de licitud, lealtad, transparencia y responsabilidad proactiva, considerados pilares esenciales de la confianza digital.
- Asimismo, el artículo 32 dispone la obligación de aplicar medidas técnicas y organizativas apropiadas que aseguren un nivel de seguridad adecuado al riesgo.

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016[2], conocida como Directiva NIS (*Seguridad de las Redes y de los Sistemas de Información*), fue pionera en el ámbito de la ciberseguridad europea, al introducir obligaciones específicas de seguridad y notificación para los operadores de servicios esenciales y los proveedores de servicios digitales.

- Esta directiva obliga a estos actores a adoptar medidas preventivas y a notificar incidentes graves.
- Su artículo 14 detalla las medidas técnicas y organizativas necesarias para gestionar los riesgos y mitigar el impacto de los incidentes.
- Con esta directiva se establecieron las bases de una arquitectura de ciberseguridad colaborativa en la Unión Europea.

Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019[3], conocido como Reglamento sobre la Ciberseguridad, refuerza las competencias de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y establece un marco europeo de certificación en materia de ciberseguridad.

- Esta certificación, regulada entre los artículos 46 y 49, se configura como una herramienta clave para generar confianza entre empresas y consumidores, al ofrecer garantías sobre la seguridad de los productos, servicios y procesos digitales.
- En ámbitos de actuación como el comercio electrónico, estas certificaciones representan un factor de diferenciación especialmente relevante.

[1] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

[2] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

[3] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) Nº 526/2013 («Reglamento sobre la Ciberseguridad»).

Además de estas normas, la Unión Europea ha aprobado otras directivas complementarias, entre ellas la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022[4], conocida como Directiva NIS2, que amplía el ámbito de aplicación de la Directiva NIS original, incorpora nuevas obligaciones de gobernanza y extiende su alcance a empresas medianas pertenecientes a sectores no críticos pero estratégicos para la economía digital.

Con este marco normativo, la Unión Europea persigue armonizar la ciberseguridad entre los Estados miembros, garantizando un **nivel básico común de preparación frente a las amenazas**. Para las empresas del sector comercial, este marco configura un entorno regulatorio cada vez más exigente, pero que al mismo tiempo proporciona recursos y orientaciones claras para reforzar su resiliencia digital.

A continuación se presenta una revisión esquemática de la adaptación nacional a estas normas europeas.

2.2. Marco Nacional: Estrategia y regulación para la protección del entorno digital

En España, la ciberseguridad ha dejado de ser un asunto exclusivamente técnico para convertirse en un eje transversal de las políticas públicas en materia digital. La **Estrategia Nacional de Ciberseguridad de 2019** configura una visión integral que se articula en torno a cinco grandes objetivos, entre los que destacan la protección del tejido empresarial, el fortalecimiento de las capacidades y la cooperación público-privada. Esta estrategia se alinea con la **Estrategia de Seguridad Nacional 2021**, que reconoce la ciberseguridad como uno de los principales desafíos para la defensa y estabilidad del Estado.

Como instrumento de ejecución, el Gobierno de España ha reforzado el papel de los organismos técnicos especializados. El más destacado es el Instituto Nacional de Ciberseguridad (en adelante, **INCIBE**), que presta servicios de respuesta ante incidentes, facilita herramientas de autodiagnóstico, impulsa la formación y ofrece apoyo a las empresas. Junto con el Centro Criptológico Nacional (en adelante, **CCN-CERT**), INCIBE integra la **estructura operativa de vigilancia y respuesta frente a amenazas y vulnerabilidades en el ciberespacio.**

En el plano normativo, el marco español se ha consolidado mediante la **aprobación de diversas leyes y reglamentos**. En este contexto, conviene destacar las siguientes disposiciones especialmente relevantes para el ámbito empresarial, y de manera particular para el sector comercial:

[4] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) Nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

Real Decreto 311/2022, de 3 de mayo[5], por el que se aprueba el nuevo Esquema Nacional de Seguridad (ENS), establece los principios básicos y los requisitos mínimos de seguridad que deben cumplir las administraciones públicas y las entidades que prestan servicios digitales esenciales.

- Su Anexo II recoge más de 80 medidas de seguridad, de carácter técnico, organizativo y físico, que constituyen una referencia esencial para garantizar la protección de los sistemas y la información.
- Este marco resulta particularmente relevante para los comercios que prestan servicios online a través de plataformas digitales.

El Real Decreto-ley 12/2018, de 7 de septiembre[6], y el Real Decreto 43/2021, de 26 de enero[7], constituyen el eje normativo de la ciberseguridad en el ámbito nacional, al materializar la transposición de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, mencionada en el apartado anterior.

- Ambas normas introducen la obligación de notificar los incidentes de seguridad y de aplicar medidas de protección basadas en la gestión de riesgos.
- El Real Decreto 43/2021 amplía y desarrolla estas obligaciones, extendiéndolas a los proveedores de servicios digitales, entre los que se incluyen las plataformas de comercio electrónico y los servicios de almacenamiento en la nube.

Ley 8/2011, de 28 de abril[8], y el Real Decreto 704/2011, de 20 de mayo[9], establecen el marco regulador para la protección de las infraestructuras críticas, incluyendo aquellas de naturaleza digital.

- Estas normas definen la figura del operador crítico y establecen la obligación de elaborar Planes de Seguridad del Operador (PSO) y Planes de Protección Específicos (PPE).
- Si bien la mayoría de los comercios no se encuadra dentro de esta categoría, los grandes operadores logísticos y de distribución pueden verse afectados por estas disposiciones.

Ley Orgánica 3/2018, de 5 de diciembre[10], adapta el Reglamento General de Protección de Datos (RGPD) al ordenamiento jurídico español y regula los denominados derechos digitales, entre los que destacan el derecho a la desconexión laboral, la protección de los menores en Internet y la portabilidad de los datos personales.

- Constituye un referente europeo en materia de integración normativa, al incorporar los principios de responsabilidad proactiva y el enfoque basado en el riesgo, que resultan de aplicación a todas las empresas que tratan datos personales, incluidas las del ámbito comercial.

[5] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

[6] Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

[7] Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

[8] Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

[9] Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

[10] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ley 11/2022, de 28 de junio, General de Telecomunicaciones

- Incorpora requisitos específicos relativos a la seguridad de las redes y de los servicios, y refuerza la obligación de colaboración con las autoridades competentes en caso de incidentes de ciberseguridad.

Este conjunto de medidas configura un entorno normativo sólido, en el que la ciberseguridad empresarial se aborda no solo desde la perspectiva del cumplimiento normativo, sino también a través de la formación, la sensibilización y el desarrollo de capacidades adaptadas a las pequeñas y medianas empresas.

Conviene recordar, además, que, dentro de este marco, las **comunidades autónomas** desempeñan un papel clave en la adaptación e implementación de estas políticas a su realidad social y productiva.

2.3. Contexto Autonómico: La Estrategia Andaluza de Ciberseguridad 2022–2025

La Administración de la Junta de Andalucía ha asumido con determinación su papel en el impulso de la ciberseguridad. Consciente de los retos específicos que presenta la economía andaluza, en 2022 se presentó la **Estrategia Andaluza de Ciberseguridad 2022-2025**. Este documento no solo adapta las directrices europeas y nacionales al contexto regional, sino que propone acciones concretas orientadas al desarrollo de capacidades, la protección del entorno digital y el fomento de una cultura de ciberseguridad entre los actores públicos y privados.

La Estrategia se estructura en diez objetivos estratégicos, entre los que destaca especialmente el **Objetivo Estratégico n.º 8: "Mejorar la cultura y las buenas prácticas de ciberseguridad**". Este eje articula una línea de actuación centrada en la **sensibilización y formación de la ciudadanía, las empresas y las administraciones públicas** sobre los riesgos y responsabilidades en materia de ciberseguridad. Se trata de una apuesta por la prevención y la concienciación, basada en la idea de que el factor humano continúa siendo uno de los eslabones más vulnerables de la cadena de seguridad digital.

Entre las líneas de actuación vinculadas a este objetivo se incluyen:

- La organización de campañas públicas de sensibilización, en colaboración con medios de comunicación, centros educativos y organizaciones empresariales.
- El fomento de las buenas prácticas en el uso de las Tecnologías de la Información y la Comunicación (TIC) en la actividad empresarial cotidiana.
- La promoción de herramientas de diagnóstico y autoevaluación para pymes.
- La creación de un ecosistema de colaboración público-privada que conecte a instituciones, proveedores tecnológicos, asociaciones sectoriales y centros de innovación.

Además, la Estrategia pone de relieve la importancia de la ciberseguridad **como elemento habilitador de la transformación digital de la economía andaluza**. Esto significa que no se aborda únicamente como una obligación legal o técnica, sino también como una oportunidad para reforzar la competitividad, la confianza y el valor añadido de los productos y servicios. En este sentido, la Estrategia incluye acciones destinadas a atraer talento, fortalecer la capacitación de los profesionales TIC y posicionar a Andalucía como un nodo avanzado de ciberseguridad en el sur de Europa.

Este marco autonómico constituye la base de programas o instrumentos más específicos, como aquellos dirigidos al sector comercial a través del VII Plan Integral de Fomento del Comercio Interior de Andalucía.

Ideas de síntesis

- El recorrido institucional a través de los niveles europeo, estatal y autonómico permite comprender que la ciberseguridad ha dejado de ser un elemento accesorio para consolidarse como un componente esencial de toda estrategia de desarrollo económico. Desde las grandes directrices europeas hasta las actuaciones más específicas en el ámbito andaluz, el mensaje es claro: *sin seguridad digital no hay transformación digital posible*.

- La implicación activa de las instituciones en la protección del entorno digital, junto con la sensibilización del conjunto del tejido empresarial y, en particular, del pequeño comercio, constituye ya un eje estructural de las políticas públicas en materia de digitalización.

3. Descripción didáctica de las ciberamenazas y medidas de protección

3.1. Introducción

La digitalización ha transformado de manera profunda la forma en que los comercios se relacionan con sus clientes y gestionan su actividad. Esta evolución ha generado grandes oportunidades, pero también nuevas incertidumbres y riesgos. Uno de los más relevantes, y a menudo menos comprendido, es el relacionado con la **seguridad en el entorno digital**.

Desde la gestión de cobros y envíos hasta la comunicación con proveedores o la promoción de productos en redes sociales, prácticamente todas las acciones cotidianas de un comercio pueden verse afectadas por **amenazas digitales** si no se aplican las precauciones adecuadas. Por ello, antes de abordar las medidas concretas de protección, conviene detenerse a comprender qué son las **ciberamenazas**, cómo actúan y por qué tienen un impacto particular en el sector comercial.

El propósito de esta sección es **acompañar al profesional del comercio** en la comprensión de las principales amenazas digitales a las que se enfrenta en su actividad, sin necesidad de contar con conocimientos técnicos avanzados. No se trata de un manual para especialistas ni de un compendio normativo, sino de una **sección divulgativa y estructurada**, diseñada para ayudar a **identificar riesgos reales y ofrecer soluciones prácticas**.

Para ilustrar estas cuestiones, se presenta una clasificación sencilla inspirada en la propuesta del **Instituto Nacional de Ciberseguridad (INCIBE, 2023)**, que agrupa las ciberamenazas en dos grandes categorías:

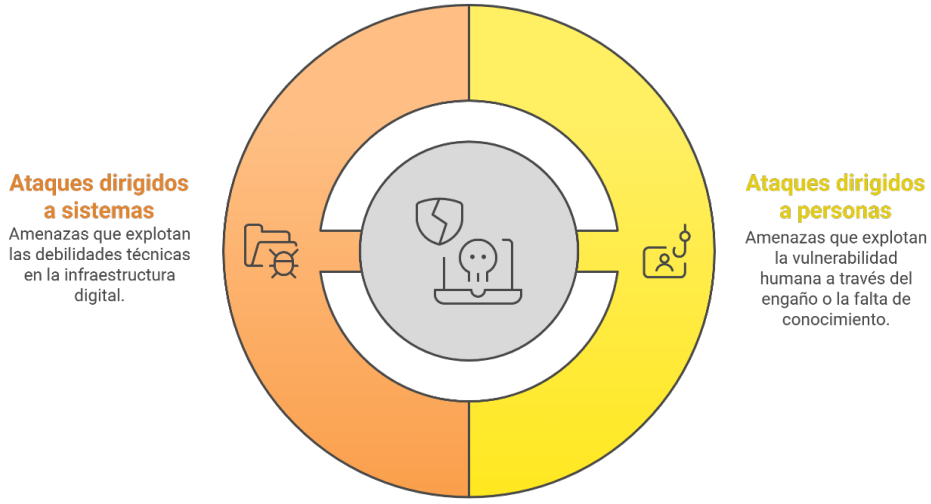
- **Ciberamenazas o ataques dirigidos contra las personas**, que se basan en el engaño, el descuido o la falta de conocimiento de quienes utilizan la tecnología. Incluyen fraudes, suplantaciones de identidad, *phishing* o manipulaciones de tipo social.
- **Ciberamenazas o ataques dirigidos contra los sistemas**, que buscan aprovechar debilidades técnicas en los equipos, programas, redes o páginas web, como virus, *ransomware*, accesos no autorizados o fallos de configuración.

Además de describir cada uno de estos grupos, la sección propone, a modo de ejemplo, un conjunto de **medidas de protección básicas y avanzadas**, alineadas con las contempladas en la **Orden de 3 de octubre de 2024**[11], que establece ayudas específicas para la implantación de soluciones de ciberseguridad en el sector comercial. Entre ellas destacan herramientas como **antivirus, cortafuegos, gestión de accesos, copias de seguridad, cifrado de datos** o **sistemas de autenticación fuerte**.

En resumen, esta sección constituye un **punto de partida práctico** para la reflexión individual de cada negocio: ¿qué está haciendo hoy mi comercio para protegerse?, ¿qué puede mejorar sin necesidad de grandes inversiones? y, sobre todo, ¿cómo puedo asegurar que mi actividad continúe con normalidad, sin incidentes ni interrupciones?

[11] Orden de 3 de octubre de 2024, por la que se aprueban las bases reguladoras para la concesión de subvenciones, en régimen de concurrencia no competitiva, destinadas a mejorar la competitividad y la digitalización del sector comercial y artesano en Andalucía.

Figura 1. Grupos de ciberamenazas



Fuente: Elaboración propia

3.2. ¿Qué son las ciberamenazas?

A diario usamos internet para gestionar tareas del negocio: enviar correos, cobrar con tarjeta, subir productos a la web o contactar con clientes. Todo parece funcionar con naturalidad, pero detrás de esa actividad cotidiana existen riesgos reales que no siempre se perciben. Esos riesgos, cuando están relacionados con el uso de tecnología, se conocen como **ciberamenazas**.

Una ciberamenaza es, en esencia, **cualquier peligro que pueda poner en riesgo los sistemas informáticos, los datos o los servicios digitales de una empresa**. Puede tratarse de un virus, de un intento de estafa a través del correo electrónico, de un acceso no autorizado a los equipos o de un ataque que bloquee una web de ventas durante horas. Algunas de estas amenazas son muy sofisticadas, pero muchas otras se aprovechan de errores comunes, como emplear contraseñas débiles o hacer clic en un enlace engañoso.

Este concepto está estrechamente relacionado con lo que la norma **ISO/IEC 27000** define como amenazas a la seguridad de la información, entendida como "la preservación de la **confidencialidad, integridad y disponibilidad de la información**". Estos tres principios constituyen los pilares esenciales que deben protegerse en cualquier organización (ISO/IEC, 2022).

Con frecuencia se piensa que este tipo de amenazas solo afecta a grandes empresas, pero lo cierto es que los **pequeños comercios son especialmente vulnerables**. Los ciberdelincuentes buscan objetivos fáciles, y muchas veces los encuentran en negocios que no cuentan con sistemas de protección adecuados ni con conocimientos o formación especializada.

Además, se debe tener en cuenta que los efectos negativos de una ciberamenaza no siempre se manifiestan de inmediato. Por ejemplo, un correo fraudulento puede pasar inadvertido hasta

que se detecta un cobro no autorizado semanas después, o un virus puede permanecer oculto en el sistema sin mostrar señales hasta que ya es demasiado tarde.

Por esta razón, además de diseñar protocolos de actuación para **recuperarnos** tras una ciberamenaza (*reacción*), debemos intentar **evitar que llegue a producirse** (*prevención*).

Ideas de síntesis

- Una ciberamenaza no es un asunto técnico alejado del día a día de un comercio. Es un riesgo real, que puede interrumpir las ventas, afectar la reputación del negocio, o incluso suponer un incumplimiento legal si se ven afectados los datos personales de clientes o proveedores.
- La buena noticia es que prevenir estos problemas está en muchas ocasiones al alcance de cualquier empresa, siempre que sepa identificarlos y aplicar unas pautas mínimas de protección y protocolos que nos permitan reaccionar rápidamente y recuperarnos en caso de que se hagan realidad.

3.3. ¿Por qué afectan especialmente al sector comercial?

El comercio, tanto en sus actividades minoristas como mayoristas, ha experimentado en los últimos años una **transformación digital profunda**. Se han incorporado sistemas de pago electrónicos, plataformas *online*, redes sociales para la promoción y venta, software de gestión conectado, canales de comunicación digital con proveedores, procesos automatizados en la red, etc. Todo ello ha generado **enormes ventajas competitivas**, pero también ha incrementado la **exposición a riesgos digitales**.

Este sector presenta una serie de características que lo hacen **especialmente sensible a las ciberamenazas**, como puede ser la interacción constante con los clientes o la relación de confianza como activo esencial del negocio. A ello se suma que muchos establecimientos utilizan tecnologías conectadas sin los niveles de protección adecuados y carecen de personal especializado en materia de seguridad digital.

A estas circunstancias se suma un aspecto clave recogido en la **norma ISO/IEC 27002:2022**, que señala que las amenazas no solo afectan a los sistemas internos, sino también a todo el **ecosistema en el que la organización opera**: clientes, proveedores, empleados y socios estratégicos. Un comercio puede convertirse en la **puerta de entrada de un ataque más amplio** si su seguridad no está correctamente gestionada (ISO/IEC, 2022). En otras palabras, cualquier negocio puede ser tanto el **objetivo directo** de una ciberamenaza como el **canal de acceso** hacia otros agentes, como proveedores, clientes o colaboradores.

Por ejemplo, una web comercial mal protegida puede ser utilizada para **alojar una campaña de suplantación de identidad**, afectando tanto a los consumidores como a otras marcas. Del mismo modo, un correo hackeado desde la cuenta del comercio puede servir para estafar a **proveedores habituales**.

Figura 2. Vulnerabilidades del comercio a las ciberamenazas

Fuente: Elaboración propia

Ideas de síntesis

- Los ataques pueden tener múltiples objetivos, y el comercio puede ser víctima, canal o punto de partida.
- Hablar de ciberseguridad en el comercio no es hablar de informática, es hablar de continuidad del negocio, de imagen, de responsabilidad legal y de confianza.

3.4. Taxonomía de las ciberamenazas.

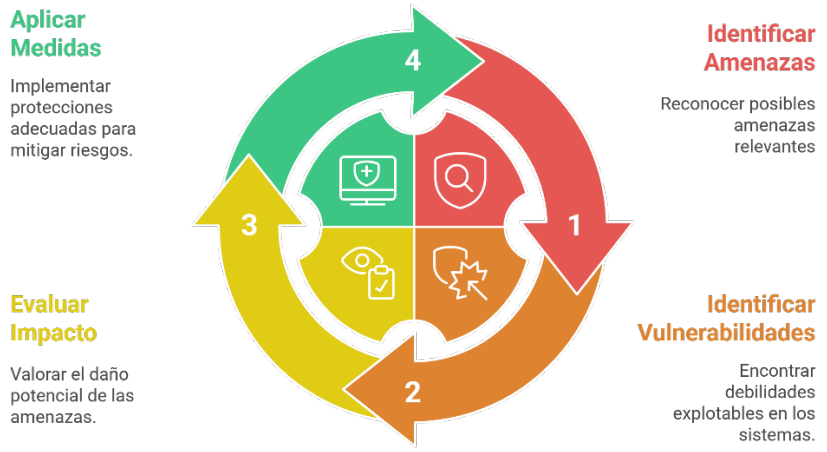
Esta sección tiene por objetivo **definir y describir** las principales ciberamenazas a las que se enfrentan los agentes que operan en el sector comercial, ofreciendo un marco que facilite su identificación precisa e integre las referencias de los estándares internacionales y nacionales, con el fin de aportar una visión completa y contextualizada.

De acuerdo con la norma **ISO/IEC 27000**, una **ciberamenaza** se define formalmente como "***una causa potencial de un incidente no deseado que puede provocar daños a un sistema o a la organización***". En otras palabras, una amenaza es cualquier circunstancia o evento con capacidad para **comprometer la seguridad de la información o de los sistemas** de una empresa. Estas amenazas pueden tener **orígenes diversos**: causas naturales (por ejemplo, desastres que afectan a infraestructuras), causas accidentales (errores humanos involuntarios) o actos intencionados de terceros con motivación maliciosa, como fraudes o ataques dirigidos (INCIBE, 2021b).

Lo relevante es que, si una amenaza llega a materializarse aprovechando una **vulnerabilidad** existente, es decir, una debilidad en los usuarios, sistemas o procesos, puede desencadenar un **incidente de seguridad** con consecuencias negativas para la organización.

En este sentido, la gestión de riesgos en ciberseguridad se basa en un proceso estructurado que permite identificar, analizar y tratar los riesgos de manera sistemática. En la siguiente figura se representa de forma esquemática este ciclo de gestión.

Figura 3. Ciclo de gestión de riesgos en ciberseguridad



Fuente: Elaboración propia

En este contexto, la **Estrategia Andaluza de Ciberseguridad 2022-2025** señala que la creciente interconexión digital y la distribución masiva de datos han incrementado la **exposición a vulnerabilidades y amenazas**, las cuales son "*cada vez más complejas, difíciles de detectar, contener y resolver*". Esto implica que las empresas, incluidas las del sector comercial minorista y mayorista, operan en un entorno donde **surgen continuamente nuevas formas de ataque y fraude digital**.

La Estrategia también subraya la necesidad de fomentar la **cibercultura y la preparación**, indicando que el crecimiento de sistemas tecnológicos cada vez más complejos y abiertos obliga a **reforzar la seguridad** para hacer frente a las amenazas **emergentes** derivadas de la digitalización. Por tanto, **conocer las principales ciberamenazas y sus métodos de ataque resulta esencial** para prevenir incidentes y proteger la continuidad del negocio.

Desde una perspectiva general, las ciberamenazas pueden clasificarse según diversos criterios: origen, motivación u objetivo. En esta sección se adopta una **taxonomía práctica**, que las agrupa según su **vector principal de ataque**, siguiendo la clasificación propuesta por **INCIBE**: (i) amenazas dirigidas contra las personas; (ii) amenazas que se dirigen contra los sistemas tecnológicos.

Ideas de síntesis

- Organismos como INCIBE advierten que ningún negocio es demasiado pequeño para ser víctima: los ciberdelincuentes atacan tanto a grandes empresas como a pymes y autónomos, aprovechando cualquier debilidad para alcanzar sus objetivos fraudulentos.

3.4.1. Ciberamenazas a través de las personas

Las amenazas dirigidas a las personas constituyen una de las formas más frecuentes y efectivas de ataque en el ámbito de la ciberseguridad. En lugar de explotar una vulnerabilidad técnica, los atacantes buscan **manipular a los propios usuarios, aprovechando la confianza o el desconocimiento.** Este tipo de amenazas se apoya en técnicas de ingeniería social, que apelan a las emociones, la urgencia o a la autoridad para inducir a las víctimas a realizar acciones que comprometen la seguridad del sistema.

Entre las modalidades más habituales encontramos:

- **Phishing (fraude por email):** uno de los métodos más comunes. Consiste en el envío masivo de correos electrónicos que simulan provenir de fuentes legítimas, como bancos, proveedores o plataformas de pago. Estos mensajes incluyen enlaces a sitios falsos que imitan a los originales, con el objetivo de obtener credenciales o información confidencial.

- **Vishing y smishing (fraude por llamada o mensaje):** variantes del phishing. El vishing utiliza llamadas telefónicas para engañar a la víctima, por ejemplo, haciéndose pasar por un soporte técnico. El smishing emplea mensajes de texto (SMS) con enlaces maliciosos o instrucciones engañosas.

- **Fraude del proveedor o del CEO:** ataque dirigido a personas con responsabilidades en pagos o gestión financiera. El atacante suplanta a un alto cargo o a un proveedor habitual para solicitar transferencias urgentes o cambios en los datos bancarios. Suele apoyarse en correos bien redactados y en un conocimiento previo del entorno empresarial.

- **Baiting (fraude mediante dispositivo perdido):** se basa en la curiosidad o el descuido. Un ejemplo típico es dejar una memoria USB infectada en un lugar visible. Cuando un empleado la conecta al sistema, se ejecuta un malware que permite al atacante acceder de forma remota al equipo o a la red.

- **Suplantación en redes sociales:** consiste en crear perfiles falsos que simulan ser empleados, clientes o socios de la empresa. A través de estas cuentas, los atacantes establecen contacto con personas del entorno profesional para obtener información sensible o lanzar otros tipos de fraude.

Estas técnicas demuestran que la seguridad no depende únicamente de las herramientas tecnológicas, sino también del comportamiento humano. Por ello, la **formación y la concienciación del personal** son factores fundamentales para reducir el riesgo y reforzar la protección frente a este tipo de amenazas.

Ejemplos comunes en comercios

	Tienda minorista: un trabajador recibe un correo que aparenta proceder de su banco habitual. El mensaje advierte de un supuesto problema con la cuenta de la empresa y solicita una verificación urgente. Al acceder al enlace incluido, el empleado es redirigido a una página falsa donde introduce sus credenciales, facilitando así el acceso de los atacantes a las cuentas corporativas.
	Comercio mayorista: el departamento de contabilidad recibe una notificación, aparentemente enviada por un proveedor habitual, en la que se informa de un cambio en el número de cuenta para el pago de facturas. El mensaje, redactado con apariencia profesional y convincente, induce a realizar una transferencia que en realidad se dirige a una cuenta controlada por ciberdelincuentes.
	Tienda online: un cliente recibe un mensaje de texto tras realizar una compra, con un enlace que invita a verificar los datos del pedido. Al acceder al enlace, se descarga un programa malicioso que compromete su dispositivo y puede afectar a su privacidad o a la seguridad de su información bancaria.

Estos casos evidencian la necesidad de establecer protocolos internos de verificación, formar al personal en la identificación de amenazas y fomentar entre los clientes una cultura de precaución digital. La prevención es mucho más efectiva que la reacción una vez se ha producido el daño.

Impactos y consecuencias

Los ataques dirigidos a las personas pueden tener consecuencias graves y multidimensionales (económicas, operativas, reputacionales,…). Aunque en muchos casos la acción inicial pueda parecer insignificante, sus efectos pueden propagarse con rapidez a otros sistemas o llegar a afectar a terceros.

Uno de los riesgos más comunes es la **pérdida de datos sensibles**, como contraseñas, información bancaria o datos personales de clientes. Este tipo de filtraciones puede dar lugar a accesos no autorizados a plataformas internas, comprometiendo la confidencialidad y la integridad de la información.

Otro impacto habitual es el **fraude económico**. Cambios de cuentas no verificados, pagos a destinatarios fraudulentos o el uso de tarjetas robadas pueden ocasionar pérdidas económicas importantes para la empresa (u otros usuarios como clientes y proveedores), con dificultades para su recuperación posterior.

Asimismo, estos incidentes repercuten directamente en la **reputación del negocio**. Un cliente que percibe que sus datos han sido mal gestionados puede perder la confianza en ese comercio y optar por no volver a comprar, algo especialmente relevante en sectores con una fuerte competencia.

Por último, se deben tener en cuenta las **consecuencias legales**. La normativa vigente en protección de datos personales (Ley Orgánica 3/2018, de 5 de diciembre y Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016) establece la obligación de notificar brechas de seguridad y contempla sanciones económicas importantes en caso de negligencia. Así, **un incidente de este tipo no solo implica una pérdida operativa, sino también un posible procedimiento administrativo**.

Ideas de síntesis

- La gestión adecuada de estos riesgos exige una combinación de medidas técnicas, organizativas y formativas. Conocer el alcance de las amenazas dirigidas a las personas es el primer paso para construir un entorno comercial digital más seguro.

3.4.2. Ciberamenazas a través de los sistemas

Además de los ataques que buscan manipular a las personas, existen ciberamenazas que se dirigen directamente a los sistemas tecnológicos de la empresa (hardware, software o comunicaciones). Estas amenazas suelen aprovechar debilidades técnicas o errores de configuración para acceder a los datos, alterar servicios o inutilizar infraestructuras. En este caso, el atacante no necesita interactuar con los empleados, basta con explotar un fallo del sistema o una medida de seguridad insuficiente.

Las principales tipologías de este tipo de amenazas incluyen:

- **Malware:** Se trata de software malicioso diseñado para causar daños o tomar el control del sistema. Entre las variantes más peligrosas se encuentra el *ransomware*, que cifra los archivos de un equipo o servidor y exige un rescate económico para recuperarlos. También son comunes los troyanos o los programas espía, capaces de recopilar información sin el consentimiento del usuario.

- **Accesos no autorizados:** También conocidos como intrusiones, consisten en el ingreso indebido a los sistemas informáticos mediante técnicas como la fuerza bruta (prueba masiva de contraseñas), la explotación de vulnerabilidades o el uso de credenciales robadas. Una vez dentro, los atacantes pueden moverse libremente, instalar puertas traseras o extraer información.

- **Ataques web:** Las páginas web con una configuración débil pueden ser vulnerables a distintas técnicas. Una de las más comunes es la *inyección SQL*, que permite modificar los datos almacenados en una base de datos on line. Por ejemplo, un ciberdelincuente podría cambiar los precios de los productos o crear un usuario con privilegios de administrador para acceder a toda la información del sistema. Otro método frecuente es el *cross-site scripting (XSS)*, que inserta código malicioso en la web (por ejemplo, un pequeño programa que envía contraseñas al atacante) y posibilita el robo de información, la manipulación del contenido o el control de la web.

- **Denegación de servicio distribuida (DDoS):** en este tipo de ataque, miles de equipos infectados envían solicitudes masivas a una web hasta saturarla y hacer que deje de funcionar. Aunque no implica robo de información, su finalidad es interrumpir la actividad del comercio y provocar pérdidas operativas.

Todas estas amenazas requieren **medidas de protección robustas y actualizadas, así como una monitorización constante de la red y los sistemas**. En muchos casos, su aparición puede evitarse mediante buenas prácticas básicas y herramientas de seguridad accesibles, de bajo coste, y sencillas de instalar y mantener en cualquier pyme o comercio.

Ejemplos comunes en comercios

	En una **tienda online** que no mantiene actualizada su página web, por ejemplo porque no dispone de las versiones más recientes de los complementos (plugin) usados para la venta online o porque no actualiza periódicamente el sistema de gestión de contenidos (CMS) para incluir nueva información en su página web, aumenta el riesgo de sufrir un ataque de inyección SQL. En este tipo de ataque, un ciberdelincuente aprovecha las debilidades del sistema para acceder a la base de datos donde se almacenan los datos de clientes, productos o pedidos, lo que puede tener consecuencias legales y comerciales muy graves.
	Un **empleado** conecta a la red corporativa una memoria USB infectada, ejecuta sin saberlo un archivo infectado recibido por correo electrónico o pulsa un botón en una página web insegura que activa un software malicioso. En estos casos, si no existe un sistema antivirus activo o medidas de control de dispositivos externos, el equipo queda comprometido y podría activarse un *ransomware* que cifra todos los archivos de la empresa, exigiendo un pago para su recuperación.
	Durante **campañas de alta demanda**, como las rebajas o la temporada de Navidad, algunas tiendas pueden sufrir ataques de denegación de servicio distribuida (DDoS) que saturan su web y la dejan fuera de funcionamiento durante horas. Esta interrupción no solo afecta a las ventas, sino también a la confianza de los clientes en la fiabilidad del comercio.

Estos casos muestran que las amenazas técnicas no son fenómenos abstractos ni exclusivos de las grandes empresas. La falta de medidas básicas de seguridad puede convertir cualquier sistema mal configurado en una puerta abierta para los atacantes.

Impactos y consecuencias

Las consecuencias de los ataques a sistemas pueden extenderse mucho más allá del momento puntual del incidente. De hecho, un fallo técnico no resuelto puede traducirse en **daños estructurales**, interrupciones prolongadas y pérdida de oportunidades de negocio.

Desde el punto de vista técnico, este tipo de ataques puede provocar la pérdida de información, la inutilización de servidores o la necesidad de formatear equipos y reinstalar aplicaciones. En muchos casos es necesario recurrir a especialistas externos para identificar el origen del ataque y restaurar el sistema con las debidas garantías.

En el plano **operativo**, una tienda que no puede facturar, atender pedidos o realizar cobros por culpa de un ciberataque sufre un daño directo. Además, el personal puede verse sobrecargado al tener que resolver el incidente sin recursos adecuados, generando retrasos, malestar interno y quejas de clientes.

Los **efectos legales** también son cada vez más relevantes. Si el ataque implica el acceso o pérdida de datos personales, la empresa debe notificar el incidente a la Agencia Española de Protección de Datos y puede enfrentar sanciones. Del mismo modo, proveedores o clientes afectados pueden reclamar responsabilidades si se considera que no se aplicaron medidas razonables de protección.

Ideas de síntesis

- Proteger los sistemas no es solo una cuestión técnica, sino una necesidad estratégica para garantizar la continuidad del negocio, su reputación y su cumplimiento normativo. La inversión en ciberseguridad debe entenderse como un coste preventivo que evita pérdidas mucho mayores.

3.4.3. ¿Cuáles son las amenazas actuales en el sector comercial?

Una vez expuestas las principales categorías de ciberamenazas y sus efectos, resulta útil considerar los análisis realizados por organismos especializados en el seguimiento de riesgos emergentes. En este sentido, la *European Union Agency for Cybersecurity* (ENISA), agencia de la Unión Europea encargada de reforzar la ciberseguridad a nivel comunitario, elabora de forma periódica informes de referencia que identifican y evalúan las amenazas más relevantes en el

A partir del **informe *ENISA Threat Landscape 2024***, elaborado con datos comprendidos entre julio de 2023 y junio de 2024, **se presenta una tabla de síntesis** que ofrece una visión general de las ciberamenazas más frecuentes en el ámbito de la Unión Europea, **con una adaptación específica al sector comercial**.

Tabla 1. Principales ciberamenazas con impacto en el sector comercial

Ciberamenaza	Subsector Comercial	Ejemplos	Particularidades
Ransomware	Retail, Proveedores de Servicios Digitales	Lockbit, Cl0p, Play	Pérdidas económicas, interrupciones operativas
Malware	Retail, eCommerce	Redline, Raccoon, Lumma	Robo de credenciales, infiltración de sistemas
Phishing / Ingeniería Social	Retail	BEC, smishing con suplantación de logística o pagos	Fraudes, robo de datos de clientes
Amenazas contra datos	Todos con gestión de datos personales / pagos	Data breach, fuga de tarjetas	Infracciones RGPD, impacto reputacional
Manipulación de información	Grandes cadenas o marcas con exposición digital	Campañas FIMI en redes sociales	Afectación reputacional, boicots

Fuente: Adaptación de ENISA Threat Landscape 2024

3.5. Medidas de protección

Tras el análisis de las principales ciberamenazas, esta sección tiene como finalidad ofrecer, de manera clara y accesible, las soluciones de seguridad esenciales que todo establecimiento debería considerar al diseñar sus sistemas de protección digital. Estas medidas no solo cuentan con el respaldo de los principales organismos especializados en ciberseguridad, sino que también forman parte de los objetivos y actuaciones contempladas en la **Orden de 3 de octubre de 2024**, destinada a impulsar la competitividad y la digitalización del sector comercial y artesano andaluz. A través de una combinación equilibrada entre tecnología, buenas prácticas y conocimiento, se puede construir un entorno más seguro, resiliente y sostenible frente a los desafíos digitales actuales.

Antivirus y antimalware

El uso de antivirus y programas antimalware constituye la base de la protección digital. Estas herramientas están diseñadas para detectar, bloquear y eliminar software malicioso, como virus, troyanos (programas malintencionados camuflados), *spyware* (programas espía) o *ransomware* (software que secuestra o cifra datos), antes de que puedan causar daños en los sistemas. Su funcionalidad no se limita a escanear archivos, sino que muchas soluciones modernas ofrecen protección en tiempo real, vigilancia del comportamiento de los programas y aislamiento de amenazas potenciales, incluyendo la navegación por internet.

Complejidad de implementación	**Bajo.** La instalación de un antivirus es sencilla y no requiere conocimientos técnicos avanzados. Cualquier pequeño comercio puede implementarlo sin dificultad. Es recomendable instalar este tipo de solución en todos los equipos que tengan acceso a Internet o almacenen información relevante.
Coste	**Bajo.** Existen soluciones gratuitas de calidad y versiones comerciales con un coste reducido.

Cortafuegos (Firewall)

El cortafuegos es una herramienta que filtra el tráfico de red, permitiendo solo las conexiones autorizadas y bloqueando las que resulten sospechosas. Su función principal es evitar accesos no deseados desde el exterior, protegiendo así los sistemas del comercio frente a intrusiones o comunicaciones maliciosas. En términos sencillos, el *firewall* actúa como una puerta blindada que protege la red del negocio.

 **Complejidad de implementación**	**Medio.** Algunos sistemas operativos incorporan cortafuegos preinstalados, pero su configuración adecuada puede requerir ciertos conocimientos sobre redes.
 **Coste**	**Medio.** El coste depende del tipo de solución elegida: los cortafuegos por software suelen ser más económicos, mientras que los dispositivos dedicados (hardware) implican una inversión mayor. En cualquier caso, la mayoría de los routers suministrados por las compañías de telecomunicaciones incluyen cortafuegos integrados. Su correcta activación y configuración resulta especialmente importante en entornos donde se gestionan datos de clientes o se utilizan servidores propios.

Sistemas de detección y prevención de intrusiones (IDS/IPS)

Los sistemas IDS (*Intrusion Detection System*) e IPS (*Intrusion Prevention System*) se utilizan para monitorizar continuamente el tráfico de red y detectar patrones que puedan indicar la presencia de un ataque. Mientras que el IDS genera alertas ante comportamientos sospechosos, el IPS va un paso más allá, actuando para bloquear automáticamente la amenaza. En términos sencillos, el IDS actúa como un sistema reactivo que detecta y avisa, mientras que el IPS es proactivo, ya que interviene para detener el ataque. Ambos funcionan como un control de acceso digital que supervisa lo que entra y sale de la red del comercio.

 **Complejidad de implementación**	**Alto.** Se trata de una solución avanzada que requiere conocimientos técnicos específicos para su instalación y configuración adecuadas. En la mayoría de los casos será necesario contar con asesoramiento o apoyo de personal especializado.
 **Coste**	**Medio o alto.** Este tipo de soluciones suele tener un coste más elevado que las anteriores, especialmente si se recurre a soluciones comerciales avanzadas. No obstante, para empresas con cierta infraestructura digital, representa un nivel adicional de protección muy valioso.

Gestión de parches y actualizaciones

Mantener el software actualizado es una de las formas más efectivas y sencillas de prevenir brechas de seguridad. Muchas amenazas conocidas explotan vulnerabilidades ya identificadas, por lo que la instalación de parches y actualizaciones reduce de forma significativa la exposición del sistema. Esta rutina debe ser idéntica a la de mantener nuestro negocio limpio y en perfectas condiciones.	
 **Complejidad de implementación**	**Bajo.** Su implementación es muy sencilla y puede automatizarse en la mayoría de los sistemas operativos y programas. La supervisión periódica de las actualizaciones garantiza que todos los dispositivos se mantengan protegidos frente a las amenazas más recientes.
 **Coste**	**Bajo.** En la mayoría de los casos, las actualizaciones y parches son gratuitos, salvo cuando se incorporan funcionalidades extra que implican un coste adicional. Se recomienda incluir la revisión de actualizaciones dentro de las rutinas habituales de mantenimiento, especialmente en entornos donde existan varios dispositivos conectados.

Control de acceso y autenticación (incluye autenticación multifactor - MFA).

El control de acceso garantiza que únicamente las personas autorizadas puedan utilizar la información y a los sistemas críticos del negocio. Se basa en la asignación de perfiles de usuario y en el uso de credenciales seguras, lo que normalmente conocemos como nombres de usuario y contraseñas robustas. Para reforzar esta protección se recomienda implementar la autenticación multifactor (MFA), que añade un segundo paso de verificación, como un código enviado al teléfono móvil o al correo electrónico. En otras palabras, es como una llave física que abre nuestro negocio, pero en este caso, supone tener varias cerraduras.	
 **Complejidad de implementación**	**Medio.** Requiere configurar cuentas de usuario, definir políticas de contraseñas y activar opciones adicionales de seguridad.
 **Coste**	**Bajo o medio, en función de la solución elegida.** Existen numerosas herramientas de autenticación multifactor gratuitas, así como otras de pago con diferentes niveles de servicio y funcionalidad. Este tipo de soluciones resulta especialmente útil para proteger accesos a correos electrónicos, aplicaciones de facturación o paneles de administración web.

Cifrado de datos (en datos almacenados y transferencia de datos)

El cifrado protege la confidencialidad de la información almacenada o transmitida, transformándola en un formato que solo puede ser leído por quienes disponen de la clave adecuada. En el ámbito del comercio electrónico, por ejemplo, el uso de protocolos HTTPS garantiza que los datos introducidos por los clientes viajen cifrados y no puedan ser interceptados por terceros. Estos sistemas de cifrados no implican que la persona usuaria deba realizar labores de encriptación o cálculos, simplemente son protocolos que deben habilitarse en el diseño e implantación de nuestros sistemas para que sean más seguros.

 **Complejidad de implementación**	**Medio.** Aunque el uso cotidiano del cifrado no afecta a las personas usuarias, su correcta implantación exige configurar certificados digitales o activar funciones específicas en los dispositivos y aplicaciones. Estas tareas pueden requerir un nivel básico de conocimientos técnicos o el apoyo de personal especializado.
 **Coste**	**Bajo o medio, en función de la solución elegida.** El cifrado de discos suele estar integrado en la mayoría de los sistemas operativos, mientras que la obtención de certificados SSL para páginas web puede implicar un coste anual reducido. En cualquier caso, se trata de una inversión recomendable para salvaguardar los datos sensibles.

Copias de seguridad y recuperación de datos ante incidentes

Realizar copias de seguridad periódicas permite recuperar la información en caso de pérdida, fallo del sistema o ataque informático. Esta medida es esencial para garantizar la continuidad del negocio y evitar pérdidas irreversibles de datos. Se recomienda aplicar la regla **3-2-1**, que consiste en mantener tres copias de la información, almacenadas en dos formatos diferentes y al menos una de ellas en una ubicación distinta, como un servicio en la nube.

 **Complejidad de implementación**	**Medio.** Su correcta aplicación requiere cierta planificación, ya que es necesario decidir qué datos se respaldarán, con qué frecuencia y en qué soporte. Este proceso de organización es tan importante como la propia activación de la solución. Además, es aconsejable verificar periódicamente que las copias puedan restaurarse con éxito y mantener una disciplina constante a la hora de cumplir con nuestra política de copias de seguridad.
Coste	**Bajo o medio, en función de la solución elegida.** El coste dependerá del medio empleado: discos duros externos, almacenamiento en la nube u otros servicios especializados.

Seguridad del correo electrónico

El correo electrónico sigue siendo una vía muy utilizada para lanzar ataques de phishing, introducir malware o estafar a los empleados. Por ello, implementar sistemas de filtrado de spam, verificación de enlaces y autenticación de dominio es clave para proteger esta herramienta.	
 Complejidad de implementación	**Medio o medio-alto.** Su correcta configuración requiere ajustar filtros avanzados, revisar los parámetros del servidor de correo y aplicar protocolos de autenticación como SPF, DKIM y DMARC. Es recomendable asegurarse de que, al implantar una plataforma de venta online, esta cuente con todos los protocolos de seguridad disponibles.
 Coste	**Bajo o medio, en función de la solución elegida.** El coste dependerá del proveedor y del tipo de servicio contratado. Existen soluciones gratuitas y planes económicos que incluyen este tipo de funciones. En cualquier caso, se trata de una medida que refuerza la confianza interna y externa en las comunicaciones del comercio.

Seguridad de dispositivos móviles (MDM)

Los dispositivos móviles, como teléfonos y tabletas, forman parte del entorno laboral en muchos comercios, ya sea para revisar pedidos, gestionar redes sociales o realizar pagos. La gestión de estos equipos debe incluir medidas de seguridad como el cifrado de datos, el bloqueo remoto en caso de pérdida o robo y el control de las aplicaciones instaladas.	
 Complejidad de implementación	**Alto.** Su correcta implementación requiere herramientas específicas de gestión y ciertos conocimientos técnicos para la configuración y el mantenimiento.
 Coste	**Medio-alto.** El coste dependerá del número de dispositivos y del proveedor de la solución. Aun así, se trata de una inversión recomendable cuando se maneja información sensible desde terminales móviles. Cabe señalar que algunas marcas tecnológicas incluyen sus propios protocolos de seguridad, como el sistema Apple® o Knox en los dispositivos Samsung®.

Filtrado de contenido web

El filtrado web ayuda a prevenir accesos accidentales a páginas maliciosas o inadecuadas desde los dispositivos del comercio. Al restringir el acceso a determinados sitios, se reduce el riesgo de descargar *malware* o de introducir credenciales en páginas de phishing. En términos prácticos, esta medida limita la navegación a webs no relacionadas con la actividad del negocio, evitando que las personas usuarias accedan, por descuido, a sitios webs no autorizados o potencialmente peligrosos.

 **Complejidad de implementación**	**Bajo o medio.** Su configuración debe adaptarse a las necesidades del negocio, sin restringir demasiado la navegación útil.
 **Coste**	**Bajo o medio, según la solución elegida.** Puede integrarse como una funcionalidad adicional del antivirus o del cortafuegos, o implantarse como un servicio independiente más avanzado. En muchos casos, este tipo de filtrado puede configurarse también directamente desde el router del proveedor de internet. En general, constituye una medida eficaz para mantener un entorno de trabajo más seguro y concentrado en las tareas del negocio.

4. Buenas prácticas para el sector comercial en materia de seguridad

Ya se ha señalado en diversas ocasiones que el contexto digital actual se encuentra expuesto a numerosos riesgos y amenazas que afectan cada vez más a las pequeñas y medianas empresas. Disponer de un catálogo de buenas prácticas no solo contribuye a prevenir incidentes, sino que también fomenta una cultura de seguridad que protege al negocio, a sus empleados y a sus clientes.

El sector comercial, por su diversidad y estructura heterogénea, requiere de soluciones de ciberseguridad realistas y adaptadas a su operativa. Bajo esta premisa, la presente sección se concibe como un instrumento de apoyo práctico, orientado tanto a los responsables de seguridad de grandes empresas como a quienes gestionan pequeños comercios sin personal técnico especializado.

A lo largo de los siguientes subapartados se presentan recomendaciones[12] organizadas por niveles de responsabilidad y tipo de actividad comercial, desde los principios básicos aplicables a cualquier establecimiento hasta pautas específicas según el grado de digitalización del negocio. Esta clasificación tiene como objetivo facilitar su aplicación y adaptación a distintos entornos empresariales, respetando siempre los principios de proporcionalidad y eficacia.

4.1. Principios generales de actuación segura

Toda organización, con independencia de su tamaño o nivel de digitalización, debe comenzar por aplicar una serie de principios básicos. Entre ellos, destaca la importancia de mantener **actualizados todos los dispositivos, aplicaciones y sistemas operativos**. Las actualizaciones corrigen vulnerabilidades que pueden ser aprovechadas por atacantes, por lo que su aplicación constituye uno de los pasos más sencillos y eficaces para reforzar la seguridad. Este principio se recoge tanto en las directrices del Instituto Nacional de Ciberseguridad (INCIBE, 2021) como en la norma ISO/IEC 27002:2022, que promueve el establecimiento de controles técnicos y administrativos en todos los niveles de la organización.

Asimismo, se debe fomentar el uso de **contraseñas robustas y únicas para cada cuenta o sistema**. Las recomendaciones de ENISA (2023) proponen el uso de gestores de contraseñas y la autenticación multifactor como mecanismos eficaces para reducir el riesgo de accesos indebidos. Limitar el acceso a la información según perfiles definidos y aplicar el principio de mínimo privilegio contribuyen también a minimizar los posibles impactos ante un incidente.

[12] Las recomendaciones incluidas en esta sección han sido elaboradas tomando como referencia documentos técnicos y guías de entidades expertas en ciberseguridad como el Instituto Nacional de Ciberseguridad de España (INCIBE), cuyo portal *Protege tu Empresa* (https://www.incibe.es/protege-tu-empresa) proporciona pautas adaptadas a pymes, así como las recomendaciones generales de la Agencia de Ciberseguridad de la Unión Europea (ENISA). De igual forma, se ha considerado el marco establecido por las normas ISO/IEC 27002:2022 e ISO/IEC 27005:2022, que incluyen controles y principios de seguridad aplicables a las organizaciones comerciales. Estas fuentes garantizan que las prácticas propuestas cuenten con un respaldo técnico sólido, habiéndose realizado un ejercicio de adaptación del lenguaje para ofrecer un enfoque más accesible y alineado con la realidad del comercio andaluz.

Otro aspecto clave es establecer un **protocolo de actuación ante incidentes de seguridad**. Este protocolo debe ser conocido por todos los empleados y contemplar tanto la notificación interna como las medidas inmediatas para contener el daño. Tal y como señala la ISO/IEC 27005, disponer de un plan de respuesta ante incidentes resulta esencial para garantizar la resiliencia organizativa.

La sensibilización del personal es igualmente fundamental. Informar a los empleados sobre las amenazas más comunes, como el phishing, el uso inseguro de redes públicas o los engaños en redes sociales, y capacitarlos para identificar señales de alerta constituye una medida de bajo coste y, a su vez, de alta efectividad. El sentido común, reforzado por una cultura organizativa preventiva y proactiva, representa uno de los activos más valiosos en materia de ciberseguridad.

4.2. Buenas prácticas para las personas vinculadas al negocio

En primer lugar, es fundamental que la dirección o gerencia lidere con el ejemplo, creando un entorno donde estas prácticas se integren de forma natural. **Establecer políticas escritas, formar al equipo periódicamente y realizar controles internos** son acciones que pueden marcar la diferencia.

El éxito de cualquier estrategia de ciberseguridad no depende únicamente de los sistemas tecnológicos que se implementen, sino del comportamiento y la actitud del conjunto de personas que participan en la actividad diaria de la empresa. Esto incluye tanto al personal de atención directa, como a quienes se encargan de la gestión y toma de decisiones. Para que la ciberseguridad no se limite a un listado de buenas intenciones, es imprescindible trasladarla al plano operativo, con orientaciones claras, comprensibles y aplicables en el contexto de cada comercio.

Personal de tienda

Los/as empleados/as de tienda suelen ser el primer eslabón de defensa frente a muchas amenazas, especialmente aquellas que se aprovechan del factor humano, como el phishing o la ingeniería social. Según INCIBE (2021), una de las medidas más efectivas es enseñar al personal a identificar correos o mensajes sospechosos. Esto no significa que tengan que ser expertos en seguridad digital, sino que deben tener interiorizadas ciertas señales de alerta: correos con urgencia desmedida, direcciones de remitente extrañas, errores ortográficos graves o enlaces que no coinciden con la web oficial de la empresa. Este tipo de formación puede impartirse en sesiones breves, utilizando ejemplos reales que conecten con su experiencia cotidiana.

Personal Operativo

Otro aspecto clave para el personal operativo es el uso responsable de los dispositivos. Tanto los ordenadores como los TPV o los móviles deben considerarse herramientas críticas. La guía de buenas prácticas de ENISA (2023) recomienda mantener siempre bloqueada la pantalla al dejar el puesto, no conectar dispositivos personales al sistema corporativo y evitar instalar aplicaciones sin autorización. Para ello, es fundamental que la empresa facilite pautas sencillas y soluciones adaptadas, como el uso de móviles dedicados al trabajo o perfiles diferenciados para la actividad personal y profesional.

Personas encargadas/responsables

Para las personas encargadas y responsables de tienda, las obligaciones van un paso más allá. No solo deben aplicar las recomendaciones anteriores, sino también vigilar que se cumplen en el día a día. En este sentido, pueden actuar como figuras de referencia, detectando comportamientos de riesgo, resolviendo dudas y fomentando un ambiente de confianza. Según señala la norma ISO/IEC 27002:2022, es recomendable que cada área cuente con una persona responsable de la aplicación de medidas básicas, aunque no disponga de formación técnica especializada. Esta figura actúa como puente entre el equipo y quienes gestionan la seguridad a nivel general.

Personas gestoras/propietarias

Desde el punto de vista de los gestores o propietarios del comercio, la principal responsabilidad consiste en crear un marco organizativo que permita aplicar estas recomendaciones de forma sistemática. La primera medida es asignar presupuesto y tiempo a la seguridad, aunque sea a pequeña escala. Por ejemplo, incluir una revisión de seguridad en las reuniones mensuales, dedicar una mañana al trimestre a actualizar los sistemas y formar al equipo, o contratar asesoramiento externo una vez al año. Estas decisiones no solo reducen riesgos, sino que generan confianza entre el personal y los clientes.

Es importante tener en cuenta que muchas de estas recomendaciones no requieren inversiones significativas ni conocimientos técnicos. Si tomamos como referencia el Plan Director de Seguridad de INCIBE, adoptar una política clara de contraseñas, realizar copias de seguridad automáticas y limitar los permisos de acceso son medidas de bajo coste y gran impacto. Lo fundamental es que estas pautas se integren en la cultura de la empresa.

Un consejo operativo es establecer rutinas. Las rutinas aportan seguridad y reducen el margen de error. Por ejemplo, revisar el correo al inicio de la jornada prestando especial atención a mensajes inusuales, comprobar que las copias de seguridad automáticas se han completado correctamente una vez por semana o cerrar sesión en todas las plataformas antes de finalizar el día. Estas acciones, repetidas y asumidas como normales, funcionan como barreras eficaces contra incidentes.

Todas estas orientaciones están recogidas, con mayor o menor nivel de detalle, en fuentes como la Guía de ciberseguridad para el comercio electrónico de INCIBE (2021), el Glosario de términos de ciberseguridad (INCIBE, 2021), la Estrategia Andaluza de Ciberseguridad (2022-2025) y los estándares internacionales como las normas ISO/IEC 27000, 27002 y 27005. Pero más allá de los documentos, lo esencial es que cada organización interiorice estas prácticas y las adapte a su tamaño, recursos y nivel de exposición digital.

Ideas de síntesis

- Conviene tener presente que la ciberseguridad es una responsabilidad compartida. No debe recaer únicamente en una persona o en un departamento.
- Cada integrante del equipo puede y debe aportar, desde mantener ordenado su espacio de trabajo hasta alertar sobre comportamientos anómalos en los dispositivos o en las plataformas online. La suma de pequeñas acciones es la que crea entornos más protegidos.

4.3. Recomendaciones específicas según el tipo de comercio

Cada tipo de comercio tiene necesidades y riesgos diferentes, por lo que las recomendaciones deben ajustarse a su realidad.

Comercios físicos tradicionales

En los comercios físicos tradicionales, donde la digitalización puede estar limitada a tareas administrativas, las buenas prácticas deben centrarse en garantizar la seguridad física y lógica de los equipos. La seguridad física hace referencia a la protección del propio dispositivo, por ejemplo, evitar daños por subidas de tensión, que no salga ardiendo o que no se moje accidentalmente, mientras que la seguridad lógica se orienta a los posibles riesgos digitales, como el robo o la corrupción de datos.

En este sentido, es crucial proteger los dispositivos que almacenan información de clientes, como los sistemas de gestión o los TPV, y mantener copias de seguridad externas actualizadas. El uso de software legal y su correcta actualización también constituye una medida esencial, tal y como recogen las directrices del Plan Director de Seguridad elaborado por INCIBE.

Comercios mixtos

Para los comercios mixtos, que combinan atención presencial con venta online, la seguridad debe aplicarse en ambos entornos. Las plataformas web deben contar con cifrado mediante certificados HTTPS, herramientas antimalware y una configuración adecuada de accesos. También es necesario revisar las políticas de privacidad, cookies y protección de datos, garantizando el cumplimiento del Reglamento General de Protección de Datos (RGPD) y de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Se recomienda disponer de asesoramiento externo o utilizar herramientas automatizadas que auditen la seguridad de la web y de las transacciones electrónicas.

Comercios digitales

En el caso de los comercios exclusivamente digitales, la ciberseguridad debe integrarse desde el diseño del negocio. Esto implica utilizar servicios de alojamiento (hosting) seguros, habilitar la autenticación multifactor en todos los accesos críticos, monitorizar los intentos de conexión y realizar auditorías periódicas. Para estos casos, INCIBE y ENISA ofrecen diversas herramientas y guías específicas para el comercio electrónico cuya consulta resulta especialmente recomendable[13].

4.4. Integración de la ciberseguridad en el día a día

Uno de los grandes retos del sector comercial es **integrar la seguridad digital en las rutinas cotidianas** sin que ello suponga una carga operativa. La normalización de estas prácticas pasa por asumir que la ciberseguridad es parte del trabajo diario, como lo son la atención al cliente o la gestión del stock; es decir, debe integrarse plenamente en la forma habitual de trabajar, hasta convertirse en un elemento propio de la cultura empresarial.

Se recomienda elaborar **listas de comprobación periódicas (checklist)** para revisar aspectos básicos, como el estado de las actualizaciones, la caducidad de los certificados digitales, la existencia de copias de seguridad válidas o el correcto funcionamiento de los sistemas de control de acceso. Estas listas pueden automatizarse mediante herramientas específicas o, simplemente, incorporarse al calendario de tareas semanales.

Además, se aconseja organizar al menos una sesión trimestral de **formación interna o de repaso de los protocolos de seguridad**. En este sentido, INCIBE propone actividades breves, como simulacros de phishing, cuestionarios de autoevaluación o micro acciones formativas. Estas dinámicas no solo informan, sino que refuerzan la conciencia del equipo sobre su papel en la protección del negocio, ya que en la mayoría de los casos una **reacción rápida y coordinada** reduce significativamente las consecuencias de un ciberataque.

[13] Se recomienda, entre otras referencias, la lectura de la *Guía de seguridad en el comercio electrónico* (INCIBE, 2021).

En definitiva, integrar la ciberseguridad en la operativa habitual no solo fortalece la defensa del comercio, sino que también **potencia la madurez digital del negocio, refuerza su reputación y mejora su capacidad de adaptación ante los desafíos del entorno actual**.

Ideas de síntesis

- La creación de una cultura de ciberseguridad debe implicar a todo el personal, desde quienes trabajan en atención al público hasta el equipo directivo. Esta cultura se construye mediante el ejemplo, la repetición de hábitos seguros y el reconocimiento de las buenas prácticas.

4.5. Decálogo práctico de ciberseguridad para comercios andaluces

La ciberseguridad constituye hoy un elemento esencial de la gestión empresarial, y no un asunto estrictamente técnico. En el caso de los comercios andaluces, especialmente aquellos que comienzan a utilizar herramientas digitales para la venta, la comunicación o la gestión, disponer de una estrategia básica de seguridad resulta fundamental para proteger los datos, evitar fraudes y mantener la confianza de la clientela.

Este apartado presenta un decálogo ampliado que recoge los pasos esenciales que debería seguir la persona responsable del comercio, incluso sin disponer de conocimientos técnicos, con el fin de comenzar a proteger su negocio frente a los principales riesgos digitales. Siguiendo las mismas directrices y fuentes utilizadas en los apartados previos, el decálogo se apoya en las recomendaciones de entidades especializadas como INCIBE y ENISA, así como en las directrices de la norma internacional ISO/IEC 27005:2022 sobre gestión de riesgos de seguridad de la información.

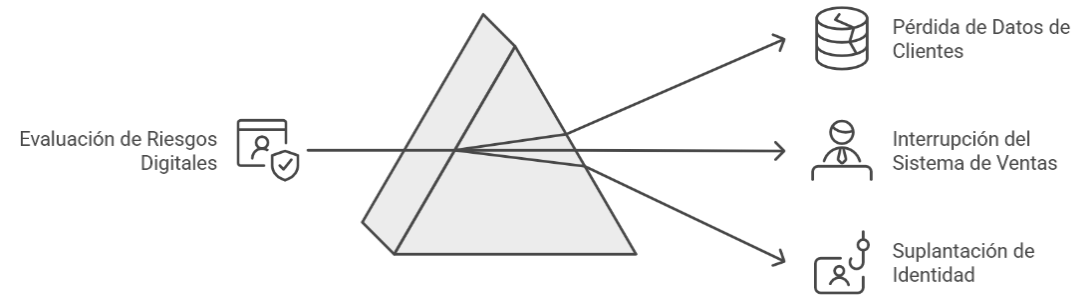
La normalización internacional en materia de prevención de riesgos establece tres grandes bloques de actuación: **identificar, evaluar y mitigar los riesgos**. Partiendo de esta base, se proponen una serie de acciones orientadas a ofrecer una respuesta operativa a estos requisitos.

En cualquier caso, cuando las empresas comerciales no dispongan de personal con la capacitación digital necesaria para ejecutar alguno de estos pasos, resulta recomendable contar con el apoyo de profesionales del sector tecnológico que puedan asesorar y acompañar en la correcta implantación de las medidas propuestas.

1. Analiza los riesgos digitales de tu negocio

El primer paso consiste en identificar qué activos digitales utiliza el comercio (correo electrónico, TPV, dispositivos móviles, tienda online, redes sociales, etc.) y valorar qué podría suceder si alguno de ellos sufriera un ataque. Esto se conoce como evaluación de riesgos (norma ISO/IEC 27005), y no requiere elaborar complejos informes: basta con reflexionar sobre las posibles consecuencias de perder datos de clientes, interrumpir el sistema de ventas o sufrir una suplantación de identidad.

Figura 4. Analiza los riesgos digitales de tu negocio

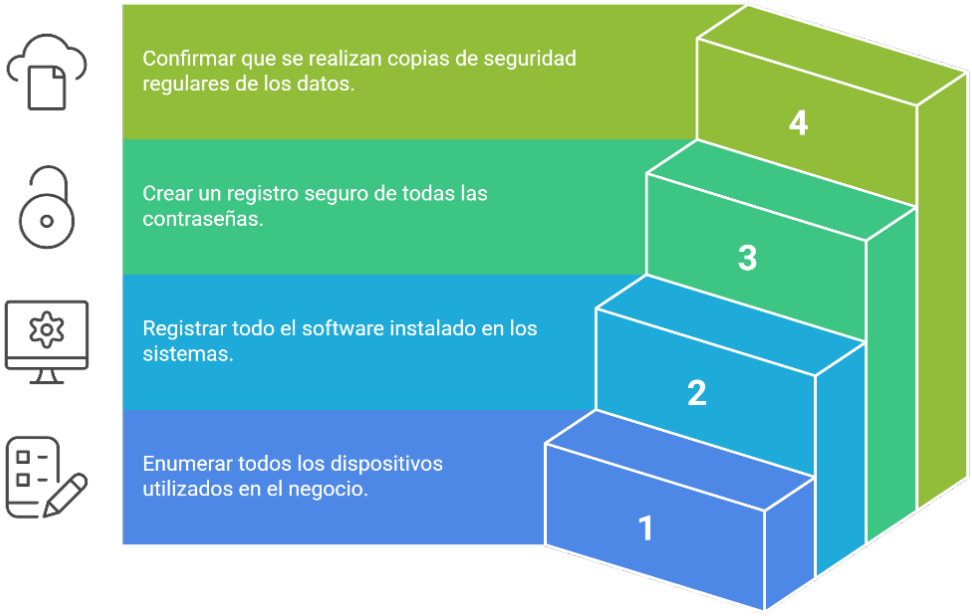


Fuente: Elaboración propia

2. Hacer un inventario básico de sistemas y medidas de seguridad existentes

Anota qué dispositivos utilizas en el negocio (ordenadores, routers, móviles, TPV), qué programas o aplicaciones tienes instalados, qué contraseñas protegen tus cuentas y si realizas copias de seguridad con regularidad. Este paso te ayudará a conocer la situación real de tu infraestructura tecnológica, saber por dónde empezar y detectar posibles puntos débiles.

Figura 5. Hacer un inventario básico de sistemas y medidas de seguridad existentes

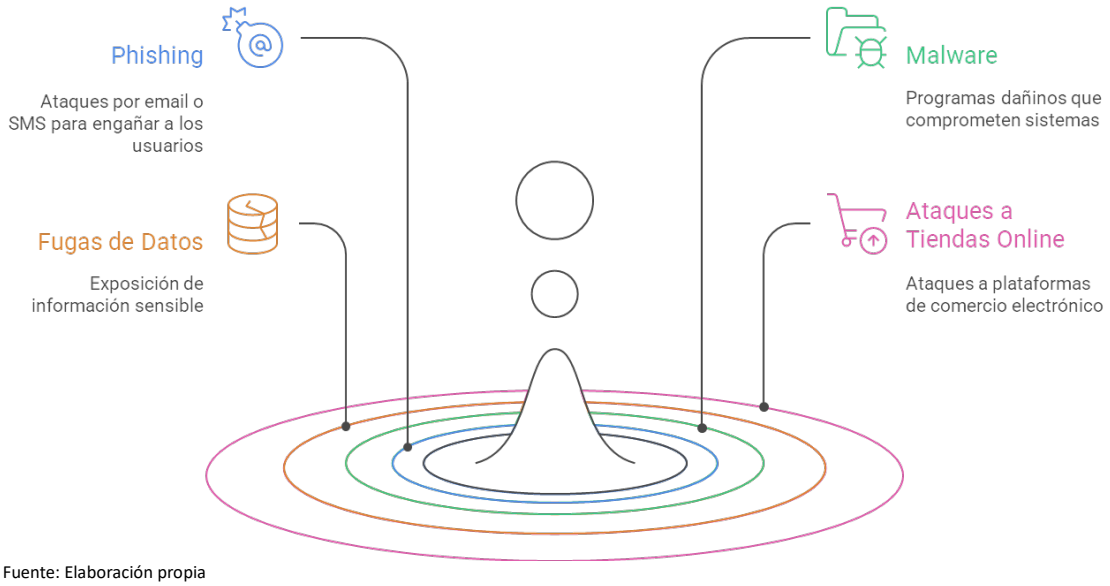


Fuente: Elaboración propia

3. Evaluación las amenazas más comunes para tu tipo de comercio

Cada negocio presenta particularidades propias, pero las amenazas suelen compartir patrones y comportamientos similares. A la hora de evaluar las amenazas, conviene reflexionar sobre cuestiones como: ¿qué resulta más probable en tu caso, un ataque dirigido a los sistemas o a las personas? Plantea esta reflexión teniendo en cuenta las características, tamaño y grado de digitalización de tu organización. Según la información presentada a lo largo del documento, los riesgos más habituales para los comercios son los siguientes:

Figura 6. Evaluación las amenazas más comunes para tu tipo de comercio

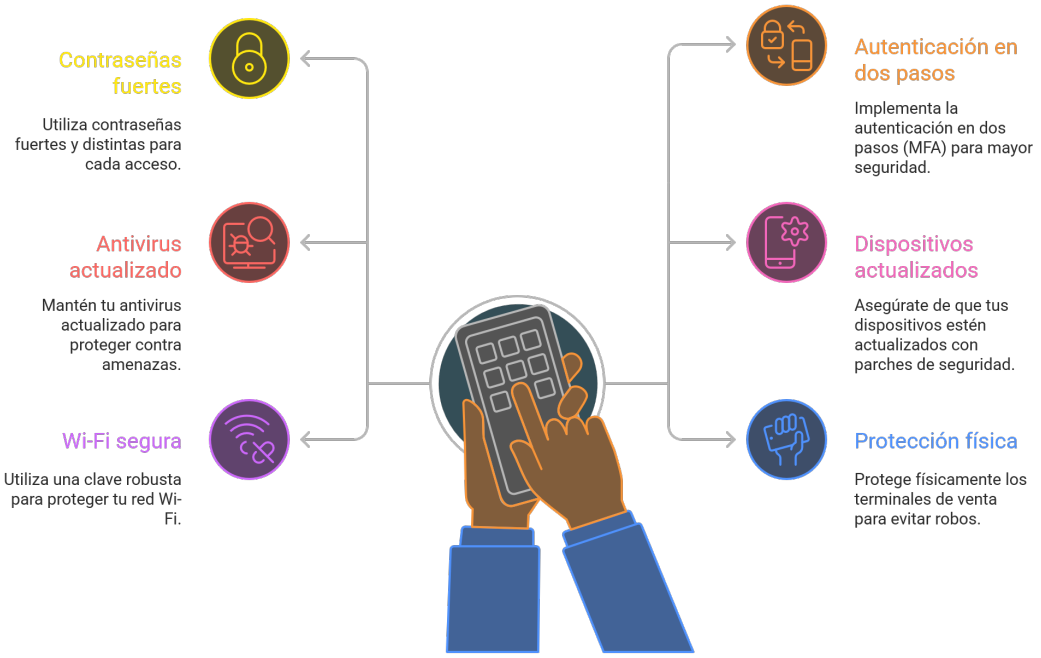


Fuente: Elaboración propia

4. Selección y aplicación medidas básicas de protección digital

Muchas veces no es necesario realizar grandes inversiones o implementar soluciones complejas. Lo más importante es garantizar que las medidas esenciales estén correctamente implantadas y se mantengan actualizadas en el tiempo. Asegúrate de cumplir con lo básico.

Figura 7. Selección y aplicación medidas básicas de protección digital



Fuente: Elaboración propia

5. Implanta un sistema de copias de seguridad periódicas

Establece un sistema y una política clara de copias de seguridad automáticas que incluya todos los archivos críticos del negocio, como los datos de clientes, facturas y documentación administrativa. Guarda las copias en ubicaciones seguras, preferiblemente combinando almacenamiento en la nube con dispositivos externos cifrados, y verifica de forma periódica que las copias se realizan correctamente y pueden restaurarse sin errores.

Figura 8. Implanta un sistema de copias de seguridad periódicas

Fuente: Elaboración propia

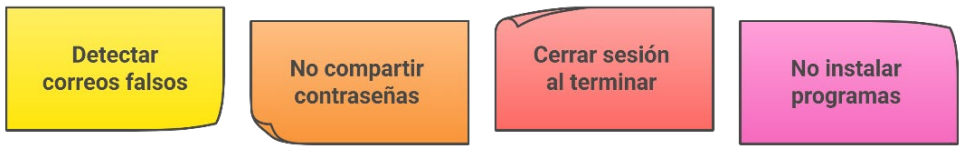
6. Forma e informa a tus empleados y colaboradores

Gran parte de los incidentes de seguridad se deben a fallos humanos o a la falta de información. Por ello, es fundamental fomentar una cultura de ciberseguridad compartida, basada en medidas sencillas. Recuerda que la ciberseguridad no depende únicamente de la tecnología, sino también de la constancia y el cumplimiento de buenas prácticas diarias.

Diversas plataformas públicas ofrecen recursos gratuitos para formación interna y buenas prácticas en tu negocio o tienda.

- INCIBE – Protege tu Empresa. (https://www.incibe.es/protege-tu-empresa)
- Agencia Digital de Andalucía (ADA). Formación Andalucía Vuela. (https://formacion.andaluciavuela.es/)
- ENISA – European Union Agency for Cybersecurity. (https://www.enisa.europa.eu)

Figura 9. Forma e informa a tus empleados y colaboradores



Fuente: Elaboración propia

7. Asegurar los canales digitales de venta y comunicación

Si tu comercio cuenta con una página web, tienda online o utiliza redes sociales para promocionarse, es fundamental proteger estos canales frente a posibles ataques o usos indebidos. Ten siempre presente lo siguiente:

Figura 10. Asegurar los canales digitales de venta y comunicación

Fuente: Elaboración propia

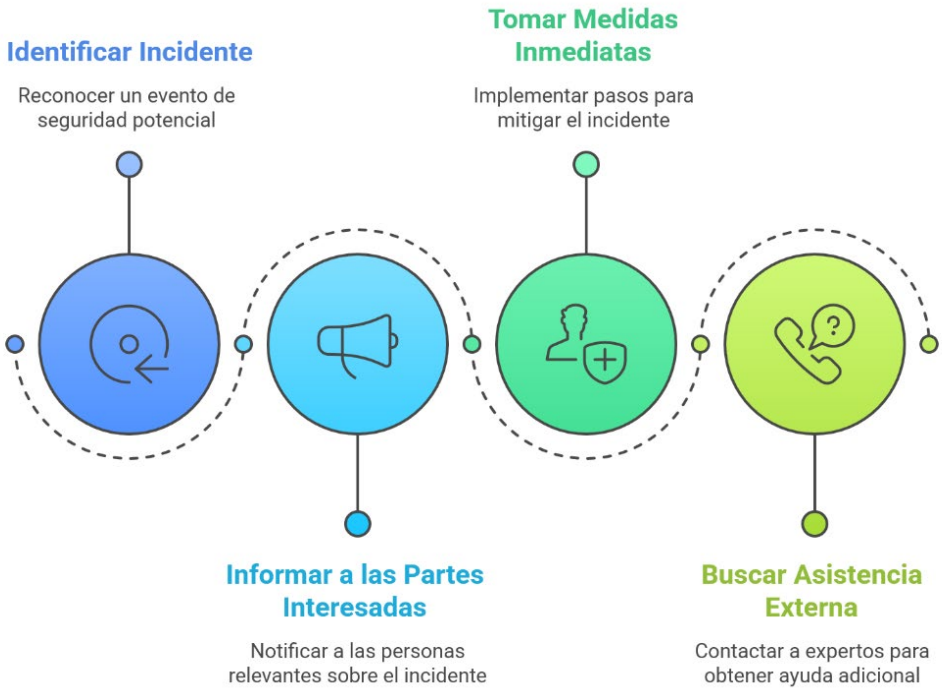
8. Establecer protocolos en caso de incidente

Las normas internacionales de gestión, como la ISO/IEC 27002, recomiendan disponer de protocolos de actuación ante incidentes, incluso en los negocios de menor tamaño. Contar con estos procedimientos no solo refuerza la protección frente a las ciberamenazas, sino que también mejora la organización y la capacidad de respuesta del comercio.

A modo de ejemplo, ¿sabrías qué hacer si se bloquea el acceso al correo electrónico o si alguien roba el perfil de Instagram del negocio? Hay que tener un plan de actuación ante incidentes que contemple, como mínimo:

- Quién debe ser informado.
- Qué pasos seguir (por ejemplo, cortar la conexión, cambiar contraseñas,…).
- A quién acudir (INCIBE, proveedor de hosting o servicio técnico especializado).

Figura 11. Establecer protocolos en caso de incidente

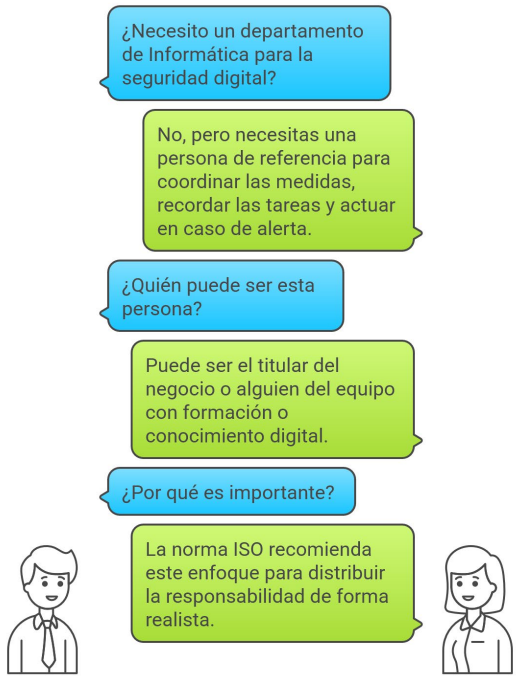


Fuente: Elaboración propia

9. Designar a una persona responsable de la seguridad digital

Independientemente del tamaño o estructura del comercio, es necesario contar con una persona de referencia que coordine las medidas de seguridad, supervise las tareas pendientes y actúe ante posibles alertas o incidentes. Esta figura puede ser el propio titular del negocio o un miembro del equipo que disponga de formación o conocimientos en materia digital.

Figura 12. ***Designar a una persona responsable de la seguridad digital***

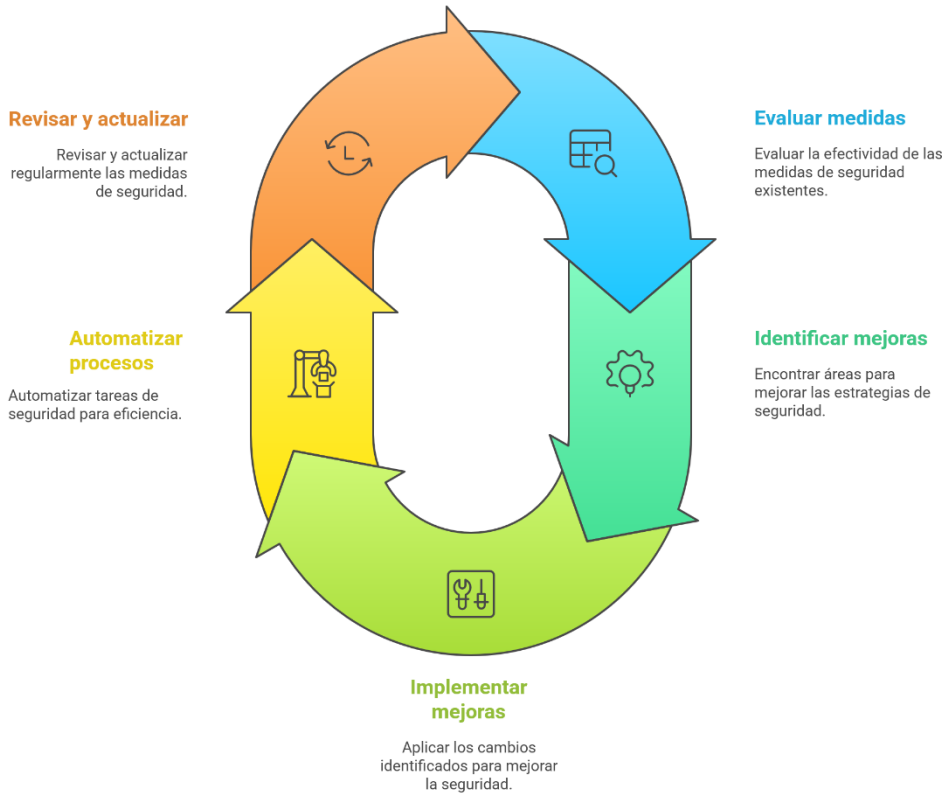


Fuente: Elaboración propia

10. Evaluar, mejorar y automatizar

Revisar periódicamente si las medidas que has tomado funcionan y si podemos mejorarlas. Podemos utilizar listas de verificación (checklists), herramientas gratuitas públicas o incluso servicios de consultoría si el negocio crece. En cualquier caso, debemos tener presente que la mejora continua es clave para mantener la protección a largo plazo.

Figura 13. Evaluar, mejorar y automatizar

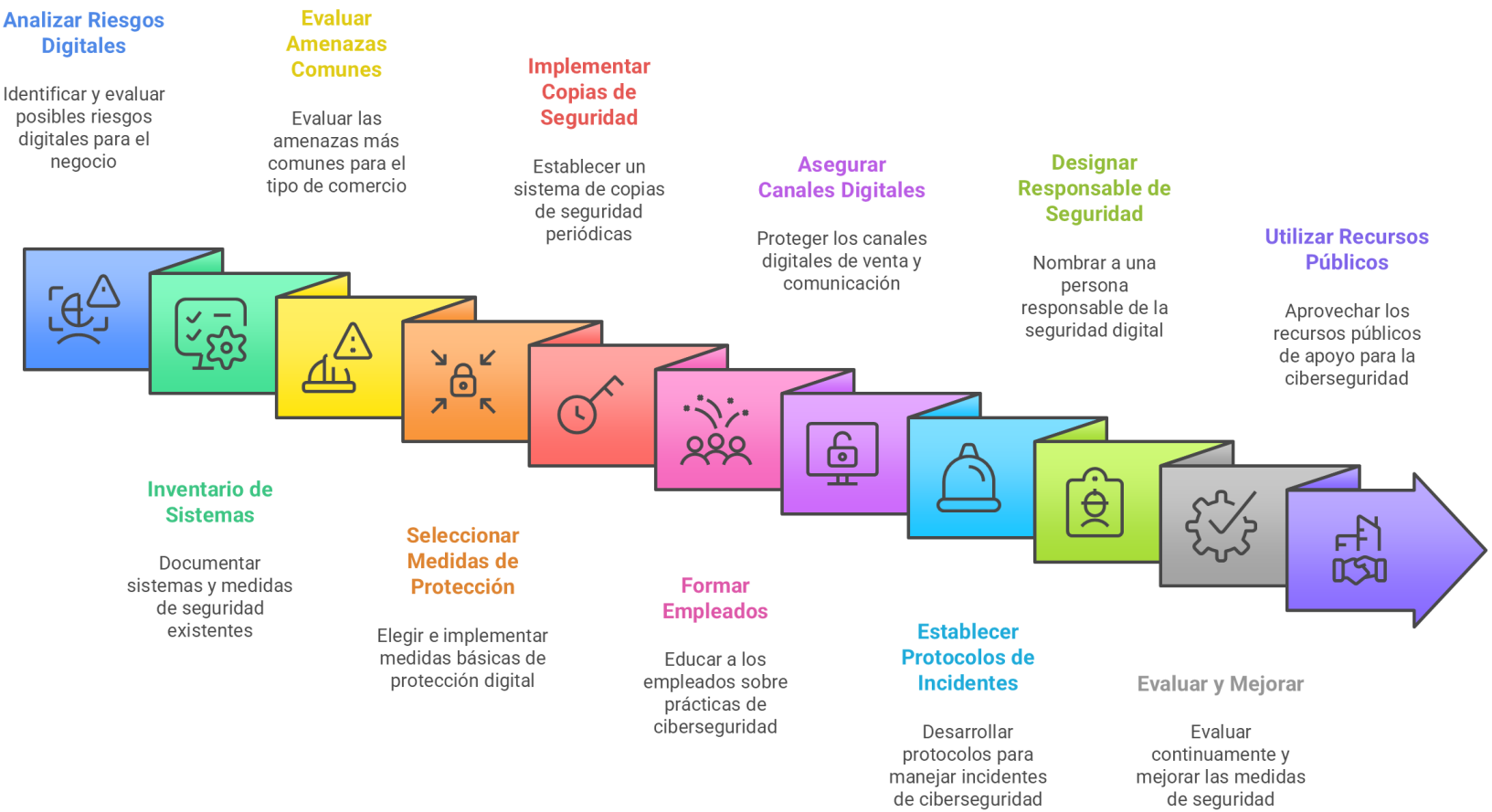


Fuente: Elaboración propia

10+1. Aprovecha los recursos públicos de apoyo

- Existe una amplia red de entidades y administraciones públicas que pueden ofrecerte apoyo con estas tareas.
- Puedes acceder a programas y ayudas públicas destinadas a impulsar la digitalización y la ciberseguridad en el comercio, como la línea de subvenciones promovida por la Dirección General de Comercio de la Consejería de Empleo, Empresa y Trabajo Autónomo de la Junta de Andalucía.
- Asimismo, existen entidades de ámbito nacional que pueden ofrecerte orientación y apoyo, como el Instituto Nacional de Ciberseguridad (INCIBE), que a través de su portal Protege tu Empresa pone a disposición de las pymes un servicio gratuito de asesoramiento y recursos prácticos.

Figura 14. Decálogo de ciberseguridad para comercios andaluces



La ciberseguridad no tiene por qué ser cara ni compleja. Lo importante es empezar por lo básico, adaptarlo a tu negocio y crear hábitos seguros. Este decálogo puede ayudarte a ordenar ideas y tomar decisiones informadas. Si no sabes cómo hacerlo tú mismo, busca apoyo profesional o utiliza los recursos disponibles. Proteger tu comercio hoy es invertir en su continuidad mañana.

Anexo


CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY
COMERCIO
de ANDALUCÍA

Introducción a la evaluación de las ciberamenazas

La evaluación de riesgos o amenazas es una etapa esencial dentro de cualquier estrategia de ciberseguridad. Su finalidad es **priorizar los riesgos** en función de dos variables clave: la **probabilidad** de que una amenaza se materialice y el **impacto** que podría tener sobre los activos y procesos del negocio. Esta metodología, recogida en la norma **ISO/IEC 27005** y promovida por **INCIBE**, constituye la base para tomar decisiones informadas y proporcionales en materia de seguridad.

En el ámbito comercial, este enfoque resulta especialmente útil, ya que permite **identificar qué ciberamenazas pueden comprometer la continuidad del negocio**, provocar pérdidas económicas o afectar a la confianza de los clientes. La combinación entre la frecuencia estimada de un incidente y el daño potencial que podría ocasionar facilita **asignar los recursos de forma eficiente** y seleccionar las medidas de protección más adecuadas al perfil de riesgo de cada empresa.

La evaluación de riesgos puede representarse mediante una **matriz de probabilidad e impacto**, que ofrece una visión práctica de los principales riesgos asociados a las ciberamenazas analizadas en los capítulos anteriores. Esta herramienta, reconocida por la norma ISO/IEC 27005, forma parte de la familia ISO/IEC 27000 sobre gestión de la seguridad de la información[14].

La siguiente tabla muestra un ejemplo de matriz elaborada con datos simulados. Su finalidad es ilustrar cómo se pueden clasificar las amenazas en función de la frecuencia con la que podrían producirse y del nivel de daño que causarían sobre la actividad del negocio.

Tabla 2. Matriz de evaluación de ciberamenazas: probabilidad e impacto

Ciberamenaza	Probabilidad	Daño potencial	Evaluación
Phishing	Muy frecuente	Alto	16
Suplantación de identidad (correo/redes)	Frecuente	Muy alto	15
Fraude del proveedor	Frecuente	Muy alto	15
Uso de malware (incl. ransomware)	Muy frecuente	Muy alto	20
Acceso no autorizado a sistemas	Frecuente	Muy alto	15
Ataques a la web (inyección SQL, XSS)	Ocasional	Alto	8
Interrupción de servicios (DDoS)	Ocasional	Medio	6
Ingeniería social telefónica (vishing)	Frecuente	Medio	9
Fugas de datos por dispositivos móviles inseguros	Ocasional	Alto	8

Fuente: Elaboración propia

Para interpretar la tabla se emplean los siguientes niveles de probabilidad y daño potencial:

[14] En particular, dicha norma establece criterios para identificar, analizar y evaluar los riesgos en función de su probabilidad de ocurrencia y su posible impacto sobre la organización. Asimismo, este enfoque es coherente con la metodología propuesta en la norma ISO 31000 sobre gestión del riesgo, que refuerza la necesidad de integrar esta evaluación en la toma de decisiones estratégicas.

Probabilidad (frecuencia estimada de ocurrencia):

- Muy frecuente (4): es esperable que ocurra varias veces al año.
- Frecuente (3): puede suceder al menos una vez al año.
- Ocasional (2): se da de manera esporádica o bajo determinadas circunstancias.
- Poco frecuente (1): es improbable, pero posible si no se aplican medidas de seguridad.

Daño potencial (impacto sobre la continuidad del negocio):

- Muy alto (5): la actividad comercial se interrumpe totalmente.
- Alto (4): el negocio sufre una interrupción parcial o prolongada.
- Medio (3): la actividad continúa, pero con incidencias importantes.
- Bajo (2): se generan molestias o costes menores sin afectar la continuidad.
- Muy bajo (1): sin impacto significativo en el funcionamiento general.

En la práctica, el proceso de evaluación asigna un valor numérico a cada nivel. Cuanto mayor sea la probabilidad o el daño, mayor será el número asignado. Al combinar ambos factores mediante un cálculo multiplicativo (**Probabilidad x Impacto**), se obtiene una puntuación que permite representar las amenazas en la matriz y establecer su prioridad de tratamiento.

Tabla 3. Escala de puntuación para la evaluación de ciberamenazas (Probabilidad × Impacto)

Probabilidad / Daño potencial	Muy frecuente (4)	Frecuente (3)	Ocasional (2)	Poco Frecuente (1)
Muy Alto (5)	20	15	10	5
Alto (4)	16	12	8	4
Medio (3)	12	9	6	3
Bajo (2)	8	6	4	2
Muy Bajo (1)	4	3	2	1

Fuente: Elaboración propia

Es importante destacar que esta matriz tiene un **carácter orientativo y debe adaptarse a la realidad de cada negocio**. No será igual la evaluación de un comercio minorista de pequeño tamaño con actividad principalmente presencial que la de un mayorista con plataformas conectadas a proveedores o la de una tienda que opera exclusivamente en línea. Cada uno de estos modelos presenta niveles de exposición y dependencia tecnológica diferentes, por lo que requiere un análisis ajustado a su infraestructura digital y a su operativa diaria. Aplicar este tipo de matriz de forma personalizada es fundamental para **tomar decisiones realistas y efectivas en materia de ciberseguridad.**

A partir de esta evaluación, cada organización debe **definir los límites de riesgo que considera aceptables**, es decir, determinar qué nivel de amenaza está dispuesta a asumir. En la matriz de evaluación anterior, por ejemplo, los riesgos con valores **superiores a 10** se consideran **críticos (rojos)**, los situados **entre 10 y 5** se clasifican como **medios (naranja)** y aquellos **iguales o inferiores a 4** se consideran **aceptables (verdes)**.

La combinación de las tablas presentadas permite obtener una **visión global del nivel de exposición** frente a las distintas ciberamenazas. Esta representación facilita identificar **qué amenazas requieren una atención prioritaria** y orientar la aplicación de medidas de protección. En primer lugar, deberán abordarse las amenazas clasificadas como **críticas**, seguidas de aquellas calificadas como **medias**.

Tabla 4. Clasificación de amenazas calificadas como críticas y medias.

Ciberamenaza	Evaluación
Uso de malware (incl. ransomware)	20
Phishing	16
Suplantación de identidad (correo/redes)	15
Fraude del proveedor	15
Acceso no autorizado a sistemas	15
Ingeniería social telefónica (vishing)	9
Fugas de datos por dispositivos móviles inseguros	8
Ataques a la web (inyección SQL, XSS)	8
Interrupción de servicios (DDoS)	6

Fuente: Elaboración propia

A modo de ejemplo, un ataque de interrupción de servicios (DDoS) puede saturar los recursos del sistema o de la conexión a Internet del comercio, impidiendo el acceso a su página web, tienda online o plataforma de gestión de pedidos. Aunque no implique una pérdida directa de datos, el daño reputacional y la pérdida de ingresos por inactividad pueden ser considerables, especialmente en fechas de alta demanda o campañas promocionales.

Una vez identificadas las principales ciberamenazas y su nivel de riesgo, resulta fundamental **cruzar esta información con la utilidad de las herramientas de ciberseguridad disponibles** y el **coste estimado de su implantación**. Este enfoque permite a cada empresa **priorizar las soluciones más eficaces** para su contexto operativo.

La siguiente tabla resume, a modo de ejemplo, distintas **medidas de ciberseguridad** valoradas según su **utilidad práctica** frente a las amenazas detectadas y su **coste aproximado de implantación y mantenimiento**. Esta información facilita la **toma de decisiones estratégicas** por parte de los responsables del comercio y orienta la planificación de inversiones en materia de seguridad digital.

Tabla 5. Evaluación coste-utilidad de medidas de ciberseguridad

Nº	Medida	Utilidad	Coste
1	Antivirus y antimalware	Muy alta	Bajo
2	Firewall (cortafuegos)	Alta	Medio
3	IDS/IPS	Alta	Medio - Alto
4	Gestión de parches y actualizaciones	Muy alta	Bajo
5	Control de acceso y autenticación (MFA)	Muy alta	Bajo - Medio
6	Cifrado de datos	Alta	Bajo - Medio
7	Copias de seguridad y recuperación	Muy alta	Bajo - Medio
8	Seguridad del correo electrónico	Alta	Bajo - Medio
9	Seguridad de dispositivos móviles (MDM)	Alta	Medio - Alto
10	Filtrado web	Alta	Bajo - Medio

Fuente: Elaboración propia

Leyenda de utilidad esperada:

- **Muy alta:** Medidas que protegen frente a amenazas frecuentes y de alto impacto potencial (*Ej: ransomware, phishing o pérdida de datos críticos*).
- **Alta:** Medidas que reducen riesgos técnicos o complementan otras barreras de protección, mitigando daños operativos o de reputación.

Leyenda de coste:

- **Bajo:** ≤ 50 € anuales o herramientas gratuitas.
- **Medio:** entre 50 € y 200 € anuales por solución o dispositivo.
- **Alto:** > 200 € anuales o requiere infraestructura específica.

Finalmente, resulta necesario **establecer la relación entre las principales medidas de protección recomendadas en esta guía y las ciberamenazas específicas** que cada una de ellas contribuye a **prevenir, mitigar o detectar**. Este ejercicio permite ofrecer una visión práctica y aplicada de la ciberseguridad, facilitando que los **profesionales del sector comercial andaluz** puedan **priorizar la implantación de soluciones** en función de los riesgos identificados en la evaluación previa.

Tal y como se observa en la tabla a continuación, cada medida está asociada a una o varias amenazas, considerando tanto su **naturaleza técnica** como el modo en que contribuye a **reducir la probabilidad de ocurrencia o el impacto potencial** de un incidente.

Gracias a esta doble perspectiva, que combina las medidas disponibles con los riesgos evaluados, cada organización puede establecer **un orden de prioridades adaptado a su perfil de exposición, presupuesto y nivel de digitalización**. Por ejemplo, si el análisis de riesgos identifica como prioritarias las amenazas relacionadas con *malware* o *phishing*, será recomendable comenzar por medidas como el antivirus, el filtrado web o la seguridad del correo electrónico, todas ellas clasificadas como de alta o muy alta utilidad y con costes asumibles para la mayoría de las empresas comerciales.

Tabla 6. Correspondencia entre medidas de protección y ciberamenazas

Medida de Protección	Ciberamenaza
Antivirus y antimalware	Uso de malware (incl. ransomware)
	Phishing
Firewall (cortafuegos)	Acceso no autorizado a sistemas
	Ataques a la web (inyección SQL, XSS)
	Interrupción de servicios (DDoS)
IDS/IPS	Acceso no autorizado a sistemas
	Interrupción de servicios (DDoS)
	Ataques a la web (inyección SQL, XSS)
Gestión de parches y actualizaciones	Uso de malware (incl. ransomware)
	Acceso no autorizado a sistemas
	Ataques a la web (inyección SQL, XSS)
Control de acceso y autenticación (MFA)	Acceso no autorizado a sistemas
	Fraude del proveedor
	Suplantación de identidad (correo/redes)
Cifrado de datos	Fugas de datos por dispositivos móviles inseguros
	Acceso no autorizado a sistemas
Copias de seguridad y recuperación	Uso de malware (incl. ransomware)
	Ataques a la web (inyección SQL, XSS)
	Interrupción de servicios (DDoS)
Seguridad del correo electrónico	Phishing
	Suplantación de identidad (correo/redes)
	Fraude del proveedor
Seguridad de dispositivos móviles (MDM)	Fugas de datos por dispositivos móviles inseguros
Filtrado web	Phishing
	Uso de malware (incl. ransomware)
	Ataques a la web (inyección SQL, XSS)

Fuente: Elaboración propia

De esta forma, la interrelación entre **amenazas, riesgos y medidas de protección** constituye la base de una **estrategia de ciberseguridad coherente, escalable y adaptada** a las realidades del comercio andaluz.

Ideas de síntesis

- Implementar medidas de protección frente a las ciberamenazas no debe entenderse como una carga técnica o económica, sino como una inversión estratégica en la continuidad del negocio y la confianza del cliente.
- Existen soluciones para todos los niveles de conocimiento y presupuestos. Una buena combinación de herramientas básicas y avanzadas puede proporcionar un nivel adecuado de seguridad para el comercio andaluz.
- La clave está en priorizar, planificar e integrar estas medidas de forma progresiva y adaptada a las necesidades de cada establecimiento. Solo así será posible aprovechar las oportunidades del entorno digital con garantías, reduciendo riesgos, mejorando la imagen de la empresa y asegurando una presencia sólida en el mercado actual.

Glosario

Este glosario reúne los términos técnicos, siglas y anglicismos empleados a lo largo del documento. Su objetivo es ofrecer definiciones claras, precisas y fácilmente comprensibles, especialmente dirigidas a personas sin formación técnica previa.

Actualización: Proceso mediante el cual se instalan mejoras o correcciones en un programa, sistema operativo o aplicación. Las actualizaciones suelen solucionar errores o tapar fallos de seguridad.

Antivirus: Programa diseñado para detectar y bloquear software malicioso que pueda dañar el equipo o robar información.

Ataque dirigido: Intento intencionado de dañar o acceder a los sistemas de una persona o empresa concreta, normalmente con un objetivo claro (económico, político o de espionaje).

Autenticación multifactor (MFA): Sistema que exige dos o más pruebas para verificar la identidad de una persona al acceder a una cuenta (por ejemplo: contraseña + código en el móvil).

Backup (copia de seguridad): Duplicado de archivos importantes que se guarda en otro lugar (un disco duro externo o en la nube) para poder recuperarlos en caso de pérdida o ataque.

CERT (Computer Emergency Response Team): Equipo especializado en responder a incidentes de ciberseguridad. En España, el CERT más conocido es el de INCIBE.

Ciberataque: Cualquier acción realizada a través de medios digitales con el fin de dañar, robar o bloquear información o sistemas.

Ciberseguridad: Conjunto de medidas y prácticas destinadas a proteger los sistemas digitales y la información que contienen frente a amenazas y ataques.

Cifrado: Técnica que convierte los datos en un formato ilegible para proteger su contenido. Solo quien tenga la clave correcta podrá leerlos.

Contraseña robusta: Clave difícil de adivinar, que suele combinar letras, números y símbolos. Cuanto más larga y variada, más segura.

Cookies: Pequeños archivos que las páginas web almacenan en el navegador para recordar preferencias o hábitos de navegación.

Correo fraudulento (phishing): Mensaje que simula ser de una empresa conocida para engañar al usuario y robarle datos o dinero.

Datos personales: Información que identifica o puede identificar a una persona, como el nombre, DNI, dirección postal o número de teléfono.

Firewall (cortafuegos): Sistema que vigila el tráfico entre el equipo y la red para bloquear accesos no autorizados.

Hosting (alojamiento web): Servicio que permite que una página web esté disponible en Internet. De forma similar a un alquiler, el proveedor de hosting ofrece capacidad y recursos en un servidor seguro para garantizar el correcto funcionamiento del sitio web.

Ingeniería social: Técnica de engaño que busca manipular a una persona para que entregue datos, abra archivos o permita accesos a un sistema sin darse cuenta.

ISO/IEC 27001 / 27002 / 27005: Normas internacionales que indican cómo gestionar la seguridad de la información en una empresa. Incluyen controles, principios y formas de evaluar riesgos.

Malware: Nombre general que se da a los programas maliciosos (virus, troyanos, spyware...) diseñados para dañar o controlar un equipo sin permiso.

Phishing: Tipo de estafa que se realiza por correo electrónico u otros medios para hacerse con contraseñas, números de tarjeta o datos sensibles.

Ransomware: Tipo de malware que bloquea los archivos del equipo y pide un "rescate" (pago) para recuperarlos.

Red Wi-Fi pública: Conexión a Internet abierta que puede ser poco segura y facilitar el robo de información.

RGPD: Normativa europea que protege los datos personales. Establece cómo deben recogerse, usarse y protegerse.

Servidor: Ordenador o sistema que ofrece servicios a otros dispositivos, como alojar una página web o enviar correos.

Simulacro de phishing: Ejercicio dentro de una empresa para comprobar si los empleados saben detectar correos falsos.

Smishing: Variante del phishing que se realiza a través de mensajes SMS, normalmente con enlaces engañosos.

Suplantación de identidad: Acción por la cual alguien finge ser otra persona para engañar al destinatario.

TPV (Terminal de Punto de Venta): Dispositivo que permite cobrar mediante tarjeta bancaria en un comercio.

Vishing: Variante del phishing en la que el engaño se realiza por teléfono.

VPN (Red Privada Virtual): Herramienta que crea una conexión segura entre el dispositivo y una red, protegiendo la información que se envía por Internet.

Web segura: Página web que protege la información mediante cifrado. Se reconoce por el candado y las letras “https” en la dirección.

Referencias

Agencia Digital de Andalucía. (2022). *Estrategia Andaluza de Ciberseguridad 2022–2025*. Junta de Andalucía.
https://www.juntadeandalucia.es/organismos/agenciadigitalandalucia.html

ENISA – European Union Agency for Cybersecurity. (2024). *ENISA Threat Landscape 2024: July 2023–June 2024*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

Instituto Nacional de Ciberseguridad (INCIBE). (2020). *Plan Director de Seguridad*.
https://www.incibe.es/protege-tu-empresa

Instituto Nacional de Ciberseguridad (INCIBE). (2021a). *Ciberamenazas contra entornos empresariales: una guía de aproximación para el empresario* (Blog "Protege tu Empresa", 12/01/2021).
https://www.incibe.es

Instituto Nacional de Ciberseguridad (INCIBE). (2021b). *Ciberseguridad en el comercio electrónico: una guía de aproximación para el empresario*. https://www.incibe.es/protege-tu-empresa/guias

Instituto Nacional de Ciberseguridad (INCIBE). (2021c). *Glosario de términos de ciberseguridad: una guía de aproximación para el empresario*. https://www.incibe.es/protege-tu-empresa/guias

Instituto Nacional de Ciberseguridad (INCIBE). (2023). *Guía de recomendaciones para empresas: Ciberseguridad en el comercio electrónico*. Instituto Nacional de Ciberseguridad de España.

International Organization for Standardization. (2018). *ISO/IEC 27000:2018 – Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
https://www.iso.org/standard/73906.html

International Organization for Standardization. (2022a). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.
https://www.iso.org/standard/82875.html

International Organization for Standardization. (2022b). *ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection — Information security controls*.
https://www.iso.org/standard/75652.html

Orden de 3 de octubre de 2024, por la que se aprueban las bases reguladoras para la concesión de subvenciones, en régimen de concurrencia no competitiva, destinadas a mejorar la competitividad y la digitalización del sector comercial y artesano en Andalucía. *Boletín Oficial de la Junta de Andalucía*, núm. 197, 9 de octubre de 2024.

Índice de Ilustraciones

Índice de Tablas

Junta de Andalucía