MINERY REPORT
Military-Grade Cybersecurity Solutions

CIBERTICS

GUÍA PRÁCTICA DE CIBERSEGURIDAD PARA PEQUEÑOS COMERCIOS

Jaén 2025

Junta de Andalucía
Consejería de Empleo, Empresa y Trabajo Autónomo

Comercio Jaén
Federación Empresarial Jiennense de Comercio y Servicios

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

ÍNDICE

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

2. INTRODUCCIÓN

La digitalización de los pequeños comercios ha traído consigo innumerables ventajas, desde la optimización de procesos hasta la expansión de mercados a través de plataformas online. Sin embargo, este avance **también los expone a riesgos cibernéticos** cada vez más sofisticados, que pueden comprometer su operación, reputación e incluso su supervivencia.

A menudo, los **pequeños establecimientos subestiman la importancia de la ciberseguridad**, creyendo que no son un objetivo para los ciberdelincuentes. Sin embargo, los **ataques dirigidos a este sector son cada vez más frecuentes**, precisamente por la percepción de "bajo riesgo" y la falta de medidas de protección adecuadas.

Esta guía tiene como **objetivo proporcionar a los pequeños comercios herramientas prácticas** y recomendaciones accesibles para mejorar su ciberseguridad. En ella se abordarán **medidas básicas de protección**, las principales amenazas a las que se enfrentan y cómo responder ante incidentes. Todo ello diseñado para ser aplicado sin necesidad de grandes recursos o conocimientos técnicos avanzados.

Objetivos de la guía:

1. Concienciar sobre la importancia de la ciberseguridad en el pequeño comercio.
2. Proveer de buenas prácticas y herramientas asequibles para proteger los sistemas y datos.
3. Establecer directrices claras para prevenir y responder a ciberataques.
4. Fomentar una cultura de seguridad digital entre los comerciantes y sus empleados.

Esta guía es un recurso esencial para fortalecer la seguridad digital de los pequeños comercios y garantizar su continuidad en un entorno cada vez más interconectado.

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

3. PRINCIPALES AMENAZAS CIBERNÉTICAS

Los pequeños comercios son cada vez más vulnerables a ataques cibernéticos debido a la percepción de que no representan un objetivo prioritario para los ciberdelincuentes. Sin embargo, su menor nivel de protección los convierte en blancos atractivos. A continuación, se describen las principales amenazas a las que se enfrentan:

1. Phishing

- ¿Qué es?
- Intentos de engañar a los usuarios para que revelen información sensible, como contraseñas, datos bancarios o accesos a sistemas, mediante correos electrónicos o mensajes fraudulentos que parecen legítimos.
- Ejemplo práctico: Un correo falso que simula ser de un proveedor, solicitando un pago urgente a una cuenta bancaria.
- Consejo de protección: Evitar hacer clic en enlaces sospechosos y verificar siempre la autenticidad del remitente.

2. Ransomware

- ¿Qué es?
- Software malicioso que cifra los datos de un sistema, bloqueando su acceso hasta que se pague un rescate.
- Ejemplo práctico: Un comerciante abre un archivo adjunto infectado, lo que bloquea su sistema de facturación y acceso a inventarios.
- Consejo de protección: Realizar copias de seguridad frecuentes y no abrir archivos de fuentes desconocidas.

3. Ingeniería Social

- ¿Qué es?
- Manipulación psicológica de personas para obtener información confidencial o acceso a sistemas.
- Ejemplo práctico: Un atacante llama haciéndose pasar por soporte técnico y solicita credenciales del sistema.
- Consejo de protección: Formar al personal para desconfiar de solicitudes no verificadas de información.

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

4. Malware

- ¿Qué es?
- Software diseñado para infiltrarse en dispositivos y dañar o robar información.
- Ejemplo práctico: Un programa descargado de un sitio no confiable que instala spyware en el equipo.
- Consejo de protección: Utilizar antivirus actualizados y evitar descargas de fuentes desconocidas.

5. Vulnerabilidades en Redes Públicas

- ¿Qué es?
- Uso de redes WiFi no seguras que permiten a atacantes interceptar datos transmitidos.
- Ejemplo práctico: Un empleado accede al sistema de inventarios desde una cafetería sin protección VPN.
- Consejo de protección: Utilizar redes seguras y herramientas como VPN para cifrar las conexiones.

6. Ataques por Fuerza Bruta

- ¿Qué es?
- Intentos automatizados de descifrar contraseñas probando múltiples combinaciones.
- Ejemplo práctico: Un atacante intenta acceder al sistema de pagos de un comercio utilizando contraseñas débiles.
- Consejo de protección: Usar contraseñas complejas y únicas, y habilitar autenticación de doble factor.

Conclusión:

Conocer estas amenazas es el primer paso para protegerse. Los pequeños comercios deben mantenerse alerta y adoptar medidas básicas de prevención para reducir significativamente el riesgo de ser víctimas de ciberataques.

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

4. BUENAS PRÁCTICAS DE SEGURIDAD

Para proteger a los pequeños comercios de las amenazas cibernéticas descritas, es fundamental adoptar una serie de buenas prácticas que permitan prevenir ataques y mitigar sus efectos. Estas prácticas son sencillas de implementar y no requieren una inversión significativa.

1. Uso de Contraseñas Seguras

- Cómo hacerlo:
  - Crear contraseñas únicas para cada servicio, con al menos 12 caracteres, incluyendo letras mayúsculas, minúsculas, números y símbolos.
  - Evitar el uso de datos personales o palabras comunes.
- Herramienta recomendada:
  - Usar gestores de contraseñas para almacenar y generar claves seguras.

2. Habilitación de la Autenticación de Doble Factor (2FA)

- Qué es:
  - Una capa adicional de seguridad que requiere un código temporal o confirmación desde un dispositivo autorizado, además de la contraseña.
- Dónde aplicarla:
  - Correo electrónico, sistemas de gestión de inventarios, plataformas de pago y redes sociales.

3. Actualización Regular de Sistemas

- Por qué es importante:
  - Las actualizaciones corrigen vulnerabilidades conocidas en sistemas operativos, aplicaciones y dispositivos.
- Consejo práctico:
  - Configurar actualizaciones automáticas siempre que sea posible y verificar periódicamente su correcta aplicación.

4. Realización de Copias de Seguridad

- Qué datos incluir:
  - Facturación, inventarios, bases de datos de clientes y otros archivos críticos.
- Frecuencia:
  - Realizar copias diarias o semanales según la actividad del negocio.
- Almacenamiento:
  - Utilizar servicios de almacenamiento en la nube cifrados y dispositivos físicos protegidos.

5. Protección de Dispositivos y Redes

- Dispositivos:
  - Instalar antivirus y habilitar el bloqueo automático de pantalla.
- Redes:
  - Configurar redes WiFi con contraseñas seguras y evitar redes públicas sin usar una VPN.
- Segmentación de redes:
  - Separar las redes de trabajo de las de clientes para mayor seguridad.

6. Formación del Personal

- Temas clave:
  - Reconocimiento de correos sospechosos (phishing).
  - Uso de contraseñas seguras.
  - Respuesta inicial ante incidentes.

7. Revisión de Permisos y Accesos

- Qué revisar:
  - Limitar el acceso a sistemas críticos a personal autorizado.
  - Desactivar cuentas de ex-empleados inmediatamente después de su salida.

Conclusión:

Adoptar estas buenas prácticas no solo protege los sistemas del comercio, sino que también fortalece la confianza de los clientes y garantiza la continuidad del negocio. La implementación de estas medidas debe ser constante y formar parte de la rutina operativa.

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

5. PLAN DE CONTINGENCIA

Un plan de contingencia es una herramienta fundamental para que pequeños y medianos comercios puedan enfrentar incidentes de ciberseguridad de manera organizada, **reduciendo al máximo el impacto sobre sus operaciones** y recuperándose con rapidez. Este apartado ofrece una guía práctica con pasos claros y ejemplos adaptados a las necesidades de este sector.

1. ¿Qué es un Plan de Contingencia y Por Qué Es Importante?

Un plan de contingencia define las acciones específicas que debe tomar un comercio cuando enfrenta un incidente de ciberseguridad. Su importancia radica en:

- **Reducción de impactos:** Permite actuar con rapidez para minimizar daños en sistemas, datos y reputación.
- Continuidad del negocio: Facilita el restablecimiento de operaciones de forma ágil.
- **Protección del cliente:** Garantiza que los datos sensibles de los clientes sean protegidos, evitando pérdida de confianza.
- **Ejemplo:** Si un comercio es víctima de ransomware y sus sistemas de facturación quedan bloqueados, un plan de contingencia permite al responsable del negocio saber a quién notificar, cómo acceder a copias de seguridad y cómo restaurar el sistema sin ceder a las demandas del atacante.

2. Pasos para Diseñar un Plan de Contingencia

PASO 1: IDENTIFICAR LOS ACTIVOS CRÍTICOS

- Hacer una lista de los sistemas, datos y dispositivos esenciales para el funcionamiento del negocio (por ejemplo, punto de venta, inventarios, datos de clientes, cuentas bancarias).
- Priorizar aquellos activos cuya interrupción tendría mayor impacto.
- **Ejemplo:** Un restaurante puede considerar su sistema de reservas y pedidos online como activos críticos, mientras que un comercio de ropa priorizará su control de inventarios y facturación.

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

PASO 2: EVALUAR RIESGOS COMUNES

- Identificar los riesgos más probables (ransomware, pérdida de datos, phishing) y sus posibles consecuencias.
- Establecer un protocolo para cada riesgo identificado.

PASO 3: ESTABLECER ROLES Y RESPONSABILIDADES

- Designar a una persona responsable de coordinar la respuesta ante incidentes.
- Instruir al personal para reconocer señales de ataque y reportarlas de inmediato.
- **Ejemplo:** El encargado del comercio debe saber desconectar el sistema afectado y contactar a un técnico especializado o proveedor de servicios de ciberseguridad.

3. ¿Qué Hacer Durante un Incidente?

Aislar el Problema:

- Si un dispositivo muestra comportamientos extraños (archivos cifrados, mensajes de rescate, accesos no autorizados), desconéctelo inmediatamente de la red WiFi para evitar la propagación del problema.

Notificar a las Personas Clave:

- Comuníquese con el técnico designado o proveedor de soporte IT para evaluar la gravedad del incidente.

Documentar el Incidente:

- Registrar la hora, fecha, tipo de problema y posibles causas. Esto será útil para investigar el ataque y prevenir futuros incidentes.

Ejemplo: Un comercio de alimentación detecta que su sistema de facturación ha sido comprometido. El encargado desconecta el sistema, avisa al técnico y registra los detalles del mensaje sospechoso en pantalla.

4. Recuperación y Restauración

Restaurar Sistemas desde Copias de Seguridad:

- Verifique que las copias de seguridad no estén comprometidas antes de utilizarlas.
- Priorice la recuperación de los sistemas esenciales para las operaciones del comercio.

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

Actualizar y Corregir Vulnerabilidades:

- Una vez restaurados los sistemas, actualícelos para garantizar que no presenten vulnerabilidades conocidas.
- Cambie contraseñas y revise configuraciones de seguridad.

5. Después del Incidente: Mejoras y Prevención

Análisis del Incidente:

- Identifique cómo ocurrió el ataque y qué medidas fallaron.
- Evalúe si el personal necesita capacitación adicional o si se requieren herramientas de protección más avanzadas.

Actualizar el Plan de Contingencia:

- Ajuste el plan para cubrir los problemas detectados durante el incidente.
- **Ejemplo:** Después de un ataque de phishing, un comercio decide incorporar autenticación de doble factor para su sistema de correo y programar capacitaciones regulares sobre cómo reconocer correos fraudulentos.

6. Consejos Clave para Comercios Pequeños y Medianos

- **Práctica regular:** Realice simulacros periódicos de incidentes para evaluar la efectividad del plan y familiarizar al personal con los pasos a seguir.
- **Herramientas sencillas:** Utilice soluciones asequibles y fáciles de implementar, como gestores de contraseñas y copias de seguridad en la nube.
- **Comunicación clara:** Asegúrese de que todos los empleados sepan a quién acudir y qué hacer en caso de incidente.

Conclusión:

Un plan de contingencia bien diseñado no requiere grandes inversiones, pero puede marcar la diferencia entre una interrupción temporal y una crisis prolongada. Para los pequeños y medianos comercios, es una inversión esencial en la continuidad y seguridad de sus operaciones.

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

6. CHECKLIST ANTE INCIDENTES

Este checklist está diseñado para guiar a los pequeños y medianos comercios en la contención de un incidente de ciberseguridad. Las acciones están organizadas en secuencia para garantizar una respuesta rápida, clara y efectiva.

1. Detección del Incidente

□ Identificar señales de ataque:
- ¿Aparece un mensaje sospechoso o de rescate en el sistema?
- ¿Hay actividad inusual en las cuentas o dispositivos?
- ¿Se detecta un acceso no autorizado o archivos cifrados?

□ Notificar al responsable designado:
- Informar al encargado del comercio o técnico de soporte.

□ Documentar detalles iniciales:
- Fecha y hora del incidente.
- Descripción de los sistemas afectados.

2. Aislamiento del Problema

□ Desconectar dispositivos comprometidos de la red:
- Deshabilitar WiFi o desconectar el cable de red.

□ Apagar sistemas no esenciales para limitar la propagación.

□ Prohibir temporalmente el uso de dispositivos no afectados hasta asegurarlos.

3. Notificación y Escalamiento

□ Contactar con soporte técnico:
- Proveer detalles documentados del incidente.

□ Informar a todos los empleados:
- Comunicar qué sistemas no deben usarse.

□ Evaluar si es necesario informar a las autoridades:
- Ataques graves o posibles filtraciones de datos sensibles.

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

4. Contención del Ataque

□ Cambiar contraseñas críticas desde un dispositivo seguro:
- Priorizar accesos a correos electrónicos, sistemas de gestión y banca.

□ Ejecutar un análisis antivirus en los dispositivos afectados:
- Usar herramientas confiables o consultar con un técnico.

□ Bloquear accesos remotos no autorizados.
□ Confirmar que las copias de seguridad no estén comprometidas.

5. Recuperación Inicial

□ Restaurar sistemas críticos desde copias de seguridad seguras.
□ Realizar pruebas en los sistemas restaurados para verificar su funcionamiento.
□ Actualizar software y parches de seguridad antes de reconectar los sistemas a la red.
□ Confirmar la eliminación de cualquier malware identificado.

6. Comunicación con Clientes y Proveedores (si aplica)

□ Informar a los clientes si sus datos pueden haber sido comprometidos:
- Proporcionar pasos claros para protegerse (como cambiar contraseñas).

□ Notificar a proveedores o socios clave sobre posibles retrasos operativos.

7. Evaluación Posterior al Incidente

□ Analizar las causas del incidente:
- ¿Qué permitió el ataque?
- ¿Qué medidas podrían haber prevenido el problema?

□ Actualizar el plan de contingencia:
- Añadir pasos específicos según lo aprendido.

□ Programar una capacitación para el personal:
- Enfocarse en prevención de ataques similares.

□ Realizar auditorías regulares de ciberseguridad.

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

8. Revisión Periódica

□ Planificar simulacros regulares para practicar la respuesta.
□ Revisar y mejorar medidas de protección al menos una vez al año.
□ Establecer un canal de comunicación para reportar problemas futuros.

Nota: Este checklist debe estar fácilmente accesible para todo el personal del comercio y revisarse regularmente para garantizar su efectividad.

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

7. FORMACIÓN Y CONCIENCIACIÓN

La formación y sensibilización son elementos clave para prevenir incidentes de ciberseguridad en pequeños y medianos comercios. La mayoría de los ataques exitosos se producen por desconocimiento o errores humanos, como hacer clic en enlaces fraudulentos o utilizar contraseñas débiles. Este punto ofrece un plan práctico de capacitación y sensibilización para los comerciantes y sus empleados.

1. Objetivo de la Formación

- Incrementar la conciencia sobre las amenazas cibernéticas más comunes.
- Enseñar prácticas de ciberseguridad fáciles de implementar.
- Fomentar un cambio cultural en el que la seguridad digital sea una prioridad cotidiana.

2. Temas Clave para la Capacitación

a. Reconocimiento de Amenazas Comunes

- Identificar correos de phishing: señales de alerta como errores gramaticales, enlaces sospechosos o remitentes desconocidos.
- Entender el riesgo de ransomware: evitar abrir archivos adjuntos de fuentes no verificadas.

b. Gestión Segura de Contraseñas

- Crear contraseñas seguras: al menos 12 caracteres, con combinaciones de números, letras y símbolos.
- Uso de gestores de contraseñas para facilitar la seguridad y reducir errores.

c. Seguridad en Dispositivos y Redes

- Activar autenticación de doble factor en cuentas críticas.
- Evitar redes WiFi públicas o, si es necesario usarlas, conectar mediante una VPN.

d. Copias de Seguridad

- Importancia de realizar copias periódicas.
- Almacenamiento seguro de datos en la nube o en dispositivos externos.

e. Respuesta a Incidentes

- Saber cómo actuar ante un ataque: desconectar dispositivos, notificar al responsable y registrar el incidente.
- Planificación de contingencias básicas.

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

3. Métodos de Formación

a. Talleres Presenciales

- Sesiones prácticas organizadas por asociaciones de comerciantes locales o proveedores de ciberseguridad.
- Simulaciones de ataques de phishing para entrenar al personal.

b. Cursos Online

- Cursos cortos enfocados en ciberseguridad para pequeñas empresas.

c. Recursos Visuales

- Infografías y carteles con buenas prácticas para colocar en lugares visibles del comercio.
- Videos explicativos sobre cómo identificar amenazas.

4. Estrategia de Sensibilización Continua

a. Comunicación Regular

- Enviar boletines mensuales con alertas sobre nuevas amenazas.
- Promover una "política de puertas abiertas" para reportar problemas de seguridad.

b. Reconocimientos Internos

- Incentivar a los empleados que adopten prácticas seguras mediante reconocimientos o pequeños premios.

c. Evaluaciones Periódicas

- Realizar pruebas regulares para medir la efectividad de la formación (ej.: simulacros de phishing).
- Actualizar los contenidos de capacitación según las nuevas amenazas.

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

5. Ejemplo de Programa de Capacitación

Mes 1: Introducción a la Ciberseguridad
- Taller inicial sobre amenazas y buenas prácticas básicas.

Mes 2: Seguridad en Dispositivos
- Sesión sobre contraseñas, autenticación de doble factor y gestión de dispositivos.

Mes 3: Respuesta a Incidentes
- Simulación de un ciberataque y entrenamiento en el plan de contingencia.

Revisión Semestral:
- Evaluación de conocimientos y refuerzo de áreas débiles.

6. Beneficios de la Formación y Sensibilización

- **Reducción de riesgos:** empleados capacitados cometen menos errores que faciliten ataques.
- **Mayor confianza:** clientes y socios verán al comercio como un lugar seguro.
- **Coste reducido:** prevenir es más económico que reparar los daños de un ciberataque.

Conclusión:
Invertir en formación y sensibilización es una estrategia esencial para fortalecer la ciberseguridad de los pequeños y medianos comercios. Los empleados informados y comprometidos son la primera línea de defensa contra amenazas digitales.

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

8. CONCLUSIONES Y PRÓXIMOS PASOS

La ciberseguridad no es un lujo, sino una necesidad para los pequeños y medianos comercios que buscan proteger su operación, reputación y confianza del cliente en un entorno digital cada vez más complejo. Este documento ha presentado herramientas prácticas y accesibles para que los comercios fortalezcan su seguridad digital, pero la clave del éxito radica en su implementación y continuidad.

1. Principales Conclusiones

a. La amenaza es real y creciente:
Aunque los pequeños comercios a menudo se perciben como objetivos secundarios, la realidad es que los ciberdelincuentes buscan empresas con medidas de protección débiles, lo que hace a este sector especialmente vulnerable.
b. La formación es clave:
La falta de conocimiento y sensibilización es una de las principales debilidades detectadas. Los empleados y responsables del comercio son la primera línea de defensa, y necesitan estar preparados para identificar y responder a las amenazas.
c. Las medidas básicas tienen gran impacto:
Acciones simples como el uso de contraseñas seguras, autenticación de doble factor y copias de seguridad periódicas pueden prevenir gran parte de los incidentes más comunes.
d. La planificación asegura la continuidad:
Un plan de contingencia efectivo no solo reduce el impacto de un ataque, sino que también acelera la recuperación y minimiza las pérdidas.

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

2. Recomendaciones de Próximos Pasos

a. Implementar lo aprendido:

- Poner en práctica las buenas prácticas descritas en esta guía.
- Priorizar la formación de empleados en ciberseguridad básica.

b. Revisar y actualizar periódicamente:

- Realizar auditorías internas cada seis meses para evaluar la efectividad de las medidas implementadas.
- Actualizar el plan de contingencia y los procedimientos según las lecciones aprendidas y las nuevas amenazas detectadas.

c. Colaborar con expertos:

- Consultar con profesionales en ciberseguridad para realizar evaluaciones más profundas.
- Participar en programas de capacitación ofrecidos por asociaciones locales o proveedores de seguridad.

d. Difundir la cultura de seguridad digital:

- Involucrar a todos los empleados en el compromiso por la seguridad.
- Compartir las mejores prácticas con otros comercios para fortalecer la comunidad empresarial.

3. Beneficios de la Ciberseguridad para el Comercio

- Protección de datos: Evitar pérdidas financieras y legales por incidentes.
- Confianza del cliente: Posicionar al comercio como un lugar seguro y confiable.
- Continuidad operativa: Minimizar interrupciones y garantizar la sostenibilidad del negocio.

La ciberseguridad no debe verse como un gasto, sino como una inversión esencial en la continuidad y éxito del negocio. Con una planificación adecuada, formación constante y compromiso de todos los implicados, los pequeños y medianos comercios pueden construir una defensa sólida frente a las amenazas digitales y aprovechar las oportunidades del entorno tecnológico con seguridad y confianza.

Paseo de la Castellana Nº 115, 10º izquierda
Madrid, CP 28046
Minery Report S.L.

9. REFERENCIAS Y BIBLIOGRAFÍA

A continuación, se presenta una lista de las fuentes consultadas para la elaboración de esta guía, con el objetivo de respaldar la información presentada y proporcionar recursos adicionales para los pequeños y medianos comercios interesados en profundizar en temas de ciberseguridad.

1. Estándares y Marcos de Referencia

- OWASP Top Ten (2021): Principales vulnerabilidades en aplicaciones web.
- Disponible en: https://owasp.org/www-project-top-ten/
- NIST Cybersecurity Framework: Guía de ciberseguridad basada en riesgos para organizaciones.
- Disponible en: **https://www.nist.gov/cyberframework**
- CIS Controls v8: Controles esenciales para mitigar riesgos cibernéticos.
- Disponible en: https://www.cisecurity.org/controls/

2. Literatura y Documentos Técnicos

- Anderson, R. y Moore, T. (2020). The Economics of Information Security: Risk and Return on Investment in Cybersecurity. Journal of Cybersecurity.
- Symantec (2023). Informe Anual sobre Amenazas de Seguridad.
- Disponible en: https://www.symantec.com/
- INCIBE (2023). Ciberseguridad para PYMEs: Guía Práctica. Instituto Nacional de Ciberseguridad.
- Disponible en: https://www.incibe.es/

4. Enlaces a Normativas y Buenas Prácticas

- Reglamento General de Protección de Datos (RGPD): https://eur-lex.europa.eu/eli/reg/2016/679/oj
- Agencia Española de Protección de Datos (AEPD): Recursos y herramientas para empresas.
- Disponible en: https://www.aepd.es/

5. Estudios y Reportes Complementarios

- ENISA (2023). Threat Landscape Report. Agencia de la Unión Europea para la Ciberseguridad.
- Disponible en: https://www.enisa.europa.eu/
- Microsoft Security (2023). Protección y Gestión de Datos para PYMEs.
- Disponible en: https://www.microsoft.com/security/

Nota:

Se recomienda a los comercios utilizar estas referencias como material de apoyo para ampliar sus conocimientos y fortalecer su seguridad digital. Todas las fuentes son de acceso confiable y ofrecen información actualizada sobre ciberseguridad.

MINERY REPORT
Military-Grade Cybersecurity Solutions

CIBERTICS

GUÍA PRÁCTICA DE CIBERSEGURIDAD PARA PEQUEÑOS COMERCIOS

Jaén 2025

Junta de Andalucía
Consejería de Empleo, Empresa y Trabajo Autónomo

Comercio Jaén
Federación Empresarial Jiennense de Comercio y Servicios