COMERCIO MAYORISTA

SECtoriza2

CIBERSEGURIDAD PARA TU SECTOR

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa

COMERCIO MAYORISTA

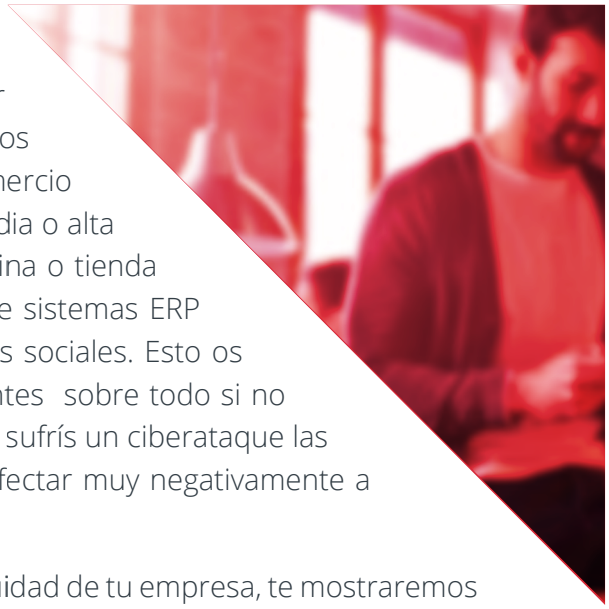
SECtoriza2

CIBERSEGURIDAD PARA TU SECTOR

ÍNDICE

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa

1. INTRODUCCIÓN



Venta o distribución de productos al por mayor en alimentación, electrónica, textil, etc. son algunos ejemplos de actividades incluidas en el sector del comercio mayorista, formado en gran parte por pymes con media o alta dependencia tecnológica, entre otras cosas, con página o tienda web, uso cotidiano del correo electrónico, empleo de sistemas ERP (*Enterprise Resource Planning*) y presencia en las redes sociales. Esto os hace estar en el punto de mira de los ciberdelincuentes sobre todo si no contáis con medidas y políticas de seguridad. Cuando sufrís un ciberataque las consecuencias pueden llegar a parar la actividad y afectar muy negativamente a vuestro negocio.

Para evitar situaciones que puedan afectar a la continuidad de tu empresa, te mostraremos los pasos que debes seguir para proteger la información y los sistemas que la gestionan, así como otros aspectos generales de la ciberseguridad.

2. ¿CONOCES TUS RIESGOS?

Lo que no se mide no se puede mejorar. El primer paso que debes dar para proteger tu negocio es **identificar los riesgos** a los que está expuesto. Seguramente seas consciente de gran parte de ellos, pero quizá existen otros que no conozcas y que, en caso de materializarse, pondrían en graves aprietos a tu empresa.

Para ayudarte a evaluar los riesgos a los que se enfrenta tu organización, te recomendamos utilizar nuestra Herramienta de Autodiagnóstico. A través de una serie de preguntas esta herramienta te guiará para que puedas determinar cuál es el estado actual de ciberseguridad en tu negocio, qué riesgos lo amenazan y qué aspectos debes mejorar.

Análisis de riesgos en 5 minutos

3. UN PASO POR DELANTE

El robo de datos de clientes, contratos con proveedores TIC que no garantizan la ciberseguridad, intentos de acceso remoto a los sistemas, manipulación de las herramientas de *tracking* (seguimiento paquetes), el fraude en comercio electrónico y pérdida de reputación en las redes sociales son algunas de las amenazas que pueden afectar a cualquier negocio de comercio mayorista. Estar al tanto de ellas es esencial para poder evitarlas. Por ello, te aconsejamos suscribirte a nuestro servicio de **boletines** para recibir un mensaje en tu correo electrónico cada vez que se publique un **aviso de seguridad**.

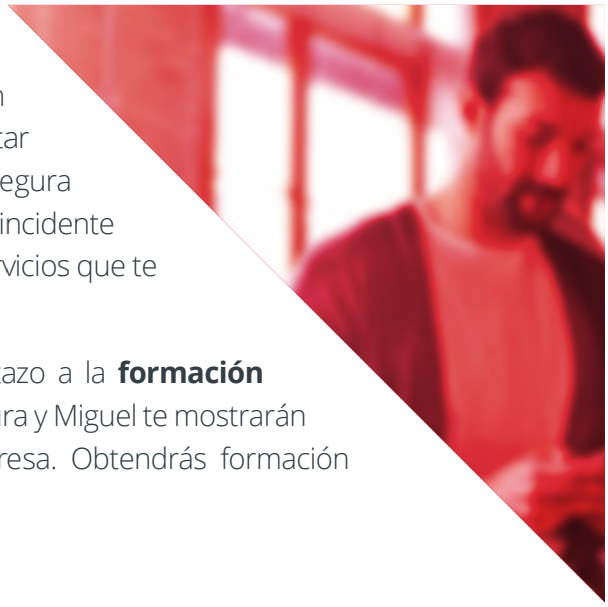
Algunas de las amenazas más comunes que afectan al sector de comercio mayorista tienen su origen en el correo electrónico y mensajes de texto. Los siguientes **avisos de seguridad** son un recopilatorio de los ciberataques más habituales:

- Nueva actualización de seguridad del gestor de contenidos de tiendas online Magento
- Suplantan la identidad de Correos mediante mensajes SMS
- Nueva campaña de correos con adjuntos maliciosos
- Si te llega un reembolso de Endesa, guarda precaución, es un *phishing*
- Campaña de correos electrónicos fraudulentos suplanta a la Agencia Tributaria
- ¡Cuidado no piques! Detectada campaña de *phishing* que suplanta a Bankia
- Campaña de *phishing* suplantando a la entidad bancaria BBVA
- Detectada campaña de *phishing* contra PayPal

Además de detectar las amenazas que llegan a través del correo electrónico, se deben mantener todos los sistemas **actualizados**, con independencia de que sean los utilizados internamente, como los necesarios para dar cualquier servicio desde Internet, como por ejemplo la página web de la empresa. Algunas muestras de este tipo de avisos son:

- Nuevas actualizaciones de la plataforma de formación Moodle
- Si utilizas Magento como gestor de tu comercio electrónico, deberás actualizarlo
- Nueva versión de Joomla!, actualiza tu gestor de contenidos
- Actualización de seguridad de Facebook
- Actualización de seguridad de WordPress
- Nueva actualización de seguridad del navegador web Firefox
- Si tienes la versión 8.7.4 de Drupal, actualiza
- Vulnerabilidad en el escritorio remoto de Windows de versiones antiguas

4. FORMACIÓN Y CONCIENCIACIÓN EN CIBERSEGURIDAD



La formación y la concienciación en ciberseguridad son siempre una apuesta segura. Conocer cómo se debe tratar la información y los sistemas que la gestionan de forma segura es clave para que tu empresa no se vea afectada por un incidente de seguridad. Desde INCIBE hemos desarrollado dos servicios que te ayudarán durante el proceso.

En primer lugar, te recomendamos que eches un vistazo a la **formación sectorial**. Mediante una serie de vídeos interactivos, Laura y Miguel te mostrarán todo lo que tienes que saber para proteger tu empresa. Obtendrás formación específica y personalizada para tu sector.

Itinerarios interactivos, comercio mayorista

Después puedes probar a entrenar a tu equipo en la respuesta a incidentes con un juego de rol. Mediante **diferentes escenarios**, que se dan comúnmente a las empresas del comercio mayorista, tú y los miembros de tu empresa deberéis gestionar distintas situaciones de crisis. Con la práctica de estos retos sentarás las bases para dar una respuesta ordenada y coordinada ante cualquier incidente de seguridad. Aunque tu empresa podría tener que hacer frente a los cinco escenarios, puedes empezar por:

Infección por *ransomware*

Un *phishing* se ha alojado en nuestra página web

Fuga de información

5. APRENDE A PROTEGERTE

En este sector son ampliamente utilizados los servicios de **venta *online***, por lo que uno de los principales riesgos a los que tiene que hacer frente es la suplantación web. Esta técnica, muy utilizada por los ciberdelincuentes, consiste en copiar una página web real y crear otra falsa con el fin de realizar una acción fraudulenta con el objetivo de realizar una estafa o de dañar la imagen y la reputación de la empresa afectada.

La web falsa adopta el diseño de la web que se pretende suplantar e incluso una URL similar, normalmente utilizando técnicas de ***cybersquatting***. De este modo, es más difícil que los compradores perciban el engaño.

Otro de los canales más usados para atacar a negocios de comercio mayorista es el correo electrónico, a través de diferentes métodos como el ***spoofing*** (suplantación de correo electrónico, bien sea de personas o de entidades, con el objetivo de llevar a cabo envío masivo de spam) o el ***spear phishing***, donde los atacantes intentan conseguir datos relevantes mediante un correo aparentemente legítimo.

Existe una tendencia generalizada en el ámbito del comercio, incluido el mayorista, en contratar y utilizar **servicios en la nube**, como son el correo electrónico, el almacenamiento de información y servicios de bases de datos y sistemas de planificación de recursos empresariales ERP (*Enterprise Resource Planning*), principalmente. A pesar de su gran utilidad, también conllevan una serie de riesgos a tener muy en cuenta, como **la pérdida de información, el cese de actividad, sanciones legales o accesos no autorizados.**

La mayoría de los negocios pertenecientes al sector del comercio mayorista trabajan con **información confidencial** que manejan desde todo tipo de equipos y dispositivos, como ordenadores, portátiles, tabletas, móviles, etc. Hoy día ya está muy extendido el uso de dispositivos móviles personales para acceder y utilizar los recursos internos de la empresa, tanto desde dentro como fuera de la protección de la red privada corporativa. Esta metodología se denomina **BYOD (*Bring Your Own Device*)**. A la hora de adoptar esta forma de trabajo, tendremos que tener en cuenta varios factores de riesgo como el **mal uso que se pueda hacer de los dispositivos, el robo de credenciales, el uso de sistemas de conexión no seguros o la sustracción de los propios dispositivos.**

La accesibilidad a la información también es crucial para la mantener la actividad diaria en la compra y venta de productos. El principal incidente de ciberseguridad relacionado con este principio es la **infección por *ransomware***. Este tipo de código malicioso o malware está diseñado para **secuestrar la información** de las víctimas **convirtiendo la información en inaccesible** al cifrar todos los archivos de valor para la organización.

Ante esta situación, el único método que garantiza poder recuperar la actividad laboral sin demasiados impedimentos es **haber realizado con anterioridad copias de seguridad regulares.**

Si te has decidido a implantar soluciones profesionales o has sido víctima de un incidente y necesitas ayuda, en Protege tu empresa disponemos de un **Catálogo de empresas y soluciones de ciberseguridad** donde encontrarás las soluciones y servicios que más se adaptan a tus necesidades. Podrás aplicar distintos filtros para que la búsqueda sea más exacta según los requisitos de tu organización.

Dosieres

- Protección de la información
- Plan de Contingencia y Continuidad de Negocio
- Protege a tus clientes

Guías

- Copias de seguridad: una guía de aproximación para el empresario
- *Cloud computing*: una guía de aproximación para el empresario
- Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario

Políticas de seguridad

- Respuesta a incidentes
- Actualizaciones de *software*

Historias reales

- Historias reales: el ciberdelincuente le «pescó» por su falta de formación
- Historias reales: mi trabajo robaron y mi proyecto plagiaron
- Historias reales: mi página web trabajaba en la mina

Artículos del blog

- Black Friday y Cyber Monday a prueba de plagios
- *Cybersquatting*, qué es y cómo protegerse
- Protección de datos en la nube en el comercio mayorista

Reporte de fraude y ayuda al empresario

- Reporte de fraude
- Línea de Ayuda en Ciberseguridad

Catálogo de empresas y soluciones de ciberseguridad

- Seguridad en la nube
- Seguridad en dispositivos móviles
- Gestión de incidentes

6. REFERENCIAS

Para acceder a los enlaces de las secciones anteriores utiliza la versión digital del documento o navega por las siguientes secciones del portal:

1. INCIBE – Protege tu empresa – Blog - **https://www.incibe.es/protege-tu-empresa/blog**

2. INCIBE – Protege tu empresa – Avisos de seguridad - **https://www.incibe.es/protege-tu-empresa/avisos-seguridad**

3. INCIBE – Protege tu empresa - RGPD para pymes - **https://www.incibe.es/protege-tu-empresa/rgpd-para-pymes**

4. INCIBE – Protege tu empresa – Dosieres - **https://www.incibe.es/protege-tu-empresa/que-te-interesa**

5. INCIBE – Protege tu empresa – Kit de concienciación - **https://www.incibe.es/protege-tu-empresa/kit-concienciacion**

6. INCIBE – Protege tu empresa - ¿Conoces tus riesgos? - **https://www.incibe.es/protege-tu-empresa/conoces-tus-riesgos**

7. INCIBE – Protege tu empresa - Herramientas de ciberseguridad - **https://www.incibe.es/protege-tu-empresa/herramientas**

8. INCIBE – Protege tu empresa – Formación - **https://www.incibe.es/protege-tu-empresa/formacion**

9. INCIBE – Protege tu empresa – Guías - **https://www.incibe.es/protege-tu-empresa/guias**

10. INCIBE – Protege tu empresa - Sellos de confianza - **https://www.incibe.es/protege-tu-empresa/sellos-confianza**

11. INCIBE – Protege tu empresa - Reporte de fraude - **https://www.incibe.es/protege-tu-empresa/reporte-fraude**

12. INCIBE - Línea de Ayuda en Ciberseguridad - **https://www.incibe.es/linea-de-ayuda-en-ciberseguridad**

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa