LOGÍSTICA

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

LOGÍSTICA

SECtoriza2

CIBERSEGURIDAD PARA TU SECTOR

ÍNDICE

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD 017 protege tu empresa

1. INTRODUCCIÓN

Empresas de almacenamiento y explotación de infraestructuras para el transporte, actividades postales, transporte y distribución de productos o pasajeros, etc. Las compañías de este sector utilizan diferentes tecnologías como las apps para dispositivos móviles, escaneo de documentos, plataformas online, IoT, herramientas de *tracking* (seguimiento de paquetes), etc., imprescindibles para que la actividad diaria no se detenga. También gestionan información personal de clientes, que debe estar protegida adecuadamente para evitar fugas de información que puedan afectar a los usuarios y a la empresa.

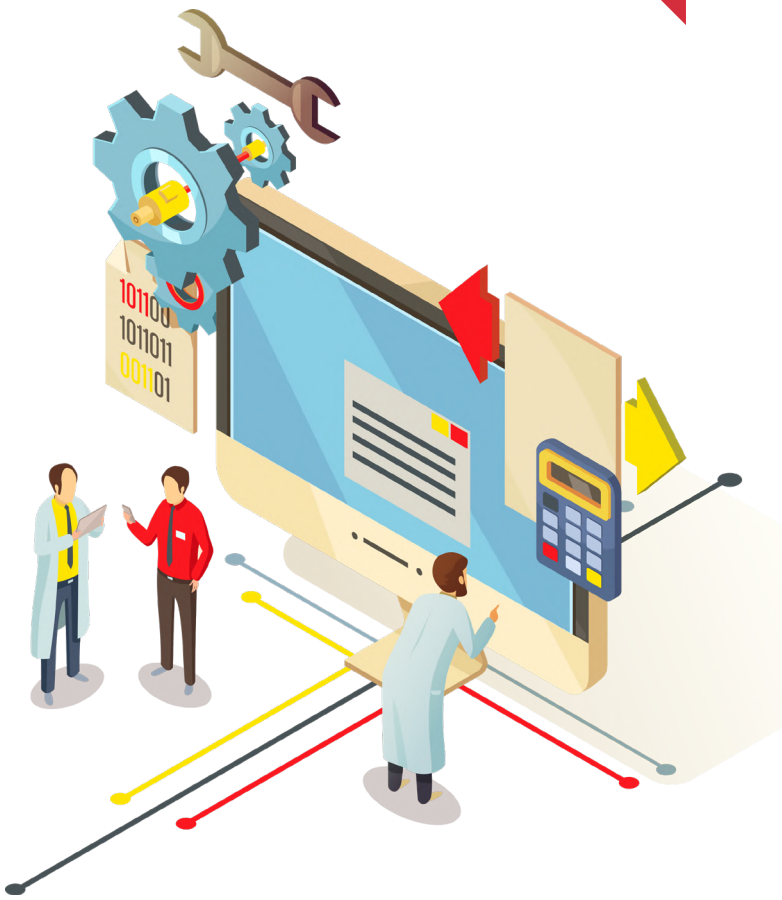
Si quieres evitar situaciones que puedan afectar a la continuidad de los servicios que ofreces o que puedan comprometer la imagen y reputación de la empresa, te mostraremos unos pasos que deberás tener en cuenta para proteger la información y los sistemas que la gestionan.

2. ¿CONOCES TUS RIESGOS?

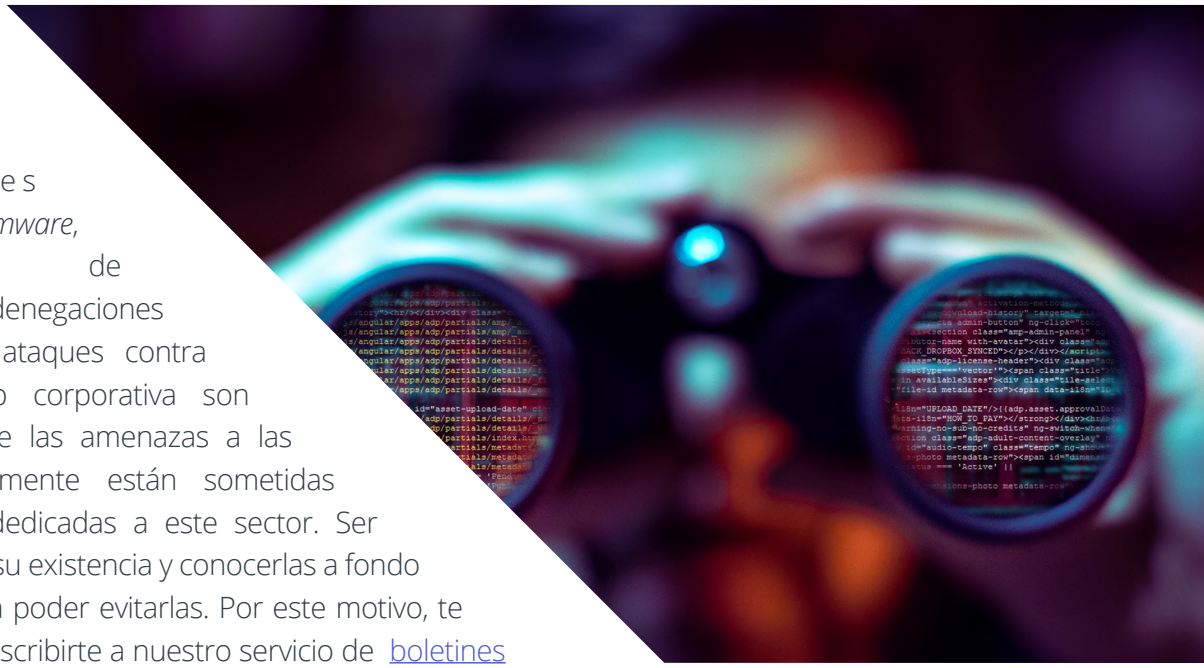
Lo que no se mide no se puede mejorar. El primer paso que debes dar para proteger tu negocio es **identificar los riesgos** a los que está expuesto. Seguramente seas consciente de gran parte de ellos, pero quizá existen otros que no conozcas y que, en caso de materializarse, pondrían en graves aprietos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



Fugas de información, ciberataques de *ransomware*, suplantaciones de identidad, denegaciones de servicio o ataques contra la página web corporativa son solo algunas de las amenazas a las que constantemente están sometidas las empresas dedicadas a este sector. Ser conscientes de su existencia y conocerlas a fondo es esencial para poder evitarlas. Por este motivo, te aconsejamos suscribirte a nuestro servicio de boletines para recibir un mensaje en tu correo electrónico cada vez que se publique algún aviso de seguridad.

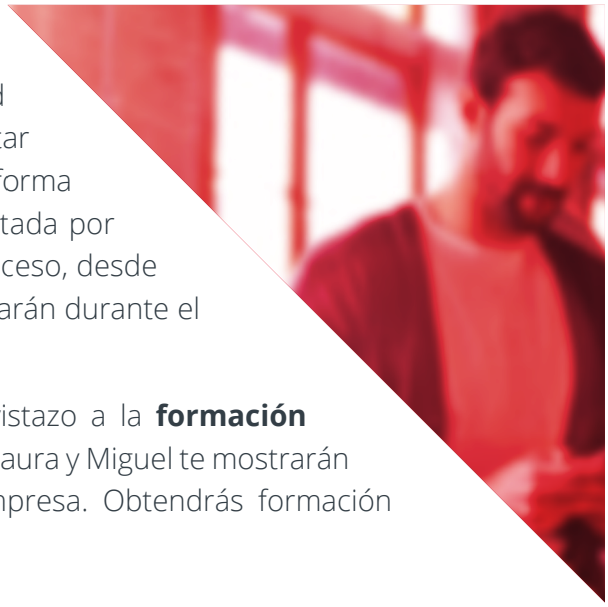
Las amenazas más comunes que afectan a las asociaciones tienen su origen en el correo electrónico. Los siguientes **avisos de seguridad** son un recopilatorio de ejemplos de ataques que más ha sufrido este sector:

- Detectada campaña de correos maliciosos. Mucho cuidado con los aumentos del salario
- Intentan suplantar al Ministerio de Economía y Empresa
- Suplantan la identidad de Correos mediante mensajes SMS
- Campaña de correos electrónicos fraudulentos suplanta a la Agencia Tributaria
- Campaña de correos electrónicos fraudulentos que trata de extorsionar a sus víctimas
- Si te llega un reembolso de Endesa, guarda precaución, es un *phishing*
- Nueva oleada de ransomware: cuidado con las macros
- Envío de falsos presupuestos en Excel como adjuntos maliciosos

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:

- Nueva versión de seguridad de WordPress. ¡Actualiza tu web!
- Nueva actualización de seguridad del gestor de contenidos de tiendas online Magento
- Nueva versión de Joomla!, actualiza tu gestor de contenidos
- Actualización de seguridad de Outlook para Android
- Nueva actualización de seguridad del navegador web Firefox
- Actualiza a la nueva versión de Drupal
- Nueva actualización de Oracle Java SE
- 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 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. Para ayudarte en este proceso, 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 videos 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, logística

Después puedes probar a entrenar a tu equipo en la respuesta a incidentes con el Juego de rol. Por medio de **diferentes escenarios**, que afectan comúnmente a las empresas del sector logística, tú y los miembros de tu empresa deberéis gestionar distintas situaciones de crisis. Mediante 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:

Fuga de información

Ataque por ngeniería social

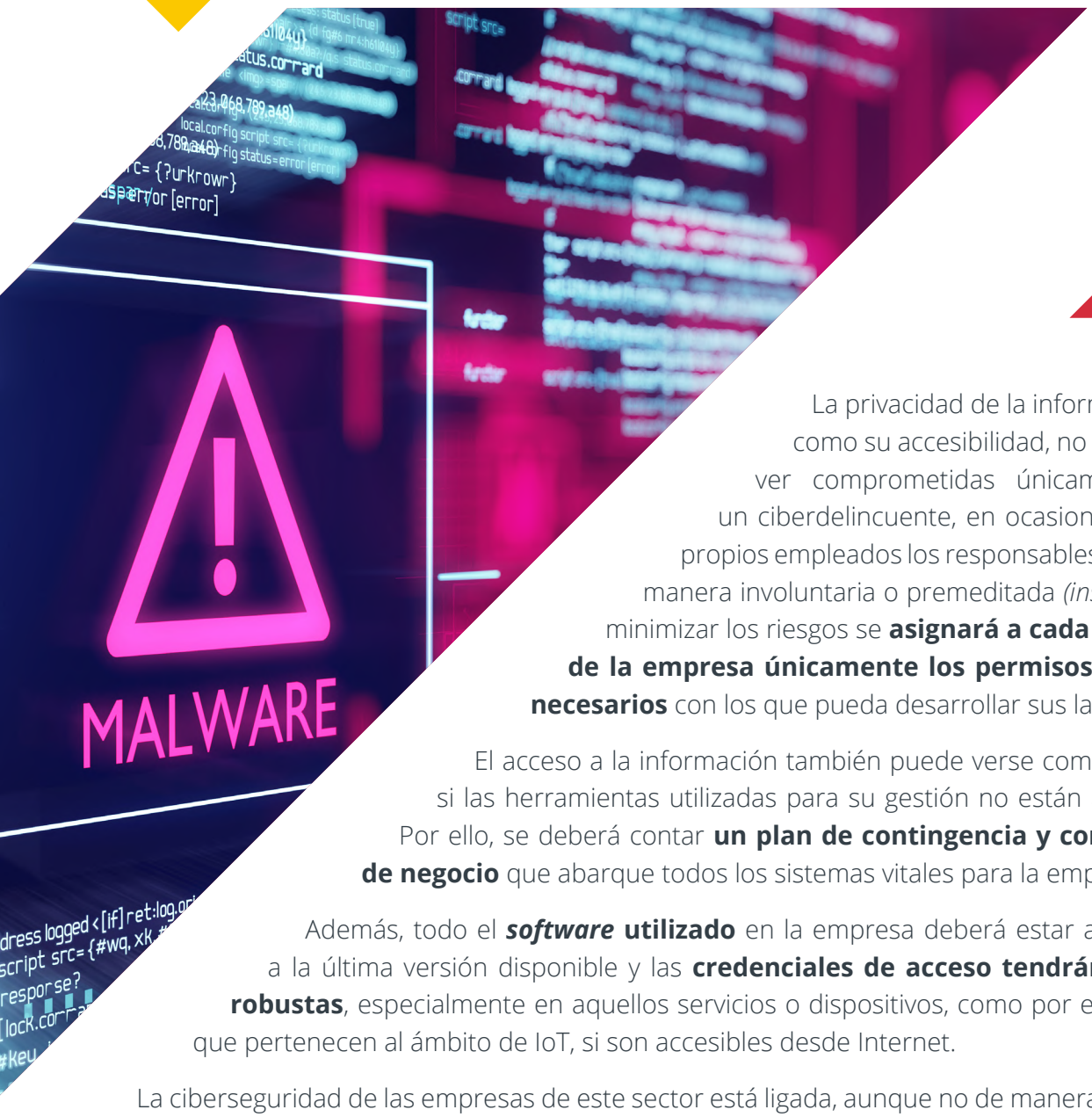
Infección por *ransomware*

5. APRENDE A PROTEGERTE

Este sector es ampliamente utilizado por usuarios de **comercio electrónico** para realizar el seguimiento de sus pedidos (tracking) vía web o a través de apps, por lo que uno de los principales riesgos a los que tiene que hacer frente es la **suplantación de identidad**. Esta técnica, muy utilizada por los ciberdelincuentes, consiste en suplantar una página web legítima por otra falsa con el fin de realizar una acción fraudulenta. Para prevenir este tipo de acciones maliciosas, se deberá **indicar a los usuarios de la forma más clara posible, y que no dé lugar dudas, cómo acceder a la información de seguimiento de su pedido**.

Las páginas web que realizan suplantaciones de identidad muchas veces utilizan nombres de dominio similares al legítimo, con el objetivo de dar más verosimilitud a la página fraudulenta, una técnica conocida como ***cybersquatting***. Para prevenir esta técnica es recomendable **monitorizar el nombre de dominio utilizado por la empresa**, y en caso de encontrar alguno que pueda estar realizando acciones fraudulentas, notificarlo a la autoridad pertinente.

La información es otra pieza clave, **mantener su privacidad y accesibilidad será fundamental**. El primer paso consistirá en **implementar una política de copias de seguridad**. De esta forma, se protegerá la información ante cualquier clase de error o ataque informático, como puede ser un *ransomware*.



La privacidad de la información, así como su accesibilidad, no se pueden ver comprometidas únicamente por un ciberdelincuente, en ocasiones son los propios empleados los responsables, ya sea de manera involuntaria o premeditada *(insider)*. Para minimizar los riesgos se **asignará a cada miembro de la empresa únicamente los permisos mínimos necesarios** con los que pueda desarrollar sus labores.

El acceso a la información también puede verse comprometido si las herramientas utilizadas para su gestión no están accesibles. Por ello, se deberá contar **un plan de contingencia y continuidad de negocio** que abarque todos los sistemas vitales para la empresa.

Además, todo el ***software* utilizado** en la empresa deberá estar actualizado a la última versión disponible y las **credenciales de acceso tendrán que ser robustas**, especialmente en aquellos servicios o dispositivos, como por ejemplo los que pertenecen al ámbito de IoT, si son accesibles desde Internet.

La ciberseguridad de las empresas de este sector está ligada, aunque no de manera exclusiva, a la autenticidad e integridad de los documentos que se manejan (albaranes de entrega, facturas, pedidos...). La **firma electrónica** es la herramienta que proporciona la suficiente garantía legal para la gestión de este tipo de documentos, y también aporta validez legal, agilidad, trazabilidad y seguridad, que se suman al ahorro de costes administrativos asociados a la digitalización documental.

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

- Plan director de seguridad
- Protege a tus clientes
- Plan de contingencia y continuidad de negocio

Guías

- Copias de seguridad: una guía de aproximación para el empresario
- Ransomware: una guía de aproximación para el empresario
- Cómo gestionar una fuga de información. Una guía de aproximación al empresario

Políticas de seguridad

- Respuesta a incidentes
- Protección de la página web
- Actualizaciones de software

Historias reales

- Historias reales: el ciberdelincuente le «pescó» por su falta de formación
- Historias reales: web segura cumpliendo la ley
- Historias reales: suplantaron a mi proveedor y a mi empresa estafaron

Artículos del blog

- Plan de contingencia y continuidad de negocio, ¿qué herramientas necesito?
- Aprende a detectar el *cybersquatting* contra tu marca
- La confianza en trámites en el sector logística, transporte y suministros
- Medidas de prevención contra ataques de denegación de servicio
- ¿Realmente necesito toda la información que almaceno?

Catálogo de empresas y soluciones de ciberseguridad

- Prevención de fuga de información
- Contingencia y continuidad
- Auditoría técnica
- Control de acceso y autenticación

Reporte de fraude y ayuda al empresario

- Reporte de fraude
- Línea de Ayuda en Ciberseguridad

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