INDUSTRIA

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

INDUSTRIA

SECtoriza2

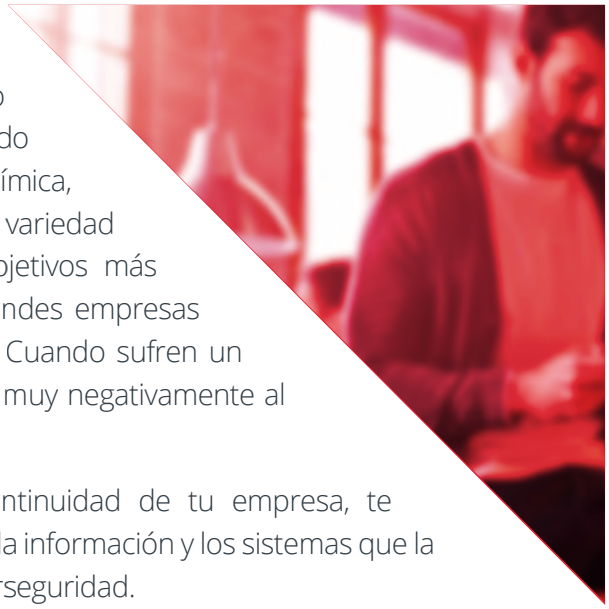
CIBERSEGURIDAD PARA TU SECTOR

ÍNDICE

1. INTRODUCCIÓN pág. 03
2. ¿CONOCES TUS RIESGOS? pág. 04
3. UN PASO POR DELANTE pág. 05
4. FORMACIÓN Y CONCIENCIACIÓN EN CIBERSEGURIDAD pág. 07
5. APRENDE A PROTEGERTE pág. 09
6. REFERENCIAS pág. 13

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa

1. INTRODUCCIÓN



Realización de procesos industriales, fabricación o transformación de materiales en productos, mecanizado o fabricación de piezas (plástico, metal...), industria química, agroalimentaria o farmacéutica, son una muestra de la variedad del sector industrial. La mayoría pymes, que son objetivos más fáciles de atacar por los ciberdelincuentes que las grandes empresas con medidas y políticas de seguridad más restrictivas. Cuando sufren un ciberataque, las consecuencias pueden llegar a afectar muy negativamente al 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 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, ataques de *ransomware, phishing*, suplantaciones de identidad, *software* con vulnerabilidades, espionaje industrial o seguridad física en el trabajo son algunas de las amenazas que pueden afectar a cualquier industria. Estar al tanto de ellas es esencial para poder evitarlas. Por ello, te recomendamos suscribirte a nuestro servicio de Boletines. Gracias a este servicio recibirás un mensaje en tu correo electrónico cada vez que se publique algún Aviso de seguridad.

Algunas de las amenazas más comunes que afectan al sector de industria tienen su origen en el correo electrónico y mensajes de texto. Los siguientes **avisos de seguridad** son un recopilatorio de los ataques más comunes que sufre tu sector:

- Suplantan la identidad de Correos mediante mensajes SMS
- Campaña de correos electrónicos fraudulentos suplanta a la Agencia Tributaria
- Si te llega un reembolso de Endesa, guarda precaución, es un phishing
- ¡Cuidado no piques! Detectada campaña de phishing que suplanta a Bankia
- Campaña de phishing suplantando a la entidad bancaria BBVA
- WhatsApp avisa sobre un fallo de seguridad en varios sistemas operativos
- Detectada campaña de phishing contra PayPal

Además de detectar las amenazas que llegan a través del correo electrónico y los SMS, se deben mantener todos los sistemas **actualizados**, tanto los utilizados en los dispositivos de los trabajadores como los utilizados para dar cualquier servicio desde Internet, como por ejemplo la página web de la compañía. Algunos ejemplos de este tipo de avisos son:

- Nuevas actualizaciones de la plataforma de formación Moodle
- Nueva actualización de seguridad del gestor de contenidos de tiendas online Magento
- Nueva versión de Joomla!, actualiza tu gestor de contenidos
- Actualización de Oracle Java SE
- Actualización de seguridad de WordPress
- Vulnerabilidad en los procesadores Qualcomm que afecta a dispositivos Android
- Si tienes la versión 8.7.4 de Drupal, actualiza

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, industria

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 a las industrias, 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 industria podría tener que hacer frente a los cinco escenarios, puedes empezar por:

Fuga de información

Un *phishing* se ha alojado en nuestra página web

Infección por *ransomware*

5. APRENDE A PROTEGERTE

Las pymes de este sector elaboran productos en áreas muy variadas y, en gran medida, tienen una **alta dependencia de las nuevas tecnologías**, utilizando equipos informáticos, conexiones a redes locales e inalámbricas y dispositivos móviles, en muchos casos para el control de sus sistemas de producción.

En las empresas de este sector, los posibles incidentes de seguridad y los desastres pueden dañar vuestra capacidad operativa, repercutiendo negativamente tanto económicamente como en vuestra imagen y reputación, haciendo peligrar la **continuidad de vuestro negocio**. Para mitigar los efectos negativos de los incidentes, las empresas, en particular en sectores industriales, deben contar con un **Plan de Contingencia y Continuidad de Negocio** que regule los mecanismos a poner en marcha en estos casos.

La accesibilidad a la información también es crucial para la correcta actividad diaria de una industria. El principal incidente de seguridad 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 cualquier incidente de seguridad relacionado con un *ransomware*, el único método que garantiza poder recuperar la actividad laboral sin demasiados impedimentos es **haber realizado con anterioridad copias de seguridad regulares.**

Adicionalmente, en el ámbito industrial es de gran utilidad realizar un registro de toda la información generada por los distintos procesos en ejecución. Para ello, es recomendable implementar una **política de gestión de *logs***, que facilite la tarea de registro y clasificación de la información generada por los eventos más significativos dentro de vuestra compañía.

La **formación de los empleados** también debe tenerse en cuenta, ya que estos conforman el eslabón más importante en la cadena de seguridad por lo que hay que fortalecerlo. Contar con un plan de formación dirigido a los empleados marcará la diferencia y reducirá considerablemente el riesgo de sufrir un incidente de ciberseguridad como, por ejemplo, una **fuga de información**, ya sea de manera **accidental, intencionada** por un miembro de la organización o *insider*, o por medio de un ataque externo llevado a cabo por **ciberdelincuentes**.

Mantener los componentes ***software* actualizados a la última versión disponible** debe ser otra de las cuestiones ineludibles en cualquier organización. Se debe contar con una **política de actualizaciones** que tenga en cuenta todo tipo de equipos, incluidos equipos de red, de videoconferencia, impresoras, móviles, dispositivos IoT y de control industrial, ya que todos ellos están expuestos a ser atacados por ciberdelincuentes.

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

Políticas de seguridad

- Continuidad de negocio
- Plan director de seguridad

Guías

- Gestión de riesgos. Una guía de aproximación para el empresario
- Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario
- Cómo gestionar una fuga de información. Una guía de aproximación al empresario

Historias reales

- Historias reales: trabaja seguro desde tu móvil o tu tableta
- Historias reales: aumento de beneficios gracias a un plan de contingencia y continuidad del negocio
- Historias reales: suplantaron a mi proveedor y a mi empresa estafaron

Artículos del blog

- ¿Ya tienes tu Plan de Recuperación ante Desastres?
- ¿Necesitas más información? Utiliza tu registro de log
- La continuidad de negocio en la industria

Reporte de fraude y ayuda al empresario

- Reporte de fraude
- Línea de Ayuda en Ciberseguridad

Catálogo de empresas y soluciones de ciberseguridad

- Contingencia y continuidad
- Gestión de incidentes
- Protección de las comunicaciones

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