SERVICIOS PROFESIONALES

SECtoriza2

CIBERSEGURIDAD PARA TU SECTOR

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

SERVICIOS PROFESIONALES

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

protege tu empresa

1. INTRODUCCIÓN

Gestorías, bufetes de abogados, asesorías, inmobiliarias, estudios de arquitectura o de fotógrafos son algunos ejemplos que muestran la variedad del sector servicios profesionales. Gran parte de estas empresas son pymes y autónomos, que son también objetivos más fáciles de atacar por los ciberdelincuentes que las grandes empresas con medidas y políticas de seguridad más restrictivas. Cuando una de estas empresas sufre un ciberataque, las consecuencias de este pueden llegar a ser nefastas para el negocio.

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

2. ¿CONOCES TUS RIESGOS?

Análisis de riesgos en 5 minutos

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.

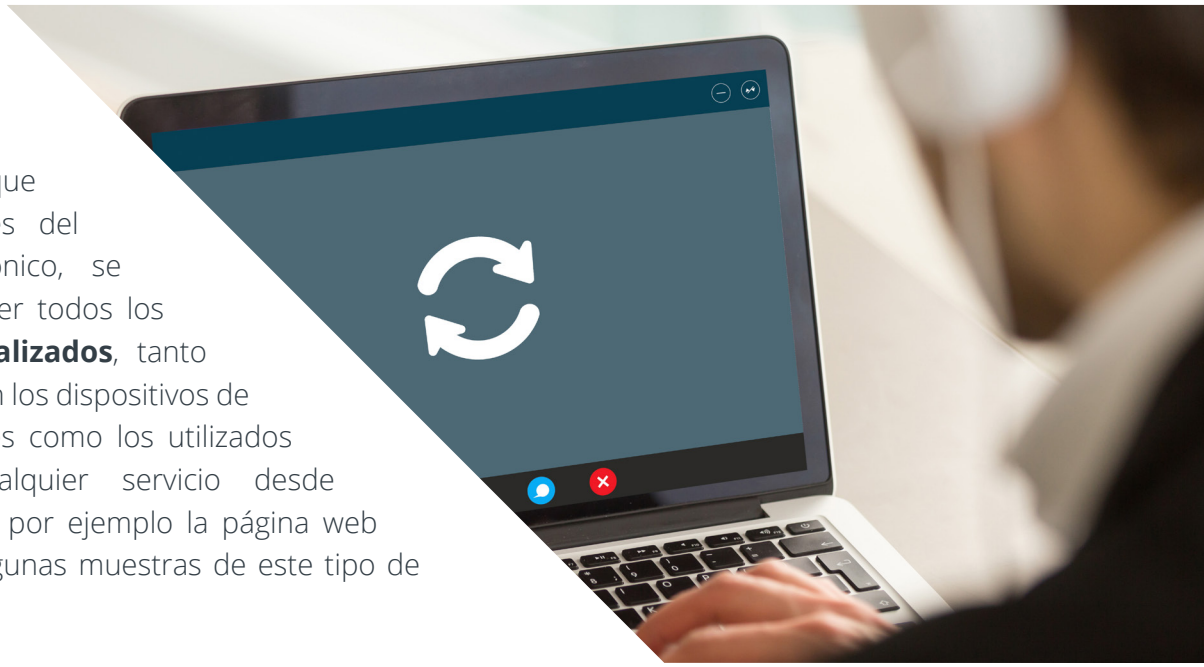
Para ayudarte a evaluar los riesgos a los que se enfrenta tu organización, te recomendamos utilizar nuestra Herramienta de Autodiagnóstico. A través de una serie de preguntas, esta herramienta te guiará para que puedas determinar cómo es el estado actual de ciberseguridad en tu negocio, qué riesgos lo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

3. UN PASO POR DELANTE

Ataques de *ransomware*, *phishing*, suplantaciones de identidad, software con vulnerabilidades, son algunas de las amenazas que pueden afectar a cualquier servicio profesional. Conocerlas 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 un Aviso de seguridad.

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

- Si te llega un reembolso de Endesa, guarda precaución, es un phishing
- ¡Cuidado no piques! Detectada campaña de phising que suplanta a Bankia
- Campaña de phishing suplantando a la entidad bancaria BBVA
- Nueva campaña de phishing que intenta suplantar a Mapfre
- Detectada nueva campaña de correos de sextorsión
- Campaña de ransomware suplantando a la Agencia Tributaria
- 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**, tanto los utilizados en los dispositivos de los trabajadores como los utilizados para dar cualquier servicio desde Internet, como por ejemplo la página web corporativa. Algunas muestras de este tipo de avisos son:

- Actualización de Oracle Java SE
- Nueva versión de WordPress, ¡actualiza!
- Si tienes la versión 8.7.4 de Drupal, actualiza
- Nueva versión de Joomla! Actualiza tu gestor de contenidos
- Actualización de seguridad de Outlook para Android
- Nueva actualización de seguridad del navegador web Firefox
- ZombieLoad: problemas de seguridad en procesadores de INTEL
- Vulnerabilidad en el escritorio remoto de Windows de versiones antiguas

4. FORMACIÓN Y CONCIENCIACIACIÓN 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, servicios profesionales

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 servicios profesionales, 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 sector profesional podría tener que hacer frente a los cinco escenarios, puedes empezar por:

Infección por ransomware

Fuga de información

Ataque por ingeniería social.

5. APRENDE A PROTEGERTE

Debido a su actividad, los despachos de profesionales gestionan **gran cantidad de información confidencial**. Si esta se viera afectada por un incidente de seguridad, las repercusiones para el negocio podrían ser muy graves. La información de una empresa puede verse afectada principalmente por dos tipos de incidentes de seguridad: el ***ransomware*** y las **fugas de información.**

El ***ransomware*** es un tipo de código malicioso o malware diseñado para **secuestrar la información** de las víctimas y que estas no puedan acceder a su contenido. El malware se encargará de cifrar todo archivo que pueda ser de valor para tu empresa, como hojas de cálculo, archivos de texto, imágenes, videos, archivos editables de software específico o bases de datos. Todo el tiempo de trabajo invertido en esos archivos no habrá servido de nada ya que estarán bajo control de los ciberdelincuentes. Habitualmente este tipo de código malicioso se enviaba mediante **campañas de correos electrónicos fraudulentos**, sin embargo estas técnicas están evolucionando y actualmente se decantan por utilizar servicios de escritorio remoto vulnerables.

Ante cualquier tipo de incidente de seguridad relacionado con un *ransomware*, el único método que garantiza poder recuperar la actividad laboral sin demasiados inconvenientes es **realizar copias de seguridad regularmente**. Para prevenir estos ataques hay que prestar atención a los correos electrónicos, especialmente si contienen enlaces o documentos adjuntos. También es necesario proteger el escritorio remoto en caso de ser accesible desde Internet.

Las **fugas de información** son el otro tipo de incidente cuyas consecuencias pueden ser muy graves. ¿Qué sucedería si te robaran o perdieras información confidencial de tus clientes, seguirían confiando en tu empresa o se pasarían a la competencia y esa pérdida podría tener consecuencias legales?

Las fugas de información se producen de tres formas distintas: **accidental, intencionada** por un miembro de la organización o insider, o por medio de un ataque externo llevado a cabo por **ciberdelincuentes**. Las causas pueden ser muy variadas pero principalmente, cuando la fuga se ha producido por causas internas en la organización, esta suele deberse a la **inexistencia o debilidad de los controles de seguridad** en el acceso a la información.

Los ciberdelincuentes pueden ser el origen de la fuga de información, mediante ***malware*** procedente de correos electrónicos o páginas **web de tipo *phishing*** pueden hacerse con información confidencial. Esta información robada será vendida posteriormente, incluso puede que a la competencia más cercana.

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
- Buenas prácticas en el área de informática

Guías

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

Políticas de seguridad

- Clasificación de la información
- Control de accesos

Historias reales

- Historias reales: me intentaron estafar con un video íntimo
- Historias reales: a mi empresa suplantaron y a mis clientes engañaron
- Historias reales: Soy tu nueva factura y te voy a secuestrar el ordenador

Artículos del blog

- ¿Es seguro tu escritorio remoto?
- DLP protege tus datos contra fugas de información
- Despachos de profesionales, la ciberseguridad llama a vuestra puerta

Reporte de fraude y ayuda al empresario

- Reporte de fraude
- Línea de Ayuda en Ciberseguridad

Catálogo de empresas y soluciones de ciberseguridad

- Prevención de fuga de información
- Contingencia y continuidad
- Implantación de soluciones

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
MINISTERIO DE ECONOMÍA Y EMPRESA

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa