ASOCIACIONES

SECtoriza2

CIBERSEGURIDAD PARA TU SECTOR

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

ASOCIACIONES

SECtoriza2

CIBERSEGURIDAD PARA TU SECTOR

ÍNDICE

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

1. INTRODUCCIÓN

Desde organizaciones empresariales, patronales o sindicales, pasando por aquellas que promueven ideas o actividades políticas y culturales, las asociaciones son en su mayoría un grupo formado por pequeñas y medianas empresas que se caracterizan por representar los intereses de un grupo de personas, conocidos como socios o miembros. La razón de ser de las asociaciones reposa **en la confianza que sus socios depositan en ellas**. Un fallo de seguridad, una infección por *ransomware*, una fuga de datos personales o críticas mal gestionadas en las redes sociales pueden quebrar esta confianza. Por este motivo, es esencial proteger la reputación y mantener seguros los sistemas, la página web, el servidor de correo o la información que manejan.

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 asociación, te mostraremos unos pasos que deberás tener en cuenta para proteger la información y los sistemas que la gestionan.

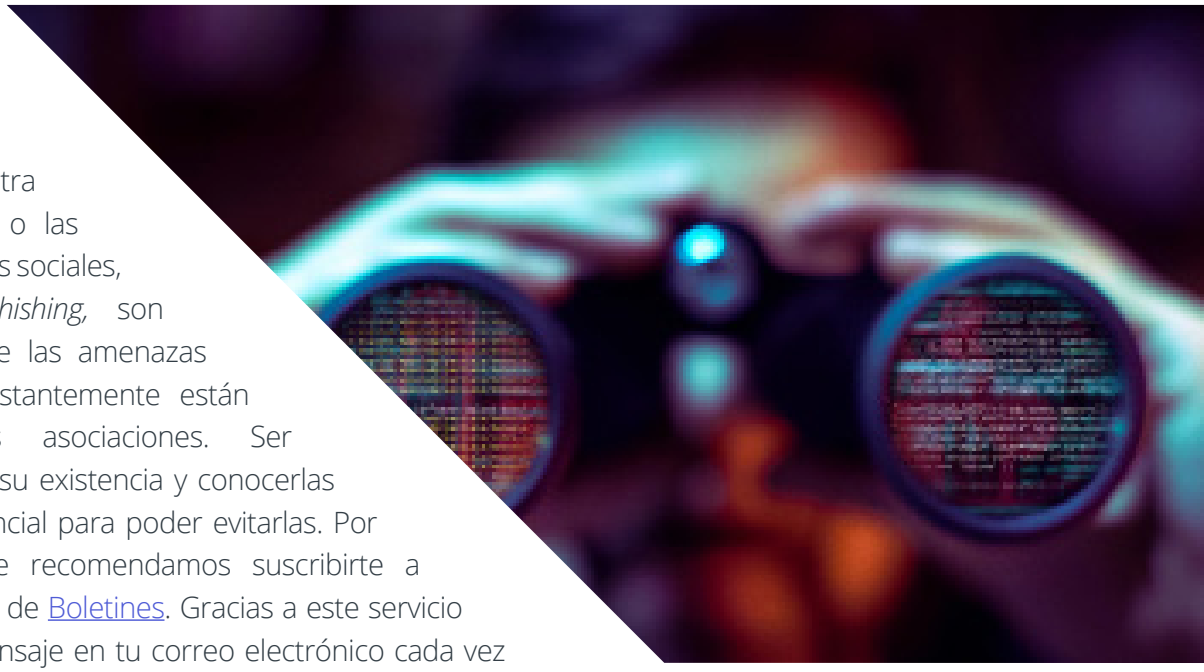
2. ¿CONOCES TUS RIESGOS?

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

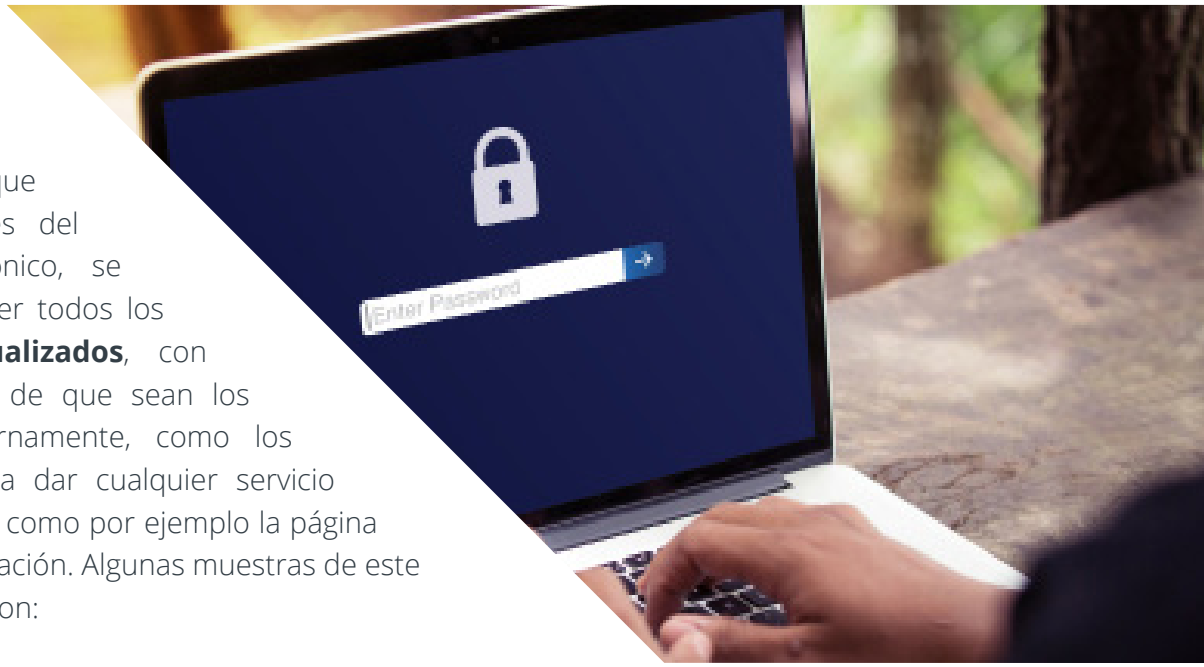
3. UN PASO POR DELANTE



Fugas de información, ataques contra la página web o las cuentas de redes sociales, *ransomware, phishing,* son solo algunas de las amenazas a las que constantemente están sometidas las asociaciones. Ser conscientes de su existencia y conocerlas a fondo es esencial para poder evitarlas. Por este motivo, 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.

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 phishing para robar credenciales de WordPress**
- **Campaña de "spear phishing" suplantando al servicio web 1&1**
- **Si te llega un reembolso de Endesa, guarda precaución, es un phishing**
- **Campaña de phishing suplantando a la entidad bancaria BBVA**
- **Detectada nueva campaña de correos de sextorsión**
- **Campaña de ransomware suplantando a la Agencia Tributaria**
- **Oleada de correos maliciosos suplantando a Vodafone ONO**
- **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 asociación. Algunas muestras de este tipo de avisos son:

- Vulnerabilidad en los procesadores Qualcomm que afecta a dispositivos Android
- Nueva actualización del gestor de contenidos WordPress
- 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
- 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, 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:

Fuga de información

Un phishing se ha alojado en nuestra página web

Infección por *ransomware*

5. APRENDE A PROTEGERTE

Las organizaciones que forman parte del sector asociaciones **basan su funcionamiento en la confianza con sus socios**. Si esta se viera afectada por un incidente de seguridad, el futuro de la asociación podría estar en entredicho. El principal reto al que se enfrenta cualquier tipo de asociación es **proteger los datos de sus asociados y evitar cualquier tipo de fuga de información**. El tipo de información puede, en el caso de asociaciones de carácter político o si se trata de datos de menores o de salud por ejemplo, ser de carácter sensible, y por ello está especialmente protegida por la legislación, por lo que se deben aplicar una serie de **medidas y controles de seguridad para protegerla, como puede ser el cifrado de la misma o llevar un control de acceso.**

Una fuga de información puede ser **accidental** o **intencionada**, causada por un miembro de la organización o *insider* o provocada 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.

La accesibilidad a la información también es crucial para la correcta actividad diaria de la asociación. 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 e impedir que puedan acceder a su contenido, **convirtiendo la información en inaccesible**.

El *ransomware* cifrará todo archivo que pueda ser de valor para la asociación. Comúnmente, este tipo de código malicioso se suele enviar mediante **campañas de correos electrónicos fraudulentos**, aunque los ciberdelincuentes siempre están innovando siendo en la actualidad uno de sus métodos favoritos, los escritorios remotos vulnerables. El único método que garantiza recuperar la actividad laboral y que la infección no sea demasiado nociva es **la realización regular de copias de seguridad**.

Hay que prestar mucha atención a los correos electrónicos, especialmente si contienen enlaces o documentos adjuntos. Además, en caso de contar con servicios accesibles desde Internet, como el escritorio remoto, tendremos que implantar mecanismos de seguridad que protejan y eviten accesos no autorizados.

Para cualquier organización, tener una página web vulnerable o una cuenta de una red social que haya podido verse comprometida sería nefasto. Además de la información gestionada, **los diferentes servicios que se utilizan o se ofrecen por la asociación a través de su página web tienen que estar debidamente protegidos**. Por ello será importante aplicar los últimos **parches de seguridad en la web** y proteger el acceso a los servicios por medio de **credenciales de acceso robustas y únicas para cada servicio** y, siempre que sea posible, habilitar el **doble factor de autenticación**.

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

- Protege a tus Clientes
- Protección de la información
- Protege tu web

Políticas de seguridad

- Control de acceso
- Uso de técnicas criptográficas

Guías

- Copias de seguridad: una guía de aproximación para el empresario
- Ransomware: una guía de aproximación para el empresario
- Ciberseguridad en la identidad digital y la reputación online. Una guía de aproximación para el empresario
- Cómo gestionar una fuga de información. Una guía de aproximación al empresario

Historias reales

- Historias reales: me intentaron estafar con un video íntimo
- Historias reales: envié correos spam sin saberlo y me han bloqueado
- Historias reales: Soy tu nueva factura y te voy a secuestrar el ordenador

Artículos del blog

- En cooperativa, la ciberseguridad es más efectiva
- Cómo funciona la firma electrónica y por qué usarla en asociaciones
- Celebra con nosotros el Día Internacional de las Cooperativas
- Día Mundial de las Contraseñas, ¿aún utilizas 123456?
- ¿Es seguro tu escritorio remoto?

Catálogo de empresas y soluciones de ciberseguridad

- Prevención de fuga de información
- Anti-malware
- WAF Web Application Firewall

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
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa