EDUCACIÓN

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

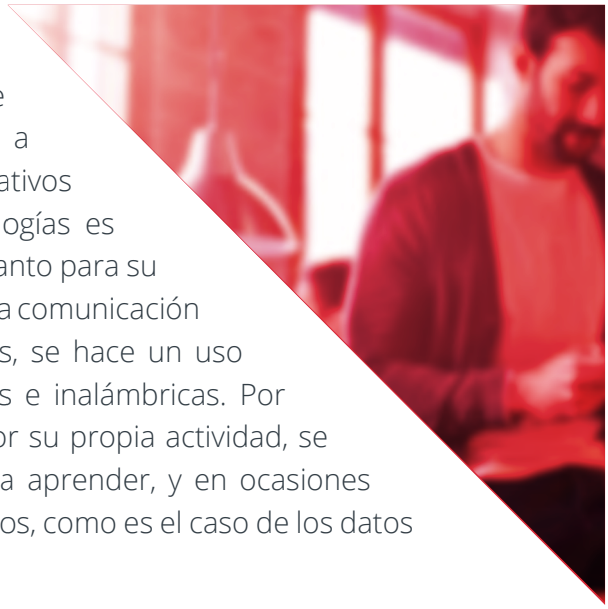
EDUCACIÓN

SECtoriza2

CIBERSEGURIDAD PARA TU SECTOR

ÍNDICE

1. INTRODUCCIÓN



El sector de la educación engloba todo tipo de organizaciones que se dedican a la enseñanza o a actividades culturales y deportivas, como centros educativos o academias. La implantación de las nuevas tecnologías es importante en este tipo de instituciones y empresas, tanto para su actividad didáctica y sus procesos internos como para la comunicación con otros centros, alumnos, profesores, etc. Además, se hace un uso intensivo de equipos informáticos y redes cableadas e inalámbricas. Por último, cabe resaltar que en estas organizaciones, por su propia actividad, se tratan datos de las personas que se matriculan para aprender, y en ocasiones estos datos pueden ser de los especialmente protegidos, como es el caso de los datos de menores o de salud.

Si perteneces a este sector y quieres evitar situaciones que puedan afectar a la continuidad de los servicios que ofreces o comprometer la imagen y reputación de tu negocio, te mostraremos los pasos que debes 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. Por ello, el primer paso que debes dar para proteger tu negocio es **identificar los riesgos** a los que está expuesto. Seguramente seas consciente de algunos, pero quizá existen otros que no conozcas y que, en caso de materializarse, pondría 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

Algunas de las amenazas que afectan a las empresas de este sector son ataques de *ransomware*, fugas de información, denegaciones de servicio, suplantaciones de identidad o ataques contra la página web corporativa. 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**, y así, recibirás un mensaje en tu correo electrónico cada vez que se publique algún **aviso de seguridad**.

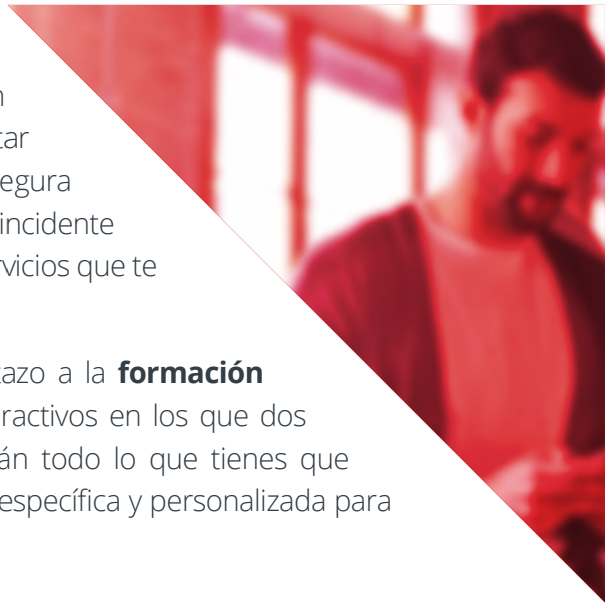
Los ciberataques más comunes llegan a las empresas a través del correo electrónico. Los siguientes **avisos de seguridad** son un recopilatorio de ejemplos de correos que se utilizan para atacar a organizaciones de este y otros sectores:

- 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 el correo electrónico, los navegadores o los propios sistemas operativos, así como los necesarios para dar cualquier servicio desde Internet, como por ejemplo, la página web del centro. 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



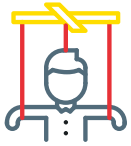
La formación y la concienciación en ciberseguridad son siempre una apuesta segura. Conocer cómo se debe tratar la información y los sistemas que la gestionan de forma segura es clave para que tu centro no se vea afectado por un incidente de seguridad. Desde INCIBE hemos desarrollado dos servicios que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

En primer lugar, te recomendamos que eches un vistazo a la **formación sectorial**. Consiste en una serie de cortos vídeos interactivos en los que dos empresarios de tu sector, Laura y Miguel, te mostrarán todo lo que tienes que saber para proteger tu empresa. Obtendrás formación específica y personalizada para empresas dedicadas a la educación.

Itinerarios interactivos, educación

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 en las empresas del sector educación, 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:

Fuga de información



Ataque por ingeniería social

Infección por *ransomware*

5. APRENDE A PROTEGERTE

Los centros educativos se caracterizan por una alta implementación de las nuevas tecnologías en los procesos internos, además de para fomentar su uso entre los alumnos. También hacen, en muchos casos, un uso intensivo de los sistemas de comunicación, en particular a través de dispositivos móviles. Por ello, el primer paso será **proteger la red privada de la organización** de accesos no autorizados, en caso de disponer de **conexión wifi se deberá proteger adecuadamente.** Se establecerá una **contraseña robusta** y **se desactivará la función WPS**. Si la organización ofrece conexión wifi a los clientes esta será una subred distinta a la utilizada por la organización de forma interna. El acceso al *router* también se protegerá por medio de credenciales robustas. Por último, las tomas que dan **acceso a la red por medio de cable Ethernet también se deberán proteger**, evitando que estas se encuentren en lugares públicos o con poco control.

No hay que olvidar también **implementar una política de copias de seguridad**. De esta forma, se salvaguardará la información ante cualquier clase de error o ataque informático como puede ser un *ransomware*. No menos importante es verificar que todos los **sistemas utilizados en la organización están actualizados a la última versión disponible**. Así, se corregirán las vulnerabilidades descubiertas y se contará con las últimas funciones implementadas por los desarrolladores.

Al gestionar datos personales de los usuarios, donde puede haber información sobre menores o salud, **se seguirán las pautas indicadas en la LOPDGDD y el RGPD**. Mantener su privacidad y

accesibilidad, además de un derecho de los alumnos, **es fundamental** para asegurar la continuidad del centro educativo. Tener identificados todos los procesos en los que intervienen este tipo de datos, verificar quién los puede tratar y utilizar el **cifrado** cuando sea necesario, son algunas medidas que tendremos que tomar y que además de proteger la privacidad de nuestros alumnos nos evitará algunas sanciones y daños de imagen en caso de que ocurra algún incidente.

Por eso, estos datos, y en general toda la información del centro, se deben proteger de accesos no autorizados. **Los miembros de la organización únicamente tendrán los permisos necesarios para desempeñar su labor**. El cifrado de los datos es otra forma de protegerlos ya que únicamente serán accesibles por quien conozca la contraseña de descifrado. Además, esta deberá ser lo más robusta posible.

Nuestra actividad también puede verse comprometida si las herramientas utilizadas para la gestión de nuestros procesos quedaran, por alguna causa, inaccesibles o inactivas. Por ello, se debe contar un **plan de contingencia y continuidad de negocio** que abarque todos los sistemas necesarios para el desarrollo de la docencia.

Los docentes, administrativos y otras personas en la organización también deben estar formados en materia de ciberseguridad, de manera que conozcan las prácticas que pueden suponer riesgos para la seguridad del centro.

Si te has decidido a implantar soluciones profesionales o has sido víctima de un incidente de seguridad y necesitas ayuda, en **Protege tu empresa** disponemos de un [Catálogo de empresas y soluciones de ciberseguridad] donde puedes encontrar empresas que ofrecen todo tipo de servicios y productos. Aplicando distintos filtros encontrarás soluciones adecuadas a las necesidades de tu organización.

¡Echa un vistazo a estos recursos seleccionados para las empresas de tu sector!

Dosieres

- Protege a tus clientes
- Protección de la información
- Buenas prácticas en el área de informática

Políticas de seguridad

- Almacenamiento en la red corporativa
- Concienciación y formación
- Prevención de fuga de información
- Contingencia y continuidad
- Auditoría técnica

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

Artículos del blog

- Prevenir la fuga de información en el sector educativo
- ¿Realmente necesito toda la información que almaceno?
- Cómo evitar incidentes relacionados con los archivos adjuntos al correo
- Seguimiento y finalización de contrato en un servicio subcontratado
- Día Mundial del Correo: cómo detectar correos fraudulentos

Historias reales

- Historias reales: me intentaron estafar con un video íntimo
- Historias reales: envié correos *spam* sin saberlo y me han bloqueado
- Historias reales: la ciberseguridad como valor diferencial

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