TURISMO Y OCIO

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

TURISMO Y OCIO

SECtoriza2

CIBERSEGURIDAD PARA TU SECTOR

ÍNDICE

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

protege tu empresa

1. INTRODUCCIÓN

Hoteles, gimnasios, restaurantes, locales de ocio, agencias de viajes... El sector servicios, debido a su actividad laboral, gestiona una gran cantidad de información personal de los clientes, así como las reservas y horarios elegidos.

Puesto que los **datos personales de los clientes son vitales para cualquier empresa**, ya que de ellos depende el correcto funcionamiento de la misma, ante un incidente en el que se vieran involucrados la compañía podría sufrir graves consecuencias legales o que afecten a su continuidad o a la confianza de los clientes.

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, sigue los siguientes pasos. De este modo, protegerás 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.

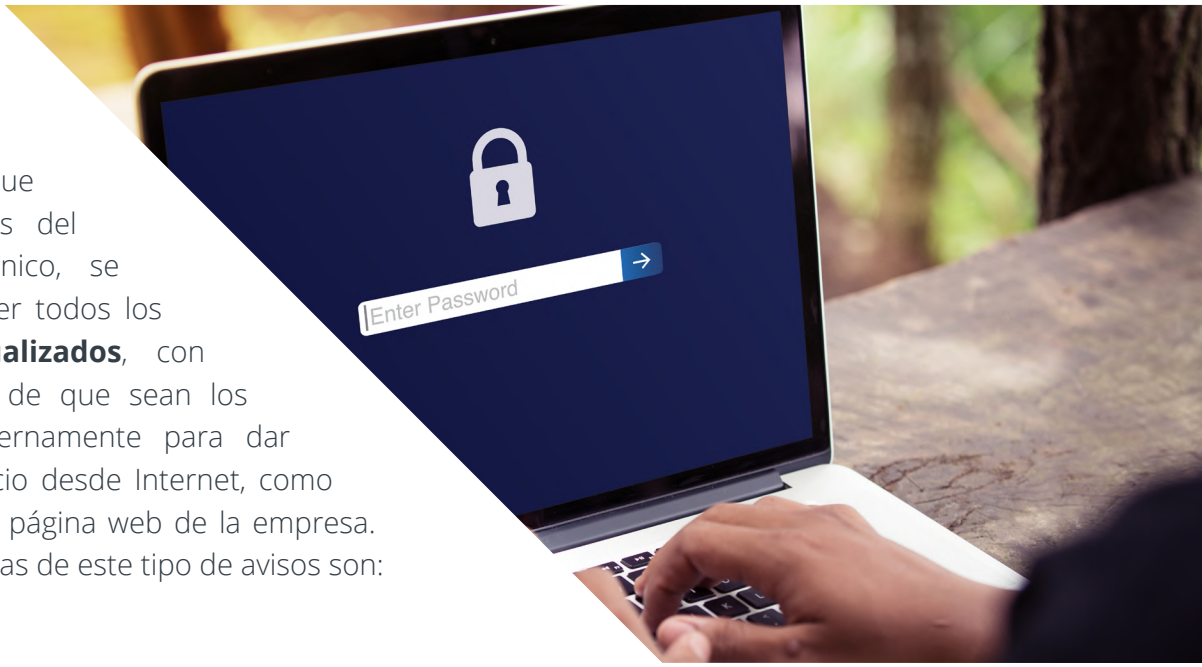
Análisis de riesgos en 5 minutos

3. UN PASO POR DELANTE

Fugas de información, ciberataques de ransomware y phishing o contra la página web, relación con proveedores TIC, uso de redes inalámbricas o acceso remoto a los sistemas, son solo algunas de las amenazas a las que constantemente están sometidas las empresas dedicadas al sector servicios. 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 empresas de turismo y ocio 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
- Nueva campaña de correos con adjuntos maliciosos
- Envío de falsos presupuestos en Excel como adjuntos maliciosos
- Suplantan la identidad de Correos mediante mensajes SMS
- Detectada campaña de phishing para robar credenciales de WordPress
- Detectada nueva campaña de correos de sextorsión
- Si te llega un reembolso de Endesa, guarda precaución, es un phishing



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 empleados internamente 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 versión de Joomla!, actualiza tu gestor de contenidos
- Actualización de seguridad de Outlook para Android
- Vulnerabilidad en el escritorio remoto de Windows de versiones antiguas
- Actualización de seguridad de Outlook para Android
- Nueva actualización de seguridad del navegador web Firefox
- Actualiza a la nueva versión de Drupal
- Vulnerabilidades en Microsoft Internet Explorer y Microsoft Defender. ¡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, turismo y ocio

Después puedes probar a entrenar a tu equipo en la respuesta a incidentes con el Juego de rol. Por medio de **diferentes escenarios**, que que afectan comúnmente a las empresas de turismo y ocio, tú y los miembros de tu organización 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 ngeniería social

Infección por *ransomware*

5. APRENDE A PROTEGERTE

La información personal de los clientes quizá sea el activo más valioso de las empresas que pertenecen al sector servicios. Su disponibilidad y privacidad es clave para mantener la confianza de los clientes y el correcto funcionamiento del negocio. Por ello, se ha de **minimizar el riesgo y las consecuencias de un incidente** que afecte a información de la empresa, independientemente de que su origen sea interno o externo a la misma.

La primera medida de seguridad a llevar a cabo es realizar **copias de seguridad de forma periódica** de la información más importante de la empresa. La información seleccionada será aquella que es vital para la organización y **sin la cual no podría desempeñar sus labores cotidianas**.

Controlar quién accede a la información es otra de las cuestiones a tener en cuenta para evitar fugas de información. Se ha de **establecer una política de control de accesos** que restrinja quién accede a un determinado activo, de forma que cada empleado únicamente pueda acceder a la información que es imprescindible para su trabajo.

Para evitar miradas indiscretas que afectan a la información más crítica de la empresa, bien sea de trabajadores malintencionados *(insiders)* o ciberdelincuentes, **se utilizarán herramientas de cifrado**. Mediante el cifrado la información no será legible a no ser que se conozca su clave de descifrado.

Uno de los t**ipos de malware más perjudiciales que afectan a las empresas de este sector es el *ransomware***, que utiliza técnicas de cifrado en contra del propietario de la información, haciendo que los activos sean inaccesibles. Ante esta amenaza, la mejor forma de protección es la prevención, por

ello, como ya se mencionó antes, **se deben realizar copias de seguridad de manera periódica**. Las copias de seguridad se **almacenarán en un lugar seguro, solamente se conectará el soporte o servicio utilizado en el momento de realizar la copia o restaurarla**, ya que en caso contrario, ante una infección el *ransomware*, podría afectar también a la copia de seguridad.

Mantener todo el software y sistemas operativos actualizados a la última versión disponible **corregirá las vulnerabilidades** descubiertas, evitando así que los ciberdelincuentes puedan explotarlas, y además, se aprovecharán las últimas funcionalidades implementadas por parte de los desarrolladores.

Se contará también en **todos los dispositivos empresariales con *software* antivirus**. Este tipo de soluciones detecta e impide que se infecten los equipos con multitud de *malware*.

Las **credenciales** utilizadas para acceder a cualquier recurso corporativo deberán ser **robustas y únicas para cada servicio**, así se evitarán ataques basados en fuerza bruta. Además, en caso de que un servicio se vea comprometido no se verán afectados el resto, ya que las credenciales son distintas.

El **correo electrónico** es la principal vía de infección por malware que afecta a las empresas. Para evitarlo, se debe prestar especial atención a **correos cuyo remitente es desconocido y que contengan enlaces o documentos adjuntos**. En caso de duda, se intentará contactar con el remitente por un canal alternativo como el teléfono y, en caso de no ser posible, se eliminará del buzón.

Si te has decidido a implantar soluciones profesionales o has sido víctima de un incidente y necesitas ayuda, en **Protege tu empresa** de INCIBE 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
- Protege a tus clientes
- Contratación de servicios

Políticas de seguridad

- Control de acceso
- Protección contra la página web

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
- Decálogo ciberseguridad empresas: una guía de aproximación para el empresario

Historias reales

- Historias reales: web segura cumpliendo la ley
- Historias reales: mi empresa se había convertido en un Gran Hermano
- Historias reales: suplantaron a mi proveedor y a mi empresa estafaron

Artículos del blog

- Medidas básicas de ciberseguridad en el sector turístico
- Prevenir los ataques de ingeniería social en las empresas de ocio
- Protégete frente al *defacement* y que no le cambien la cara a tu web
- Protección del puesto de trabajo. Escenarios de riesgo
- ¿Realmente necesito toda la información que almaceno?

Catálogo de empresas y soluciones de ciberseguridad

- Prevención de fuga de información
- Antimalware
- Protección de las comunicaciones

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