SALUD

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

SALUD

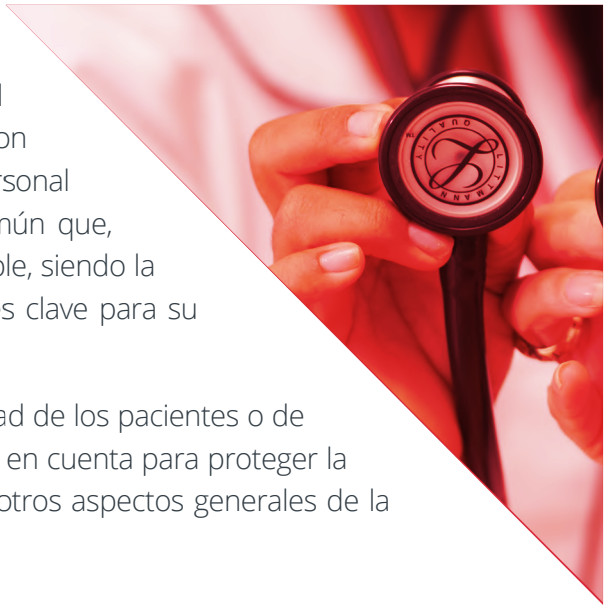
SECtoriza2

CIBERSEGURIDAD PARA TU SECTOR

ÍNDICE

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa

1. INTRODUCCIÓN



Clínicas de todo tipo, especialistas sanitarios, personal de enfermería y obstetricia, laboratorios o farmacias son algunos ejemplos de empresas de este sector. El personal de estas empresas es muy variado pero tiene en común que, de una manera u otra, gestiona información muy sensible, siendo la privacidad y disponibilidad de esta información factores clave para su negocio.

Para evitar situaciones que puedan afectar a la privacidad de los pacientes o de la 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.

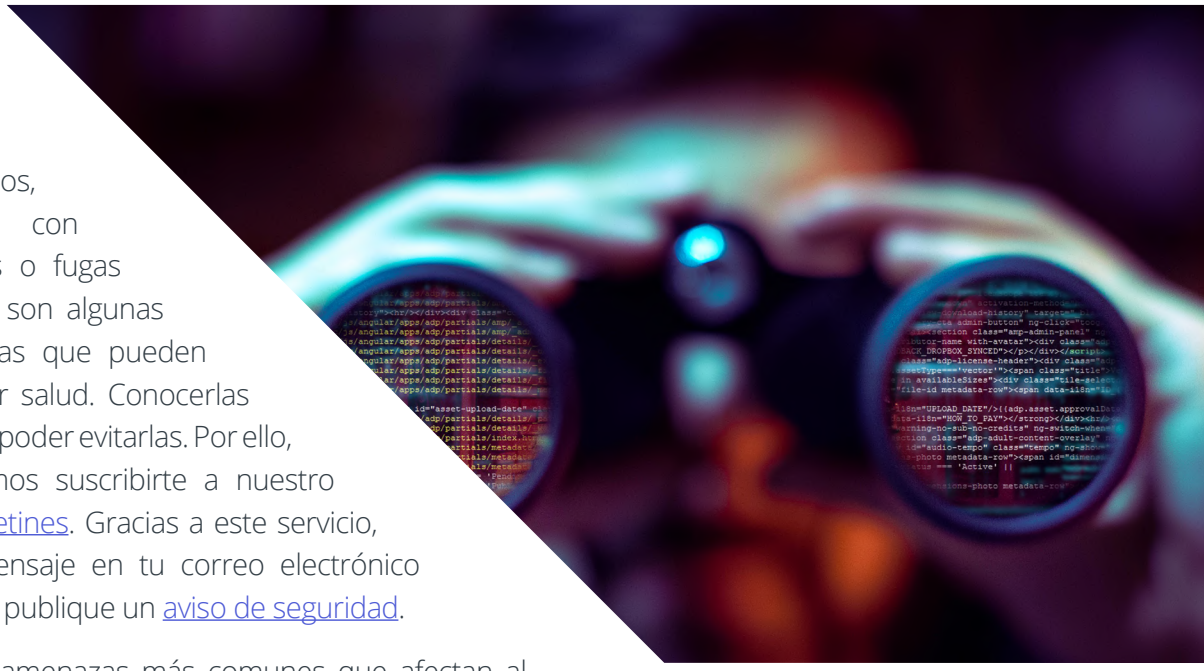
2. ¿CONOCES TUS RIESGOS?

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



Ataques de *ransomware*, correos maliciosos, *software* con vulnerabilidades o fugas de información son algunas de las amenazas que pueden afectar al sector salud. 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 salud 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:

- Intentan suplantar al Ministerio de Economía y Empresa
- Campaña de correos electrónicos fraudulentos suplanta a la Agencia Tributaria
- Campaña de phishing suplantando a la entidad bancaria BBVA
- Nueva campaña de phishing que intenta suplantar a Mapfre
- Nueva campaña de correos con adjuntos maliciosos
- Detectada nueva campaña de correos de sextorsión
- 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, como por ejemplo la página web corporativa. Algunas muestras de este tipo de avisos son:

- Nueva versión de Joomla!, actualiza tu gestor de contenidos
- Actualización de seguridad de WordPress
- Si tienes la versión 8.7.4 de Drupal, actualiza
- Nueva actualización de Oracle Java SE
- Vulnerabilidad 0-day en el navegador Internet Explorer
- Vulnerabilidad en el escritorio remoto de Windows de versiones antiguas
- Vulnerabilidades en Microsoft Internet Explorer y Microsoft Defender. ¡Actualiza!
- ZombieLoad: problemas de seguridad en procesadores de INTEL

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, salud

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 salud, 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 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

Las organizaciones en este sector gestionan datos sensibles, como los que afectan a la salud de los pacientes y, en ocasiones, datos genéticos o datos biométricos. Las fugas de información son uno de los principales incidentes de seguridad que afectan a este tipo de datos, y pueden producirse de tres formas distintas:

· **Accidental** por error o desconocimiento,

· **Intencionada** por un miembro de la organización o insider,

· 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.

Las fugas de información también pueden ser **originadas por un ciberdelincuente**, mediante malware, correos de tipo phishing o aprovechando vulnerabilidades presentes en los sistemas de la empresa. La información robada puede poner en riesgo la seguridad y la privacidad de los pacientes y de la propia empresa, pudiendo además incurrir en un delito. Para evitar este tipo de situaciones se debe **aplicar una serie de medidas de seguridad técnicas y organizativas** que minimicen el riesgo de accesos no autorizados o fugas de información.

Los datos relativos a salud, biometría o genética son considerados **datos especialmente protegidos en el RGPD**, por lo que se deberán aplicar medidas organizativas y de seguridad específicas para su protección.

Otro aspecto a tener en cuenta es el **acceso a la información**. ¿Cuáles serían las consecuencias de sufrir un incidente de seguridad relacionado con ransomware que imposibilitara el acceso a los resultados de las pruebas médicas de un paciente o a su historial? El acceso a la información es crítico para el correcto desempeño de las labores de la empresa, para ello se deberán aplicar las medidas de seguridad necesarias que lo garanticen. Ante esto, la mejor defensa es contar con una **política de copias de seguridad** que garantice la recuperación de la información perdida en caso de incidente, sin que esto afecte a la continuidad de la empresa o a los pacientes.

La **formación de los empleados** también debe tenerse en cuenta, ya que estos conforman el eslabón más importante en la cadena de la seguridad. Contar con un plan de formación dirigido a los empleados marcará la diferencia y reducirá considerablemente el riesgo de sufrir un incidente de ciberseguridad.

Mantener todo el ***software* actualizado 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 el *software* utilizado, como son ordenadores, servidores o dispositivos móviles sin olvidarse de los dispositivos médicos, los cuales también pueden 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** 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
- Plan Director de Seguridad
- Protege a tus Clientes

Políticas de seguridad

- Concienciación y formación
- Uso del correo electrónico

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

Historias reales

- Historias reales: comprometí la seguridad de mi empresa y mis pacientes sin darme cuenta
- Historias reales: Soy tu nueva factura y te voy a secuestrar el ordenador
- Historias reales: érase una vez un ransomware que secuestró los expedientes médicos de mis pacientes
- Caso de éxito: Protección del puesto de trabajo en una clínica

Artículos del blog

- ¿Por qué cifrar la información sensible?
- Día Europeo de los Derechos de los Pacientes: protege su información personal y sensible
- 8 consejos para la privacidad de los datos del sector sanitario

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
- Formación y concienciación
- Soporte y mantenimiento

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