CONSTRUCCIÓN

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

CONSTRUCCIÓN

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
017
protege tu empresa

1. INTRODUCCIÓN

Reformas de viviendas, construcción de edificios, carpintería, aislamiento, fontanería u obra civil son algunos ejemplos de actividades del sector de la construcción. Un sector constituido en gran medida por pymes y micropymes con plantillas y lugares de trabajo que varían con frecuencia según el tamaño y ubicación de los proyectos que van surgiendo.

Cabe destacar que se encuentra inmerso en la transformación digital, sobre todo en la gestión de los procesos que son de por sí complejos debido a la **subcontratación** y la **movilidad**. Además, la llegada del **IoT** (Internet de las Cosas) será muy útil gestionar la ubicación de materiales y personas. Sin embargo, las empresas de construcción pueden ser, por estas características, objetivos fáciles para los ciberdelincuentes, y ante un ciberataque las consecuencias pueden ser muy negativas para el negocio.

Para evitar situaciones que puedan afectar en particular a la **movilidad** y a la **continuidad** de tu empresa, te mostraremos los pasos que debes seguir 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

Deterioro o pérdida de información confidencial de la obra, ataques de *ransomware*, *phishing*, fuga de datos, *software* con vulnerabilidades, interrupción de la actividad, espionaje de proyectos o seguridad física en el trabajo son algunas de las amenazas que pueden afectar a cualquier empresa de construcción. Estar al corriente de ellas 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 algún Aviso de seguridad.

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

- **Suplantan la identidad de Correos mediante mensajes SMS**
- **Vulnerabilidad en la aplicación ES File Explorer de Android**
- **Campaña de correos electrónicos fraudulentos suplanta a la Agencia Tributaria**
- **Si te llega un reembolso de Endesa, guarda precaución, es un phishing**
- **Nueva oleada de ransomware afectando a múltiples equipos**
- **WhatsApp avisa sobre un fallo de seguridad en varios sistemas operativos**

Además de detectar las amenazas mencionadas anteriormente, se deben mantener todos los sistemas **actualizados**, tanto los utilizados en los dispositivos de los trabajadores como los empleados para dar cualquier servicio desde Internet, como la página web de la compañía. Algunos ejemplos de este tipo de avisos son:

- Vulnerabilidades en Microsoft Internet Explorer y Microsoft Defender ¡Actualiza!
- Vulnerabilidad en el escritorio remoto de Windows de versiones antiguas
- La tecnología Bluetooth usada para infectar dispositivos
- Actualización de seguridad en Adobe Acrobat y Adobe Reader
- ZombieLoad: problemas de seguridad en procesadores de INTEL
- Nueva versión de Joomla!, actualiza tu gestor de contenidos
- Actualización de Oracle Java SE
- Vulnerabilidad en los procesadores Qualcomm que afecta a dispositivos Android

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, construcción

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 de la construcción, 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:

Infección por *ransomware*

Fuga de información

Ataque por ingeniería social

5. APRENDE A PROTEGERTE

La **subcontratación de servicios de ciberseguridad** es una práctica habitual en las empresas de construcción. Una de sus principales ventajas que tiene la contratación es la inmediatez de resultados, pero tenemos que tener en cuenta que la subcontratación en muchos casos involucra el acceso por parte de una tercera entidad a nuestra información, por lo que debe protegerse mediante **contratos, acuerdos de confidencialidad y a nivel de servicio (SLA)**.

La construcción aprovecha la **hiperconectividad** que permite la tecnología utilizando aplicaciones específicas para **dispositivos móviles** (partes de obra o geoposicionamiento de materiales y equipos), el **almacenamiento en la nube** y las **conexiones remotas** para el envío y recepción de documentación. Otra tecnología que está teniendo impacto en la construcción son las aplicaciones del **Internet de las Cosas (IoT)** en la gestión de partes de obra o de inventarios y en la prevención de riesgos laborales, entre otros

Como empresas y profesionales de este sector tenéis que redoblar vuestros esfuerzos en mantener su ciberseguridad, incluyendo aspectos como la **seguridad de los recintos de vuestras oficinas, de los dispositivos móviles** y de las **conexiones remotas**.

Los posibles incidentes de seguridad y los desastres pueden dañar vuestra capacidad operativa, repercutiendo de manera negativa tanto económicamente como en vuestra imagen y reputación, haciendo peligrar la **continuidad de vuestro negocio**. Para mitigar los efectos negativos de los incidentes, las empresas deben contar con un **Plan de Contingencia y Continuidad de Negocio** que

regule los mecanismos a poner en marcha en estos casos.

La accesibilidad a la información también es crucial para la mantener la actividad diaria de las obras. 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 **convirtiendo la información en inaccesible** al cifrar todos los archivos de valor para la organización.

Ante esta situación, el único método que garantiza poder recuperar la actividad laboral sin demasiados impedimentos es **haber realizado con anterioridad copias de seguridad regulares**.

Mantener los componentes ***software* actualizados con la última versión disponible** debe ser otra de las cuestiones ineludibles en cualquier organización. Hay que contar con una **política de actualizaciones** que tenga en cuenta **todo tipo de equipos**, incluidos equipos de red, dispositivos portátiles, tabletas y móviles, impresoras y dispositivos IoT, ya que todos ellos están expuestos a ser atacados por ciberdelincuentes.

La **formación de los empleados** también es importante, en especial si la plantilla varía con frecuencia. Puesto que estos conforman el eslabón más importante en la cadena de seguridad, hay que fortalecerlo. Contar con un plan de formación dirigido a los trabajadores, que incluya a los nuevos, marcará la diferencia y reducirá considerablemente el riesgo de sufrir un incidente de ciberseguridad como, por ejemplo, una **fuga de información**.

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 del puesto de trabajo
- Contratación de servicios
- Protección en movilidad y conexiones inalámbricas

Políticas de seguridad

- Concienciación y formación
- Relación con proveedores
- Almacenamiento en la nube

Guías

- *Cloud computing*: una guía de aproximación para el empresario
- Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario
- Almacenamiento seguro de la información. Una guía de aproximación para el empresario

Historias reales

- Historias reales: trabaja seguro desde tu móvil o tu tableta
- Historias reales: la importancia de los acuerdos de nivel de servicio
- Historias reales: suplantaron a mi proveedor y a mi empresa estafaron

Artículos del blog

- Protección de la información en la construcción: ¡manos a la obra!
- Incorporación segura de dispositivos móviles a la empresa
- Sube a la nube, pero no estés en "las nubes" sin continuidad del negocio

Reporte de fraude y ayuda al empresario

- Reporte de fraude
- Línea de Ayuda en Ciberseguridad

Catálogo de empresas y soluciones de ciberseguridad

- Control de acceso y autenticación
- Seguridad en dispositivos móviles
- Seguridad en la nube

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