Ciberseguridad en la digitalización de tu empresa de construcción

nalanda

Índice

Introducción:

la digitalización del sector de la construcción

Aunque el sector de la construcción y afines son esencialmente manuales, la tecnología también ha irrumpido en este ámbito. El móvil es una **herramienta de comunicación básica para cualquier obrero, tampoco es extraño ver a encargados que gestionan la obra a través de dispositivos móviles, tablets o portátiles**, y según el volumen del proyecto, encontramos tornos de entrada y salida o distintos tipos de maquinaría que ya está conectada a la nube.

Es decir, **la digitalización también ha llegado para quedarse y -en definitiva- mejorar-la actividad en el sector de la construcción** porque las empresas se han dado cuenta de los beneficios de gestionar proyectos, automatizar tareas, coordinar suministros o personal a través de herramientas tecnológicas.

No obstante, todo tiene su "cara b". El uso masivo de la tecnología entre pymes que forman parte de una cadena de suministro pueden ser objeto fácil para los ciberataques. El mal uso de la tecnología, el desconocimiento, las debilidades de los diferentes tipos de software que se utilizan... pueden resultar un caldo de cultivo para los ciberdelincuentes. Por eso, tomar medidas relacionadas con la ciberseguridad que protejan a nuestra empresa, empleados y clientes es fundamental.

¿Conoces tus riesgos?

Empresas, gobiernos... en los últimos meses se han repetido las noticias del impacto de ciberataques a entidades relevantes. **Pero nadie estamos exentos de sufrir estos delitos.**

De hecho, las pequeñas y medianas empresas son las que más sufren los ataques informáticos. Así lo atestigua un estudio realizado en 2021 por SSH Team Consulting, que recoge que **“el 71% de las pymes en España sufrieron algún ataque durante la pandemia”.**

La concienciación en ciberseguridad cada vez mayor fruto del aprendizaje y la investigación de medidas de prevención. Pero, la lucha contra los ciberataques es permanente porque **la tecnología no deja de actualizarse y la ciberdelincuencia, también.**

De esta manera, es necesario estar revisando nuestros riesgos de manera continua. Además, cada industria tiene sus propias características y riesgos en materia de ciberseguridad, y los ataques pueden producirse durante meses sin que nos demos cuenta, por lo que puede hacer más difícil solucionar un ataque. Llegados a este punto, nos hacemos la siguiente pregunta: **¿Conoces bien qué y quiénes usáis tecnología y los riesgos de cada producto tecnológico? El primer paso es conocer nuestro sistema y qué brecha de seguridad digital tenemos.**

Pincipales amenazas

Cada empresa tiene su propio ecosistema digital. Pero, de manera genérica, estas son las principales amenazas o situaciones favorables a ciberataques que pueden afectar a la actividad de tu negocio:

Phishing: Nosotros o nuestros empleados recibimos un email, una llamada telefónica o un mensaje SMS que, en realidad, es un timo. A través de este método, intentarán robarnos los datos personales, o nuestra web puede ser atacada para suplantar a otra y enviar correos de *phishing* con los que robar datos personales de clientes de la entidad suplantada.

Ransomware: Un programa restringe el acceso a nuestro sistema operativo o a algunos archivos, por lo que nuestros datos quedan secuestrados a cambio de un rescate.

Vulnerabilidades de software: Las debilidades en un programa informático pueden estar en errores en el código o en su configuración. Los ciberdelincuentes tratan de identificar esas vulnerabilidades para provocar un secuestro, robo de datos...

Espionaje informático: Sistema por el que nos pueden espiar y, por tanto, robar datos de nuestra empresa, empleados, proveedores o clientes.

Recuerda en este punto que la buena gobernanza no implica únicamente la gestión de la ciberseguridad en nuestros propios sistemas de información si no también, cómo gestionamos los datos de terceros. Hay casos en los que los hackers llevan a cabo ciberataques a proveedores de grandes empresas no como objetivo final, si no como un medio para acceder a sus clientes.

Consejos para proteger tu actividad digital

¿Cómo puedo proteger los datos de mi empresa, empleados, clientes y proveedores?

Recogemos un listado con los principales consejos para prevenir riesgos de ciberataques y contar con una relación segura con la tecnología.

Plan de Contingencia y Continuidad de Negocio

Contar con un Plan de Contingencia y Continuidad de Negocio ante posibles ciberataques. Es un instrumento que nos ayudará a regular los mecanismos que debemos activar en caso de que un incidente grave ponga en peligro nuestra actividad. Estas medidas favorecerán el mantenimiento de unos servicios mínimos y un periodo de recuperación, analizarán resultados y los motivos del incidente.

Contraseñas seguras

Utilizar contraseñas seguras para el acceso a los sistemas. Es importante que las contraseñas se almacenen en sistemas cifrados. Asimismo, contar con una política que obligue a actualizarlas de forma periódica y no utilizar la misma contraseña para distintos servicios. Es muy recomendable implantar un segundo factor de autenticación como una prueba adicional al empleo de usuario y contraseña.

Copias de seguridad

Realizar copias de seguridad de manera constante. Ante la posibilidad de que nuestro sistema o datos queden paralizados, las herramientas de copias de seguridad nos pueden ayudar a recuperarnos del incidente, como se recoge en el Reglamento General de Protección de Datos. De esta manera, la empresa ha de contar con una política de realización de copiar de seguridad donde establezca qué protocolo seguir para llevarlas a cabo.

Sistemas de antivirus

Contar con sistemas de antivirus activos y actualizados en todo momento. Las actualizaciones ayudan a proteger mejor nuestros equipos y la información que hay en ellos ya que los fabricantes van perfilando su software en función de los problemas que van detectando en su uso. Es esencial determinar un calendario de actualizaciones para poder llevarlas a cabo de manera periódica y quede registrada toda la actividad al respecto.

Consejos para proteger tu actividad digital

Exposición en Internet

Vigilar la exposición de nuestros servicios y datos en internet porque en el día a día se dan numerosas situaciones en las que tenemos que permitir el acceso libre desde internet a una base de datos o accesos al escritorio en remoto de un servidor. Esto se puede traducir en agujeros de seguridad que quedan abiertos y por los que nuestra información se puede ver amenazada. Aquí también es necesario establecer una norma sobre los servicios expuestos en internet, a la par que los accesos remotos han de realizarse siempre a través de VPN, proxy o medidas igual de seguras.

Dispositivos cifrados

Tener dispositivos cifrados para blindar la confidencialidad de la información. Es decir, solo las personas autorizadas pueden acceder al dispositivo y a los datos. Protegemos así nuestros equipos en caso de extravío. Se puede aplicar este cifrado en portátiles, pero también en móviles, tabletas, discos duros, memorias USB... en definitiva todos aquellos aparatos electrónicos conectados a Internet donde están reflejados nuestros datos y que pueden quedar al aire en caso de robo o extravío.

Es vital la protección de los datos de la empresa, empleados, clientes y proveedores

Y, por supuesto,

Formación de empleados

es vital la formación de todos los empleados de la empresa en buenas prácticas de ciberseguridad. A través de formación continua, los trabajadores han de aprender a reconocer ataques y evitarlos, proteger adecuadamente el puesto de trabajo con antivirus actualizados, tratamiento y manejo de dispositivos (portátiles, móviles, tabletas...), entender los riesgos que conlleva el uso de páginas web externas, aplicaciones de terceros, descargas o actualizaciones que no están validadas por los departamentos de informática o seguridad.

¿Tienes en cuenta la ciberseguridad en tu proceso de digitalización?

¡No todo vale!

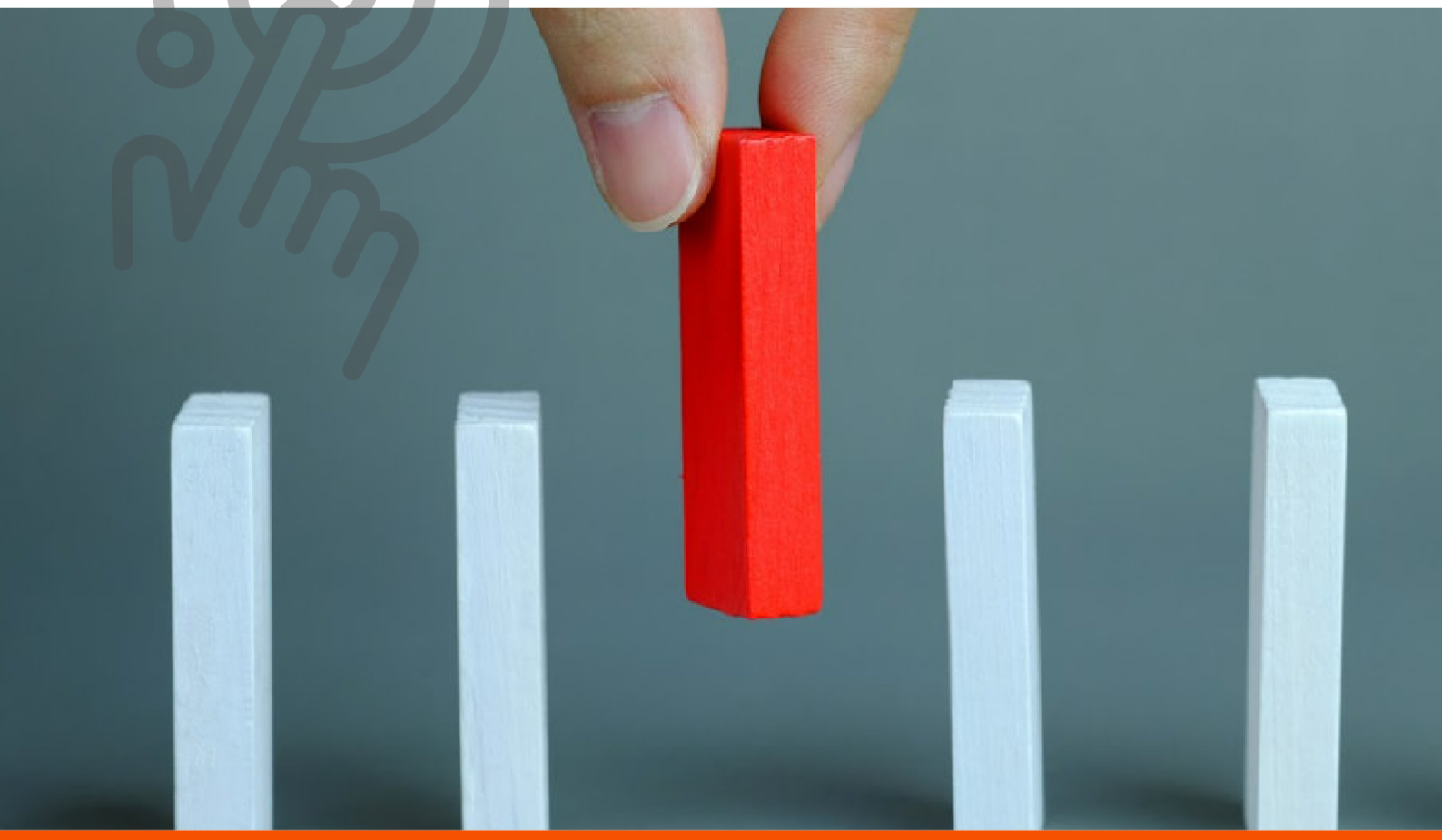
Si tu empresa está experimentando un cambio hacia lo digital, con la instalación de programas informáticos que ayuden a gestionar procesos, personas o bienes, maquinaria digitalizada, presencia en internet... es preciso revisar las estrategias de ciberseguridad que están siguiendo para evitar riesgos.

En este sentido, **lo importante es asegurarnos de que nuestros proveedores de herramientas digitales velan por la seguridad de todos nuestros datos.**

Para cuidar este aspecto has de fijarte en las garantías que nos ofrecen los proveedores digitales con los que trabajamos.

En el caso de Nalanda, como gestores de datos de más de 500 clientes y 57.000 proveedores, somos conscientes de la necesidad de proteger su información de manera rigurosa.

Importante : garantías de nuestros proveedores digitales



¿Cómo gestionamos la ciberseguridad en Nalanda?

Profesionales preparados y en constante formación

En nuestro caso, contamos con un perfil de CISO (Dirección de Seguridad) y DPO (Oficial de Protección de Datos) en permanente actualización para estar al día de normativas, medidas, ataques, experiencias y novedades del sector. Además, los empleados de cada departamento están formados en áreas específicas que tienen que ver con la seguridad y protección de datos.

Medidas para la protección de la información

Procesos para securizar los equipos de oficina, bases de datos...pero también herramientas desarrolladas para los clientes, como la información por roles o el doble factor de autenticación.

Auditorías periódicas

Análisis internos y externos para conseguir certificaciones de cumplimiento de las medidas de seguridad.

El desarrollo de soluciones digitales como la plataforma CAE, el servicio de homologación de proveedores, herramienta de facturación electrónica o la APP de Acabados y Repasos hacen que la ciberseguridad siempre haya estado en el centro del negocio para Nalanda.

Es parte esencial de nuestra actividad.

Sin embargo, la colaboración de los propios clientes y proveedores es imprescindible si queremos blindarnos ante los temidos riesgos y evidentes impactos de los ciberataques.

Para Nalanda la ciberseguridad siempre ha estado y estará en el centro del negocio.

¿Hablamos?

nalanda

nalandaglobal.com