

La ciberseguridad en el teletrabajo. Buenas prácticas Talio para proteger un negocio

Debido a la situación de pandemia actual, muchos hábitos han cambiado. La nueva normalidad trae consigo cambios que se quedarán una larga temporada, entre ellos, el teletrabajo

En el teletrabajo la tecnología juega un papel fundamental, los ordenadores, las comunicaciones y otros dispositivos tecnológicos se han convertido en herramientas indispensables para trabajar, es por ello que han de cuidarse y protegerse para evitar incidentes y que cumplan con su función de la manera esperada.

¿Qué es la ciberseguridad?

La digitalización, las autopistas de la información y ahora la industria 4.0, permiten acceder a más información, tener más datos para la toma de decisiones y mejorar los procesos.

La información es generada, procesada, guardada y transmitida. La información digital aparece en todas las facetas de la vida y el mundo industrial y empresarial no es ajeno.

Esta información es un valor que hay que salvaguardar y la forma de hacerlo es manteniendo los sistemas informáticos protegidos, son necesarias medidas de seguridad que ayuden a evitar estar expuestos a situaciones de peligro.

La ciberseguridad es una práctica que se utiliza para proteger tanto a ordenadores como servidores, dispositivos móviles, redes y otros sistemas electrónicos de ataques maliciosos.

¿Se está realmente preparado para un ciberataque?

Tal y como muestra el CCN-CERT en su Informe Ciberamenazas y Tendencias Edición 2020, la covid-19 ha influido en el ámbito de la ciberseguridad global, muchos actores adversos aprovechan los momentos de crisis para actuar de forma indebida, y en muchas ocasiones, dañar los PCs.

Para evitar o mitigar esta situación es imprescindible contar con medidas de ciberseguridad para proteger la información y los elementos que la manejan, la computadora, los servidores, las comunicaciones, etc... En TALIO cuentan con los elementos técnicos y humanos para proteger la actividad.

“La pandemia de COVID-19 seguirá marcando muchas de las amenazas y riesgos en los próximos meses, muchos de estos directamente relacionados con el aumento del teletrabajo”, CCN-CERT, 2020

Vigilancia y respuesta

En talio ayudan a la continuidad del negocio desde el propio diseño. Diseñan las infraestructuras onpremise, virtualizadas, Cloud o la combinación de ellas de forma que se reduzca el impacto ante un incidente.

Diseñan sistemas de copia y restauración y mantienen monitorizados los sistemas y herramientas defensivas para que se encuentren siempre dentro de los parámetros deseados. Realizan mantenimientos preventivos y correctivos que mantengan la seguridad

Son Partner Gold y Empresa certificada por el CCN-CERT para implementar sistemas de vigilancia de deficiencias en la capa de acceso a la red, Respuesta y compliance. Tanto en el mundo IT como en OT y IoT

CSIRT

Los CSIRT (Computer Security Incident Response Team), son equipos de respuesta a diferentes incidentes de seguridad, restituyen las actividades con un impacto mínimo para las organizaciones o empresas.

En Talio hacen uso del servicio CSIRT para que, en caso de que una amenaza o ciberataque logre hacer efecto, anularlo y restablecer el equipo en el menor tiempo posible y con el impacto mínimo para las organizaciones.

Funciones

- Controla y minimiza los daños a la organización y su información.
- Coordina las actividades para una recuperación rápida y eficiente.
- Prevé eventos similares que puedan ocurrir en el futuro.
- Mantiene una base de conocimientos que permite registrar las lecciones aprendidas de estos sucesos.

Formación y concienciación

El usuario es el eslabón más débil en la cadena

La Ciberseguridad, como la seguridad, empieza por uno mismo. En Talio utilizans las mejores herramientas para la monitorización y detección de amenazas, asimismo disponen de un servicio para la gestión de la ciberseguridad a varios niveles. Además, cuenta con una línea de formación y concienciación en ciberseguridad. Estas medidas formativas pueden ser presenciales, Online o una combinación de ambas de manera que se personalice a las necesidades de la empresa y/o del puesto. También participan con distintos organismos en la divulgación de la ciberseguridad.

La concienciación permite conocer los riesgos y entender las precauciones que se deben adoptar, pero también ayudan a comprender las medidas preventivas que toma la organización minimizando el rechazo y acompañando en el cambio.

En conclusión, los equipos informáticos cada vez corren más peligro. Se debe proteger tanto a éstos como la información que portan. Gracias al CSIRT se evita la materialización de amenazas, o en caso de que esto suceda, se aplica un plan en el que se minimizan las consecuencias.

Si interesa el tema de la ciberseguridad o se tiene cualquier consulta, Contactar con Talio en www.talio.it

Datos de contacto:

Eva Garcia
94 651 99 90

Nota de prensa publicada en: [Bilbao](#)

Categorías: [Programación](#) [Hardware](#) [Software](#) [Ciberseguridad](#) [Recursos humanos](#) [Otras Industrias](#)

NotasdePrensa

<https://www.notasdeprensa.es>