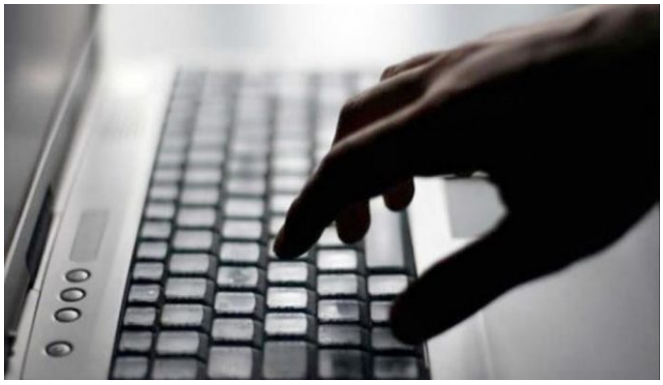

Auditoría de infraestructuras críticas, la clave de la seguridad de tu negocio

Cada empresa necesita su propio protocolo de ciberseguridad y el que una estrategia de defensa funcione en un negocio, no garantiza éxito en otro.

El tamaño, giro e incluso la ubicación geográfica de un negocio, son factores que hacen que haga falta realizar una auditoría de infraestructuras críticas que ayuden a crear sistemas efectivos de seguridad contra cibercriminales para cada empresa.

Ignorar esta realidad solo provocará la pérdida de millones de dólares en ingresos y la paralización de los procesos de productividad que hacen funcionar un negocio.

Es un hecho que saltar al mundo digital trae consigo riesgos. No hay porqué aderezar la verdad: con

cada nueva tecnología, surge una nueva amenaza que podría poner en riesgo la existencia de tu negocio, pero para resolver esto se pueden realizar auditorías de seguridad especializadas.

Con una auditoría de este tipo, podrás conocer las áreas de oportunidad para mejorar la seguridad y también las brechas en tus sistemas que podrían convertirse en puertas de entrada de un nuevo y letal malware que ponga de rodillas tus operaciones.

La seguridad de una empresa dependerá de la eficacia con la que se lleve a cabo cada gestión, pero si tu negocio es grande, complejo o vive en un ecosistema más susceptible a ser atacado, será aún más necesario realizar una auditoría de infraestructuras críticas.

La información corporativa con la que trabajas todos los días es un botín demasiado jugoso como para que los cibercriminales lo

ignoren, así que mantener una actitud siempre alerta ayudará a mantenerse seguro.
De acuerdo a datos de la consultora IDC Windows, el Directorio Activo de Microsoft sigue siendo el sistema operativo para servidores en redes corporativas más utilizado del mundo, pero también es el ecosistema más atacado por los cibercriminales.

Una sola falla en este directorio, paralizará tus operaciones pues gran parte de los servicios realizados en línea o de forma digital dependen de este.

Casi cada aspecto de tu negocio funciona a través del Directorio Activo de Microsoft, así que debes prestar mucha atención a este cuando creas un cerco de seguridad efectivo.

¿Y cómo se crea un cerco a la altura de los peligros actuales de ciberseguridad? Con una auditoría de infraestructuras críticas que permita conocer dónde están los huecos por los que se podría colar un malware o ransomware.

Nosotros recomendamos actualizar contraseñas de cada usuario del directorio con regularidad, realizar una gestión de roles de usuario y privilegios, y regular adecuadamente el nivel de accesibilidad a la información para cada usuario.

Estas medidas ayudan a mantener seguros nuestros sistemas más esenciales, pero muchas veces no llegan a ser suficientes para protegerlos de los cibercriminales más persistentes.

Confiar únicamente en nuestras contraseñas para evitar que las amenazas infecten nuestros sistemas es como usar un candado barato para mantener el oro de una bóveda lejos de las manos de los ladrones pues una contraseña depende completamente del factor humano, mismo que suele ser susceptible a fallas.

Por ello recomendamos contratar un servicio permanente de vigilancia que se haga a través de un proveedor externo que siempre contará con tecnología de punta y con las herramientas más novedosas para contrarrestar cualquier intento de intrusión de los cibercriminales.

Este proveedor puede hacer una estrategia de prevención y reacción ante ataques, pero también realizar rastreos de las redes del Directorio Activo para descartar que este, el repositorio de nuestros procesos e información más importante, sea vulnerado.

Una auditoría de infraestructuras críticas sirve justo para eso, pero no puede hacerse sola, así que recomendamos acercarte a un experto en ciberseguridad que te oriente y te ayude a mantener bajo candado esos procesos e información que te dan ventaja sobre tu competencia y te permiten crecer cada trimestre.