



Managed secure IT | no matter what

The background image shows a perspective view of server racks in a data center. In the foreground, a hand is holding a tablet that displays a blue-tinted image of a hand holding a globe. A semi-transparent blue box with white text is overlaid on the tablet image.

SEIS PASOS PARA BLINDAR TUS REDES DE LAS AMENAZAS DE INTERNET

¿Qué hacer para proteger un negocio de las amenazas que abundan en internet? ¿Cómo empezar?

Con esta breve explicación dividida en seis pasos, buscaremos explicar cómo blindar las redes de cualquier negocio de los hackers, los piratas y los cibercriminales.

PROTEGE CADA EQUIPO

Cada computadora, terminal y dispositivo móvil es una apertura para un criminal cibernético, pero es posible complicarle la vida a una posible amenaza cerrando su primera opción de entrada a tu red.

Actualiza el sistema operativo que utilices. Este tipo de correcciones suelen tapar con “parches digitales” los posibles agujeros de seguridad que tal vez no se habían descubierto cuando este fue instalado en las computadoras de tu negocio.

Los plugins de seguridad de cada navegador son importantísimos. También debes pedirle a tu CIO que los actualice todos, en especial los relacionados a las web apps de finanzas y contaduría.

Pide que se cambie constantemente la contraseña de la red inalámbrica y se hagan chequeos regulares de la estructura a la que están conectadas todas las computadoras y dispositivos dentro de la empresa.

Recuerda prestar especial atención a los equipos donde haya software de finanzas o se lleven registros de los ingresos y egresos.



MANTÉN UNA RED DOMÉSTICA BAJO CONTROL

Ciérrale la puerta de tus redes e intranet a los hackers. Pide a tu CIO que encripte las teclas que los empleados presionan en su día a día para que un cibercriminal no conozca contraseñas o analice la regularidad en la que las finanzas son revisadas.

Crea contraseñas individuales para cada aplicación que use el equipo de finanzas y el resto de la oficina.

Busca el asesoramiento de un experto en herramientas basadas en la Nube para ver qué aplicaciones y servicios pueden migrarse a este ecosistema con el fin de mantenerlas en un ambiente blindado y en constante evolución.



MIGRA TUS EQUIPOS A UNA ESTRUCTURA DE CLOUD

Actualmente es difícil no encontrar herramientas financieras, de productividad o gestión de información que no se alojen en la Nube. Estas, además de ofrecer mucha más movilidad al personal de una empresa, habitan un espacio seguro y en constante actualización que las vuelve casi invulnerables a los hackers.

Siempre será más seguro manejar y almacenar información desde la Nube que en un servidor In-House que tenga que ser vigilado constantemente por personal especializado en evitar brechas de seguridad.



CONCIENCIA A TU PERSONAL

Cada elemento de una empresa, especialmente el de finanzas, debe entender que la seguridad en la empresa comienza desde que se enciende la computadora y se abren los primeros programas para trabajar.

Esto, unido a un uso inteligente de dispositivos móviles y una restricción razonable del uso de navegadores web y las redes sociales, evitarán que un cibercriminal pueda aprovechar cualquier brecha de seguridad accidentalmente abierta para provocar estragos en la red de una empresa.



Evita malas prácticas

Divulgar información sensible en redes sociales, tomar a la ligera la importancia de las contraseñas de seguridad, usar dispositivos móviles para gestionar información importante para una empresa y conectarse a cualquier red inalámbrica para trabajar, son todas malas prácticas que deben evitarse a toda costa.

Pídele a tu CIO que informe a todo el staff de las acciones que debe evitar para que la compañía no se vuelva una víctima más del cibercrimen, o en caso de no haber CIO, busca la ayuda de un experto en seguridad que asesore a todo tu equipo de trabajo en cuanto a las buenas prácticas dentro y fuera de la oficina.

Busca un experto que te asesore sobre nuevas formas de protegerte

Resulta relativamente sencillo hacer recomendaciones como “usar las mejores herramientas para proteger las finanzas y redes de un negocio”, pero ¿por dónde se empieza?

Lo mejor es consultar a un experto en temas de ciberseguridad, protocolos de protección y tecnologías innovadoras como el Cloud Computing o el IoT, con el fin de saber qué herramientas son las mejores para cada situación y de qué manera se pueden proteger los datos de un negocio sin invertir demasiados recursos.

No dudes en acercarte junto a tu CIO y CEO a una empresa certificada y con experiencia en el ramo de la protección digital de empresas, para recibir asesoramiento útil y preciso que en el futuro se convertirá en el asset más valioso de cualquier compañía.



Síguenos en nuestras redes sociales:



MexisMX



Servicios
Administrados
Mexis, S.A. de C.V.



Mexis TI



Servicios
Administrados
Mexis, S.A. de C.V.