
mexus®
Managed secure IT | no matter what
Cómo tus colaboradores pueden ayudar a **proteger tu negocio**
M·Security

Managed secure IT | no matter what

Cómo tus colaboradores pueden ayudar a **proteger tu negocio**

Cometer un error que pondría en riesgo todo tu negocio es muy fácil y puede suceder en cualquier momento, pero ¿Cómo mantener a tu equipo lejos de hacerlo cuando maneja información tan sensible todos los días?

Responder esta pregunta puede parecer un reto importante para garantizar la seguridad digital de un negocio, pero con esta lista de siete No's que tu equipo debe aprender, será un poco más fácil.

1. No abras ningún enlace inesperado
Este consejo es de los más básicos, pero sorpresivamente existe un porcentaje cada vez mayor de ingenieros y usuarios comunes que no lo piensan dos veces antes de abrir un hipervínculo que recibieron de parte de un usuario desconocido.

Recomendamos no abrir ningún enlace inesperado, pues este es uno de los métodos más comunes para propagar ransomware.

De hecho, el último ataque de este tipo (#WannaCry) se propagó de esta manera antes de

paralizar a miles de organizaciones en Europa, Asia y América; el cual hace perder millones de dólares a las empresas que afectó.

2. No dejes de actualizar el firewall o antivirus

Tu primera línea de defensa ante los ataques de cibercriminales es tu firewall y antivirus, pero si no los mantienes actualizados, de poco te servirán una vez que tus redes o bases de datos se enfrenten a un nuevo tipo de código malicioso.

Nunca dudes en actualizar tus herramientas de protección, pues los técnicos responsables de sus algoritmos de seguridad siempre están buscando la manera de mejorar sus filtros para evitar que cualquier malware se infiltre en tus redes y afecte la forma en la que opera tu negocio.

3. No pares de realizar respaldos periódicos

Si fuiste atacado por ransomware o un código malicioso que ha borrado la información con la que trabaja todo el equipo, lo mejor que puedes hacer para minimizar el impacto de cualquier ataque de este tipo es realizar respaldos periódicos que mantengan tu información lejos de los daños que un hacker pueda provocar. Recuerda siempre realizar estos respaldos con ayuda de un experto para asegurar que ningún dato se pierda en el proceso.

También es importante que mantengas ese backup desconectado de la red de internet y colocado en un medio de almacenamiento independiente al que usa el personal de la compañía para trabajar.

4. No ignores las nuevas tecnologías en nube

Almacenar información importante en tecnologías on premise puede parecer seguro, pero las plataformas basadas en la nube se han convertido en una opción cada vez más atractiva para los técnicos preocupados por la seguridad cibernética.

Hoy en día, los servicios Cloud no solo ofrecen soluciones personalizadas para cada empresa, sino también una opción más económicamente viable a mediano y largo plazo, y una plataforma siempre en evolución, escalable y altamente segura.

Acude a un experto en tecnologías en nube para que te oriente sobre los servicios que mejor le convienen a tu negocio.

5. No abuses de las redes sociales

Es común ver que los empleados de una empresa pasan demasiado tiempo visitando sus redes sociales y compartiendo datos de su vida privada desde las computadoras (y redes) de la empresa, pero un jefe de TI siempre sabrá poner un alto a este tipo de actividades, pues con cada like o share compartido en Facebook, se abre una puerta de la empresa a los hackers que quieran vulnerarla.

Hace unos meses, una empresa importante de seguros fue afectada por un cibercriminal que había creado una página falsa de Facebook en la que varios de sus empleados metieron datos sensibles al pensar que era la real.

Al hacerlo, le concedieron de manera involuntaria los accesos a algunos de los sistemas clave de la empresa y la rindieron a los pies de los hackers que robaron todo lo que pudieron de ella y cometieron cuantos fraudes bancarios como les fue posible hasta que un experto en seguridad digital los detuvo.

Limita el acceso a las redes sociales y concientiza a tus empleados para que las visiten solo desde sus dispositivos móviles personales y cuando estén lejos de la red del trabajo.

6. No subestimes a los cibercriminales
Hace algunos meses, unos hackers se metieron a la red de una importante empresa a través del celular de uno de sus ejecutivos de más alto nivel cuando este abrió un enlace inesperado que había recibido en su bandeja de correo electrónico.

Así como en el ejemplo anterior, miles de ataques cibernéticos han cumplido su objetivo por las cada vez más creativas maneras de vulnerar las redes de una empresa o usuario particular.

Creer que un antivirus o firewall es suficiente para contener a un cibercriminal es un error que se paga con la afectación parcial o total de las actividades de una empresa.

Si necesitas más información sobre las amenazas que abundan en la era digital, acércate a alguien que te pueda informar más sobre cómo defenderte de ellas y prevenir convertirse en su próxima víctima.

7. No ignores las recomendaciones de los expertos
Cuando un experto en seguridad te recomienda hacer algo para mantener intactas las operaciones de tu negocio, no debes subestimarlo, pues nunca habrá nadie más interesado en la seguridad digital que él.

Acudir a una autoridad en esta industria no es una cuestión temporal que se presenta solo cuando ya fuimos víctimas de un cibercriminal, sino que se trata de un compromiso a largo plazo que debemos cumplir siempre para continuar evolucionando nuestra empresa en la red sin sufrir ninguno de los males que la habitan.

Sigue los consejos de un equipo comprometido con la seguridad en internet son una inversión que se pasa sola.