24/05/2025

Ciberseguridad en el teletrabajo: 10 claves para proteger los entornos remotos



El teletrabajo ofrece flexibilidad y ahorro, pero también plantea nuevos retos para proteger la información empresarial. Acceder a sistemas desde múltiples ubicaciones y dispositivos eleva el riesgo de ciberataques. Por eso, la ciberseguridad en el teletrabajo debe ser una prioridad estratégica. Las organizaciones que no actúen a tiempo exponen sus datos, reputación y confianza de clientes. Reforzar la seguridad requiere actualizar políticas, formar a los equipos e implementar herramientas fiables. La clave está en ver la ciberseguridad no como una barrera, sino como un habilitador que permite trabajar en remoto de forma segura y eficiente.

Las mejores prácticas de ciberseguridad en el teletrabajo

La instauración del teletrabajo en numerosas empresas españolas ha coincidido con un notable repunte de los ciberataques. Según datos del Instituto Nacional de Ciberseguridad (INCIBE), durante el año pasado se registraron la friolera de 97.000 incidentes en toda España, casi un 16,6% que el año anterior. Entre las amenazas más comunes a las que se enfrenta un trabajador en remoto incluyen prácticas como el phishing, accesos no autorizados o malware; con un impacto considerable entre pymes y autónomos.

Este contexto sitúa a las empresas españolas en una situación nunca antes vista, donde deben priorizar la ciberseguridad como un pilar estratégico, antes relegado al departamento de IT. En este sentido, las compañías deben hacer un esfuerzo en reforzar infraestructuras críticas, mejorar la capacidad de sus equipos a la hora detectar amenazas y combatir ataques cada vez más complejos y elaborados, en parte gracias a la expansión de la inteligencia artificial.

Todas las empresas deberían tener en cuenta estas claves para asegurar un teletrabajo seguro, eficiente y que esté preparado para cualquier amenaza externa

1.- Formación continua sobre ciberseguridad: la mejor defensa empieza por las personas y su conocimiento

Pocos antivirus pueden compararse con el sentido común de una persona capacitada para detectar un intento de ciberataque. La gran mayoría de brechas de seguridad en las empresas españolas tienen su origen en un descuido evitable, como abrir un archivo sospechoso, introducir datos personales en páginas fraudulentas o utilizar contraseña débiles. Por eso, una de las herramientas más eficaces —y a menudo más olvidadas— es la formación. No basta con una charla al año: se necesitan sesiones prácticas, adaptadas a cada perfil, que incluyan simulaciones reales y actualizaciones periódicas. No son pocas las empresas que ‘simulan’ un

ciberataque para analizar la respuesta de sus empleados, y muchas veces los resultados no son los esperados.

Además, debemos tener en cuenta que no todos los trabajadores parten del mismo nivel. Un perfil técnico perteneciente al equipo de IT quizás necesita menos formación sobre ciberseguridad que el personal de administración. Lo ideal es que cada área de la empresa cuente con formaciones específicas que puedan aprovechar al máximo las medidas de ciberseguridad adaptadas a su día a día.

2.- Fuera tecnicismos: normas claras sobre dispositivos y redes

Durante el teletrabajo, las condiciones de seguridad cambian por completo. Desde los dispositivos a las redes, la interacción del trabajador con las herramientas debe sustentarse en políticas de seguridad claras sobre qué está autorizado, cómo deben producirse las conexiones y qué herramientas de seguridad son obligatorias. Estas normas deben ser accesibles a todo el equipo, comprensibles y, sobre todo, aplicables.

El objetivo debe ser crear un marco de actuación sencillo, pero sin perder su carácter de rigurosidad. Si creamos un documento extenso y lleno de tecnicismos, solo conseguiremos que el empleado no comprenda el porqué de las medidas de seguridad y, por lo tanto, las descuide. Establecer reglas para conexiones Wi-Fi, uso de correo electrónico, almacenamiento en la nube o contraseñas seguras puede marcar la diferencia entre un entorno vulnerable y uno preparado, especialmente si hablamos de ciberseguridad en el teletrabajo.

3.- VPN corporativa: acceso remoto con garantías

Una red privada virtual (VPN) permite acceder a la red de la empresa desde cualquier lugar con total seguridad, sin la problemática de depender de conexiones personales o públicas que no podemos controlar ni supervisar. En el caso de una VPN, el tráfico de datos se cifra, lo que impide que terceros intercepten información sensible. Implementar una VPN corporativa bien configurada es una medida básica para cualquier organización que permita el trabajo remoto.

Además, las VPN deben actualizarse y mantenerse de forma constante. No sirve con instalar una herramienta y olvidarse. También es importante formar a los usuarios para que no desactiven esta capa de protección por comodidad. Su uso debería ser obligatorio siempre que se acceda a recursos internos desde fuera de la red corporativa.

4.- Equipos protegidos desde el primer día

Nunca debemos entregar un ordenador a un empleado sin antes configurarlo cuidadosamente para su uso en trabajo remoto. Desde la instalación de antivirus, activar cortafuegos, cifrar discos duros o desactivar funciones innecesarias que puedan presentar una puerta de entrada.

Y, por supuesto, es recomendable que los equipos puedan gestionarse de manera centralizada por el departamento especializado de IT de la empresa. De esta forma, se pueden aplicar políticas de seguridad, controlar actualizaciones y detectar posibles amenazas sin depender de la acción individual de cada trabajador.

La ciberseguridad en el teletrabajo es un reto real, pero también una oportunidad para mejorar procesos y fortalecer la resiliencia digital de las empresas

5.- Verificación en dos pasos: una barrera eficaz para la ciberseguridad en el teletrabajo

Aunque pueda parecer incómoda, la autenticación en dos factores (2FA) se ha convertido en uno de los estándares más eficaces para prevenir accesos no autorizados. Se trata de una medida extra de seguridad que puede evitar muchos dolores de cabeza a la empresa. Una contraseña puede ser robada con relativa facilidad, pero si además se requiere un código adicional enviado al móvil o a una app, el acceso se complica notablemente para los atacantes.

Cuanto más habitual sea el uso de la verificación doble, menos resistencia generará entre los empleados, que en un principio pueden verlo como obstáculo. Herramientas como el correo corporativo, el acceso a aplicaciones críticas o las plataformas de gestión deben contar con este sistema activado por defecto.

6.- Diferentes roles, diferentes accesos: la clave para limitar las brechas de seguridad

No todos los empleados necesitan acceder a toda la información de la empresa. Limitar los permisos según roles permite reducir el impacto de un posible ataque. Si un usuario con acceso restringido cae en una trampa, las consecuencias serán mucho menores que si se trata de alguien con acceso total a datos confidenciales.

Además, segmentar los accesos también facilita las auditorías internas y el cumplimiento de normativas como el RGPD. Cuanto más claro esté quién puede ver qué, más sencillo será detectar anomalías o abusos que se produzcan desde dentro o desde fuera de la empresa.

7.- Plan de respuesta ante incidentes

Tan importante como prevenir un ataque es saber cómo actuar cuando ocurre. Muchas empresas no tienen un protocolo claro ante incidentes de seguridad, lo que genera confusión, pérdidas de tiempo y, en el peor de los casos, daños irreversibles. Tener un plan de respuesta bien definido, con responsables asignados y un protocolo establecido, es imprescindible.

Este plan debe incluir una cadena de comunicación interna, una lista de pasos a seguir según el tipo de incidente y procedimientos para notificar a terceros si fuera necesario (proveedores, clientes, autoridades).

8.- Auditorías y revisiones periódicas

La seguridad es un proceso constante que debemos practicar todos los días. Revisar de forma regular los dispositivos, las configuraciones de cada empleado, los accesos y el cumplimiento de políticas internas ayuda a detectar cualquier problema o incidencia antes de que se convierta en una crisis.

Estas auditorías de seguridad deben programarse y realizarse por profesionales. También es recomendable usar herramientas de monitorización que alerten de comportamientos anómalos, accesos sospechosos o brechas de seguridad en tiempo real.

9.- Dispositivos personales: mejor prevenir que lamentar

Debemos evitar, en la medida de lo posible, que los trabajadores de la empresa trabajen con sus dispositivos personales. Un portátil sin cifrado, un móvil sin contraseña o un software no autorizado tienen todas las papeletas para convertirse en un punto de entrada para un ciberataque. Si no se pueden evitar del todo, al menos deben estar regulados mediante políticas BYOD (Bring Your Own Device) bien definidas.

¿El mejor escenario? Trabajar siempre con herramientas y dispositivos proporcionados por la empresa, preparados específicamente para ello. Si eso no es posible, deben aplicarse controles técnicos, como cifrado de datos, gestión remota y restricción de acceso a ciertas funciones.

10.- Cultura de la seguridad: más allá de la tecnología

Quizás esta es la clave que mejor resume todo: la ciberseguridad en el teletrabajo no solo es cuestión de firewalls y antivirus: es una cuestión de actitud dentro de la empresa. Es imprescindible fomentar una cultura de seguridad que implique que todos los miembros de la organización —desde la alta dirección hasta los becarios— para que sean conscientes de su papel en la protección de la empresa.

Cuando la seguridad forma parte del ADN de la empresa, se nota. Los errores se reducen, las amenazas se detectan antes y los equipos se sienten más preparados para responder.

En definitiva, la ciberseguridad en el teletrabajo es un reto real, pero también una oportunidad para mejorar procesos y fortalecer

la resiliencia digital de las empresas. No se trata de implantar medidas por cumplir, sino de generar un entorno de trabajo donde la seguridad sea una prioridad compartida.

Revisar las prácticas actuales, aplicar estos consejos de ciberseguridad, formar a los equipos y adoptar tecnologías adecuadas es el primer paso. Pero lo más importante es mantener una actitud proactiva y abierta al cambio. Porque si algo hemos aprendido en los últimos años es que el entorno digital evoluciona rápido... y la seguridad debe evolucionar aún más rápido.

Fuente: https://www.apd.es/

LINK DE LA NOTICIA