Guía del colaborador remoto: Parte 2

Herramientas de trabajo

Trabajar de forma remota requiere de herramientas que ofrezcan portabilidad y la habilidad de conectarse de forma segura a los sistemas y servicios de sus empleados. Dichas herramientas consisten de una mezcla de productos físicos y digitales que se han vuelto populares en el ámbito del trabajo remoto. A continuación, analizamos los más conocidos y explicamos cómo protegerlos.

Dispositivos móviles

De las tantas herramientas que permiten el trabajo remoto, la más común son los dispositivos móviles. Desde laptops a tablets y smartphones, estos equipos permiten movilidad y dan la posibilidad a los usuarios de llevar adelante diversas tareas desde la comodidad de sus hogares, viajes de trabajo o cualquier otro sitio remoto.

Es inevitable que los empleados utilicen estos equipos para almacenar y acceder a información sensible del negocio, por eso es importante considerar los riesgos asociados, principalmente la pérdida y el robo.

Contraseñas

Es importante no dejar nunca el smartphone desprotegido, sin un pin o una contraseña fuerte. Actualmente, la mayoría de los teléfonos ofrecen opciones de autenticación biométrica, que hacen de esta tare algo sencillo de implementar.

Además, debería asegurarse de habilitar el **bloqueo automático**, dado que es común que las personas desatiendan sus móviles. De esta manera, podrá prevenir que alguien obtenga acceso a las funcionalidades o la información almacenada en el dispositivo.

Protección antirrobo

Ante la posibilidad de que el dispositivo se pierda o sea robado, algunas soluciones móviles, como ESET Endpoint Security para Android, incluyen capacidades antirrobo, para prevenir que la información y las cuentas abiertas en los equipos sean accedidas por terceros, además de colaborar en la locación y recuperación del mismo. La protección antirrobo le permitirá rastrear el dispositivo a través de la señal GPS para localizarlo y enviar mensajes que pueden ser leídos por quien lo haya encontrado.

Además, es posible realizar un **monitoreo del uso de las tarjetas SIM**, al aceptar solo una de una lista confiable. Si se tratara de un robo y el delincuente insertara una tarjeta SIM que no estuviera en dicha lista, la pantalla del móvil se bloquearía automática y se enviaría una alerta mediante SMS a su administrador de IT.

Por último, esta funcionalidad le permite tomar **medidas preventivas** en un dispositivo de forma remota, por ejemplo, enviando comandos SMS que pueden **bloquearlo**, **restaurarlo**, o incluso **eliminar todo lo que esté almacenado** en el equipo.

Es altamente recomendable activar las medidas de protección tanto en dispositivos móviles corporativos como personales.

Dispositivos de almacenamiento

Mucha información es transferida hacia y desde dispositivos, ya sean archivos, certificados, o sesiones de información de tus varias cuentas. Estos datos suelen estar almacenados en discos y memorias internas de muchos equipos, incluyendo disco duro de laptops, memoria de *smarthpones* y dispositivos USB.

Si un equipo se pierde, la información allí almacenada también, por eso es importante considerar las siguientes tecnologías y medidas de seguridad:

Cifrado

El cifrado es una práctica de seguridad muy útil para proteger información almacenada en un dispositivo. Consiste en modificar esos datos de acuerdo a patrones matemáticos o una o más llaves, de forma tal que solo pueda ser descifrada por quienes poseen las llaves.

Cuando ciframos información, la hacemos ilegible. Si un dispositivo cifrado cae en manos equivocadas, o un malware exfiltra archivos cifrados, todo lo que podrán ver es una cadena de caracteres sin sentido.

Más allá de lo que otros puedan pensar, utilizar herramientas de cifrado es algo práctico y sencillo para cualquier usuario. Solo se necesita conocer qué información queremos proteger y configurar la herramienta que utilizamos con una contraseña fuerte y segura.

Las herramientas de cifrado ofrecen en dos niveles básicos:

1. **Soluciones de Cifrado de disco completo**, como ESET Full Disk Encryption, que cifra el disco duro entero del dispositivo. Esta solución optimiza las capacidades antirrobo.

2. **Soluciones de Cifrado de archivos**, como ESET Endpoint Encryption que, además de cifrar discos duros, puede cifrar documentos o correos específicos. Esta solución realza la privacidad y ayuda al cumplimiento de las regulaciones de datos personales.

Backup

Si bien hemos hablado sobre cómo proteger la información cuando los dispositivos se pierden o son robados, también es importante pensar en cómo recuperar la información perdida para poder seguir adelante con nuestro trabajo.

Por este motivo, debemos realizar respaldos de cualquier archivo que pueda ser difícil de recuperar si se pierde. Esto aplica particularmente a documentos de autoría personal, reportes, investigaciones, hojas de cálculo, presentaciones y fotos.

Existe una gran variedad de tipos de backup que pueden utilizarse, por lo cual es importante que cada usuario evalúe qué solución se adapta a ellos. ESET recomienda Xopero Backup & Recuperación para los negocios.

Soluciones de seguridad en computadoras

Un empleado que adopta todas las medidas que hasta ahora han sido recomendadas en esta guía, ya ha recorrido gran parte del camino para asegurar la información de la compañía. Sin embargo, sigue habiendo diversos vectores de riesgo, incluyendo ataques de malware, phishing o enlaces maliciosos en correos y redes sociales, sitios web falsos o maliciosos, y otros peligros consecuentes de las conexiones a redes inseguras.

Esto hace que sea crucial combinar todas las precauciones mencionadas con un **sistema proactivo de detección de amenazas**, que puede obtenerse instalando una **solución de seguridad integral** en los equipos.

El motivo por el que hablamos de una solución integral, y no simplemente de un "antivirus", es que detectar código malicioso por sí solo ya no es suficiente.

Las soluciones integrales incluyen una variedad de módulos que detectan distintos tipos de amenazas, como conexiones inseguras, sitios falsos, paquetes malformados, y otras señales de potenciales riesgos.

En aquellas compañías donde se utiliza equipamiento corporativo para trabajar con información de forma remota, suele haber soluciones de seguridad provistas y administradas por la compañía para proteger esos equipos.

Sin embargo, **cuando los empleados utilizan sus propios dispositivos, es esencial implementar las mismas medidas de seguridad**. No solo necesitan contar con soluciones de seguridad instaladas en cada equipo de escritorio o móvil que empleen para manejar información del negocio, sino también **tenerlos actualizados**, para prevenir nuevas amenazas.

Con los equipos hogareños, particularmente aquellos que se comparten entre muchos miembros de la familia, el riesgo de una amenaza aumenta, debido a la complejidad de controlar por completo el uso que se hace de la computadora, los archivos que allí se descargan y los sitios a los que se accede desde ese equipo.

Contar con una solución como ESET Endpoint Security, respaldada y desarrollada por una compañía de seguridad informática confiable, con buena trayectoria en el mercado, resuelve estos inconvenientes rápidamente, proveyendo múltiples capas de protección para todos los usuarios hogareños.

En la tercera parte de esta serie, hablaremos acerca de las precauciones que debería tomar para asegurar su actividad en las redes.