Guía del colaborador remoto: Parte 1

Riesgos, amenazas y políticas empresariales

Introducción

Con los avances de las tecnologías de la información y la comunicación, los empleados tienen la posibilidad de conectarse fácilmente para trabajar de forma remota. Sin importar dónde se encuentren, y con una conexión a internet disponible, es realmente sencillo armar una estación de trabajo remoto.

Las ventajas del teletrabajo son fáciles de ver: ahorro de tiempo y dinero al no tener que transportarse, manejo dinámico de largas horas de trabajo y mejor gestión de su tiempo. Para los negocios, esto significa un incremento en la productividad y una disminución en los costos de infraestructura local.

Sin embargo, la realidad del teletrabajo trae consigo ciertos desafíos de seguridad para las organizaciones a la hora de asegurar que toda su información esté protegida de actores maliciosos y mantenga su confidencialidad. Las típicas medidas de seguridad disponibles en una red corporativa no protegen la información a la que se accede desde redes externas. Esto vuelve más complejo llevar un control de los accesos y el uso de la información del negocio, asignando una responsabilidad mayor a la fuerza de trabajo.

En la serie de artículos que aquí comienza, compartiremos algunos consejos claves para que los empleados puedan ejercitar una mayor responsabilidad al acceder a la información del negocio, especialmente trabajando desde casa. Hoy, tomaremos en consideración los **riesgos** y las **amenazas**, así como las **políticas corporativas**, para el trabajo remoto.

Riesgos y amenazas

El teletrabajo tiene sus claros beneficios, pero conlleva también ciertos riesgos que deben tenerse en cuenta. Si bien pueden ser correctamente mitigados en la red corporativa, también es posible que, dichos riesgos, queden fuera del control inmediato de los empleados una vez que se permite que los activos de información sean accedidos de forma remota.

Los mismos pueden materializarse tanto de forma intencional como accidental. Según cómo llevan a comprometer la información, estos riesgos pueden categorizarse de tres maneras:

1. Los riesgos que comprometen la confidencialidad de la información son aquellos que pueden permitirles a los atacantes acceder a información privada sin autorización. Por ejemplo:

- Conectarse a redes Wi-Fi desconocidas o inseguras puede hacer que terceros, conectados a la misma red, intercepten la información recibida o enviada desde los dispositivos allí presentes.

- Si los dispositivos son robados, la información que almacenan también lo es, y podría terminar en manos de criminales.

2. Los riesgos que comprometen la disponibilidad de la información son aquellos que pueden hacer que los atacantes destruyan información. Por ejemplo:

- Un malware presente en los equipos de los empleados puede comprometer no solo la información allí almacenada, sino también cualquier información a la que se acceda desde esos dispositivos.

- Utilizar una conexión insegura a internet abre un camino para que los atacantes modifiquen firmas o certificados digitales, y falsifiquen identidades digitales.

3. Los riesgos que comprometen la integridad de la información son aquellos que pueden hacer que los sistemas no estén disponibles o utilizables cuando son necesarios. Por ejemplo:

- La información almacenada en un dispositivo, o incluso el propio dispositivo, puede ser cifrado por un ransomware, y volverse inmediatamente inutilizable.

- El acceso remoto a la información o a servicios provistos por los servidores de la compañía puede ser interrumpido si la conexión es inestable.

Dentro de las oficinas, estos riesgos son mitigados y controlados por el equipo de IT, al aplicar una serie de medidas de seguridad apropiadas. Sin embargo, **fuera de este ecosistema protegido, es crucial que los empleados mitiguen o reduzcan estos riesgos de forma activa.**

Políticas corporativas

Antes de considerar los aspectos técnicos, las herramientas de trabajo y la óptima configuración para un trabajo remoto, es esencial comprender los elementos que hacen a un buen marco normativo.

Una compañía debe dar a sus empleados una política de teletrabajo clara que abarque temas como:

- Quién tendrá acceso a la opción del teletrabajo y bajo qué circunstancias.
- El procedimiento para la conexión remota.
- Qué computadoras y herramientas serán utilizadas para realizar tareas.
- Cómo debería manejarse la información al estar en otro sitio.
- Cuál es el procedimiento, o cómo contactarse, cuando se necesita soporte técnico.
- Las responsabilidades y obligaciones del trabajador remoto en cuanto a la seguridad de la información.

Es crucial, tanto para empleados como empleadores, que las reglas estén claras. Antes de comenzar a trabajar de forma remota, conectarse a la red corporativa desde afuera o utilizar servicios distintos para acceder a la información de la compañía, es importante que su fuerza de trabajo conozca y comprenda las políticas para el trabajo remoto y el acceso a la información.

Los empleados deben tener en claro cuáles son sus responsabilidades en torno a la seguridad, ya sea si tienen permitido utilizar sus propios dispositivos y – de ser así – qué precauciones deben tomar, para qué tienen permitido usar los servicios de comunicación de la compañía, y, ante todo, qué medidas de seguridad han sido establecidas y qué herramientas están disponibles para poder cumplir con todos estos requisitos.

Ya sea que estemos tratando directamente del personal o de trabajadores independientes, en todos los casos es vital que éstos comprendan sus políticas de trabajo y acceso remoto, para asegurarse que siempre estén siguiendo los **lineamientos de seguridad de su negocio**.

En la segunda parte de esta serie, hablaremos sobre cómo asegurar las herramientas de trabajo remoto que utilizan sus empleados.