01/05/2020

La seguridad empresarial y el teletrabajo en tiempos de ERTE

La combinación de teletrabajo y ERTE puede provocar situaciones no contempladas en los protocolos de seguridad y control de las empresas



Los efectos del covid-19 han provocado que un gran número de empresas en España se hayan acogido o estén en proceso de acogerse a un ERTE, con la incertidumbre además de cuántos de ellos podrían acabar en expedientes de regulación de empleo definitivos. La actual **paralización de la actividad** y sus posibles consecuencias han provocado que a muchas compañías no les quede más remedio que iniciar estos trámites para poder subsistir.

Asimismo, gran parte de las empresas españolas se han acogido al teletrabajo, algunas de forma precipitada y sin la experiencia o preparación necesarias; esto supone llevar inesperadamente sus **recursos tecnológicos al límite.**

Los departamentos de Compliance, Legal, Auditoría, Tecnología y Seguridad llevan años trabajando para crear y perfeccionar **medidas de control**, procedimientos de actuación y adecuación a los requerimientos regulatorios (GDPR, competencia, etc.). Sin embargo, como consecuencia del covid-19, muchas empresas comienzan a sentirse vulnerables, ya que varias de las medidas y políticas implantadas, y que tan rigurosamente empleaban, resultan de **difícil aplicación** en esta compleja situación.

Existen medidas eficaces y de fácil aplicación para minimizar el riesgo para las empresas

La combinación de teletrabajo y ERTE puede provocar situaciones no contempladas en los **protocolos de seguridad y control** de las empresas. Por ello, es imprescindible tener en cuenta la importancia de la seguridad de la información y aplicar las medidas necesarias para conservarla.

El factor más relevante es que millones de empleados están realizando un **intenso uso de los medios tecnológicos** que las empresas han puesto a su disposición para su desempeño profesional (portátiles, smartphones, tabletas, correo electrónico, la nube, etc.). En este contexto, resulta crítico definir protocolos de trabajo, seguimiento y control de empleados, del uso de la tecnología y del acceso a los servidores e información de la empresa, más aún si consideramos que algunos de estos empleados podrían, lamentablemente, verse afectados por un ERTE.

La empresas deben adoptar medidas para proteger sus datos antes de que sea demasiado tarde

Es imprescindible que los **sistemas informáticos** sigan funcionando a pleno rendimiento para permitir que los trabajadores puedan realizar su actividad. Sin embargo, esto conlleva que se pueda estar dejando en segundo plano la seguridad y la **salvaguarda de información sensible** de las empresas. El riesgo de sufrir pérdidas de esta información se incrementa significativamente en estas circunstancias, lo que puede acarrear pérdidas económicas, daños reputacionales, etc.

Existen diversas **medidas implementables**, de forma rápida y sencilla, con el objetivo de salvaguardar y garantizar la integridad de dicha información.

Algunos ejemplos de estas medidas serían los siguientes:

- Revisar y actualizar el **inventario de dispositivos electrónicos** por empleado. El objetivo es tenerlos localizados en todo momento y poder reclamarlos si fuese necesario.
- Control de firmas electrónicas: aumentar el control en los **métodos de autenticación** de empleados en operaciones donde sean necesarios (por ejemplo, que para realizar transferencias se necesite la aprobación de dos personas). Hoy más que nunca, las empresas deben permanecer alerta con respecto a los afamados fraudes del CEO y CFO.
- Muchas empresas emplean **sistemas de almacenamiento en la nube** (OneDrive, G Suite, Dropbox, etc.), que permiten aplicar distintos niveles de control de acceso y gestión de ficheros. Es importante tomar medidas para conocer y asegurarse de que dichos controles están implantados de forma adecuada y saber cuáles son los que utilizan sus empleados.
- Los **registros (logs) de actividad** (accesos a internet, compartir ficheros, conexiones de dispositivos externos, etc.) que generan los empleados mientras se encuentran conectados o utilizando los medios electrónicos corporativos que les han sido asignados para su desempeño profesional suelen almacenarse en los servidores de las empresas por un tiempo limitado (30, 60 o 90 días), tras el cual podrían ser borrados o sobrescritos de forma automática. Es importante adaptar las políticas de rotación y retención de logs, con el objetivo de alargar dicho periodo de almacenaje y salvaguardar los registros de actividad para que no sean destruidos.
- **Monitorización de acceso a la red/servidores** por empleados (por ejemplo, aquellos sujetos a ERTE), o bien, control de accesos en horas poco convencionales. Asimismo, tener en cuenta que cada empleado teletrabajando podría estar conectado a una red wifi con un nivel de seguridad inferior al que disfrutaría en el entorno empresarial (doble autenticación, etc.).
- Los sistemas de **proveedores externos o terceros** (antivirus, seguridad, etc.) pueden almacenar mucha información sensible y registros de actividad. Hay que asegurarse de que el nivel de servicio contratado incluye la salvaguarda y el posible acceso a esta información en caso necesario.
- Revisar o implantar sistemas de administración y/o gestión de los **dispositivos de telefonía móvil corporativos,** que permitan a la empresa controlar y mantener un registro de las conexiones, instalación y borrado de aplicaciones, así como de actividades irregulares que pudieran cometerse con los mismos (borrados masivos, accesos indebidos, etc.).
- Asegurar la creación, salvaguarda y **ampliación del backup del sistema de correo corporativo**, de datos almacenados en servidores y registros de la empresa, así como realizar revisiones regularmente, con el objetivo de confirmar que efectivamente están almacenados los datos que se pretenden y que su contenido permanezca accesible e inalterado.

Las empresas, si no lo han hecho ya, deberían tomar nota y adoptar, cuanto antes, todas aquellas medidas a su disposición para proteger y asegurar sus datos, así como aquellos dispositivos y/o medios corporativos que los puedan almacenar, antes de que sea demasiado tarde.

Autor: **Javier García Chappell**. Senior director de Technology en FTI Consulting España.

Fuente: El Confidencial

https://blogs.elconfidencial.com/espana/blog-fide/2020-04-30/seguridad-empresarial-teletrabajo-tiempos-erte-coronavirus_2570507/