www.mexis.net

CIBERSEGURIDAD:

CUANDO UN DIRECTOR PIDE QUE LE 'DESBLOQUEEN' EL USB

¿Por qué los líderes, algunos de ellos que promueven la ciberseguridad, son los primeros en ignorar sus propios lineamientos?

Hace poco, en una empresa, el director general llegó a la oficina de TI con una petición: necesitaba que le desbloquearan el puerto USB en su computadora.

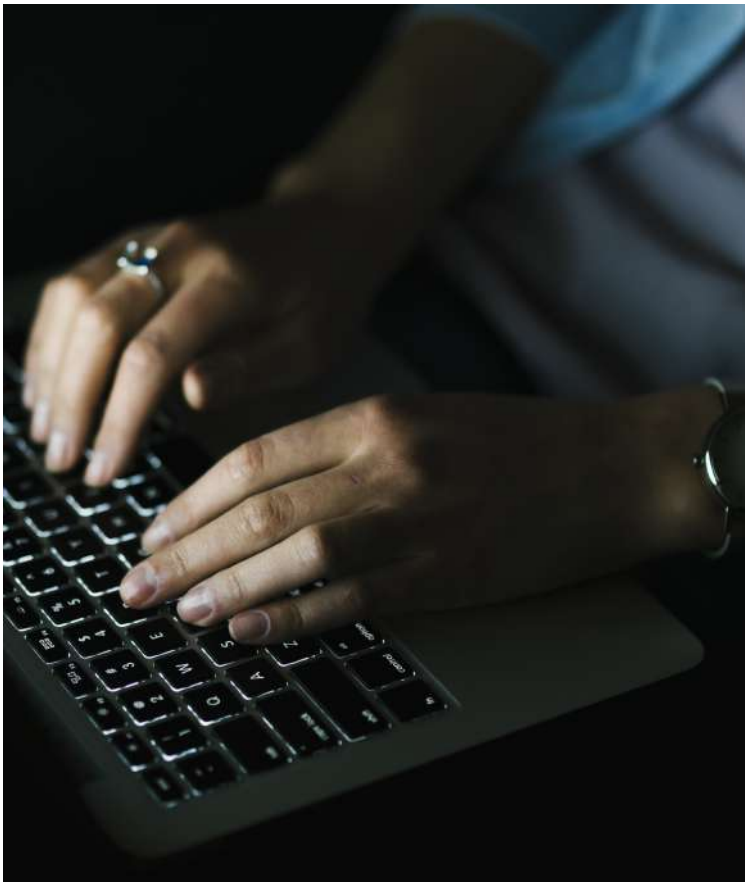
Había traído un dispositivo de almacenamiento para una presentación importante y **el sistema de seguridad de la empresa había bloqueado el acceso automáticamente.** El equipo de TI y ciberseguridad, consciente de las políticas estrictas, explicó que **desbloquear el puerto representaba un riesgo significativo.** Sin embargo, ante la insistencia del director, que necesitaba el material "urgentemente", el equipo no tuvo más remedio que cumplir.

¿Por qué los líderes, algunos de ellos que promueven la ciberseguridad, son los primeros en ignorar sus propios lineamientos?

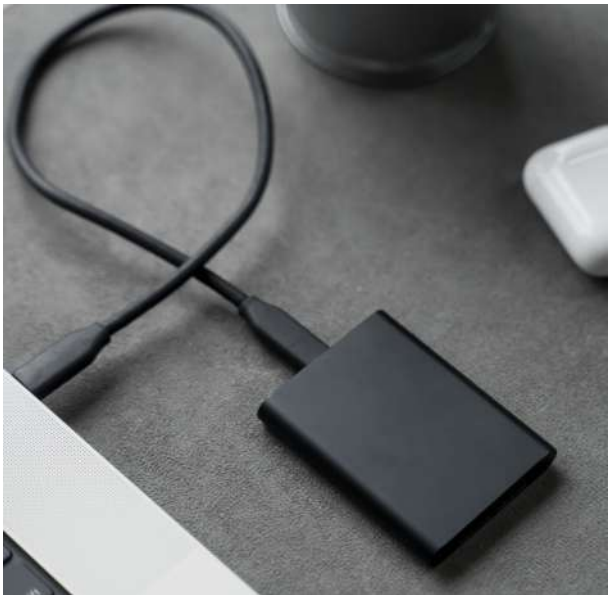
El escenario descrito es más común de lo que parece. Los directores, consejeros y altos ejecutivos, personas encargadas de tomar decisiones críticas para el negocio, suelen ser quienes, por diversas razones, eluden los protocolos de seguridad que ellos mismos ayudan a implementar. Esto genera una contradicción peligrosa: mientras los colaboradores reciben capacitación constante sobre la importancia de seguir las políticas de ciberseguridad, **los líderes envían un mensaje contradictorio cuando no las cumplen.**
Existen múltiples razones para este comportamiento.

Uno de los principales factores es la presión operativa. Los altos ejecutivos suelen estar inmersos en múltiples tareas simultáneas, gestionando aspectos clave del negocio, **lo que les lleva a considerar las medidas de seguridad como obstáculos a su productividad.** En lugar de esperar a que el equipo de TI o ciberseguridad evalúe el riesgo de conectar un dispositivo externo, el director general prefiere tomar el camino más rápido para evitar retrasos, **sin evaluar realmente las posibles consecuencias de una violación de seguridad.**

Además, **muchas veces las políticas de ciberseguridad no están diseñadas pensando en los ejecutivos,** quienes requieren de flexibilidad y agilidad en sus operaciones. Mientras que **para un empleado regular seguir el proceso de ciberseguridad es parte de su rutina diaria,** los directores, acostumbrados a tomar decisiones rápidas, **ven en estos protocolos un impedimento para la eficiencia.** Esto lleva a muchos a evadir ciertas reglas o a **pedir "excepciones" que ponen en riesgo la ciberseguridad general de la empresa.**
El problema también radica en la falta de capacitación práctica específica para altos ejecutivos. Si bien están al tanto de la importancia de la ciberseguridad, **muchos directores no reciben la misma formación detallada que sus equipos.** Los protocolos de seguridad suelen ser vistos como algo ajeno a su rol, cuando en realidad son ellos los principales responsables de proteger la información sensible de la empresa. **Esta falta de alineación entre lo que se espera de ellos y lo que realmente practican genera una brecha de ciberseguridad.**



Sin embargo, quizás el factor más preocupante es la priorización de otras responsabilidades sobre la ciberseguridad. Los directores están enfocados en el crecimiento del negocio, las finanzas y la competitividad en el mercado. **Aunque reconocen que la seguridad es importante, tienden a verla como algo que compete únicamente al equipo técnico,** sin comprender que ellos son parte fundamental de la defensa digital de la organización. **Este desinterés o falta de implicación directa puede resultar en decisiones apresuradas o riesgos innecesarios** sobre las amenazas más recientes puede ayudarlos a ver la ciberseguridad como una parte integral de su rol. De este modo, los líderes no solo estarán más informados, sino también más comprometidos con cumplir los lineamientos de seguridad que protegen a la empresa.



Cuando los directivos ignoran las políticas de ciberseguridad, no solo están poniendo en peligro sus propios sistemas, sino también la seguridad de toda la organización. Si los líderes no cumplen con las reglas que exigen a sus empleados, el mensaje que se envía es que estas medidas son opcionales, **lo cual debilita la cultura de ciberseguridad que se intenta implementar.**

La ciberseguridad debe empezar desde arriba. Los directores y altos ejecutivos deben ser los primeros en seguir estrictamente los lineamientos y dar ejemplo al resto de la empresa. Al demostrar que toman en serio la ciberseguridad, fomentan una cultura de responsabilidad digital que permea en todos los niveles. Solo entonces, la ciberseguridad dejará de verse como una carga burocrática para convertirse en un **elemento esencial para la continuidad y el éxito del negocio.**

Así que, la próxima vez que un director pida que le desbloqueen el USB, la verdadera pregunta es: **¿estamos realmente dispuestos a correr ese riesgo?**

Este ejemplo fue con un simple USB. Hay muchos otros riesgos que toman como el uso de un equipo personal, accesos remotos inseguros, evitar la doble autenticación, instalación de software no autorizado, entre otros.

Fuente de información: forbes.com
Autor: Andrés Velázquez