Artículo de Opinión
Abril 2020

Criminales ponen a prueba la cultura de seguridad digital de las empresas: 8 recomendaciones

5 de cada 10 directivos en México cuentan con un modelo estratégico de ciberseguridad

Por: Christian Andreani,
Socio de Asesoría en Tecnología
y Transformación de
KPMG en México
asesoria@kpmg.com.mx
Visita: www.delineandoestrategias.com


KPMG MÉXICO


KPMG MÉXICO


@KPMGMEXICO


KPMGMX

La pandemia de COVID-19 cambiará la forma en que debemos administrar la ciberseguridad de las organizaciones y, cómo, individualmente, estaremos evolucionando en la madurez y control de los proyectos de forma remota.

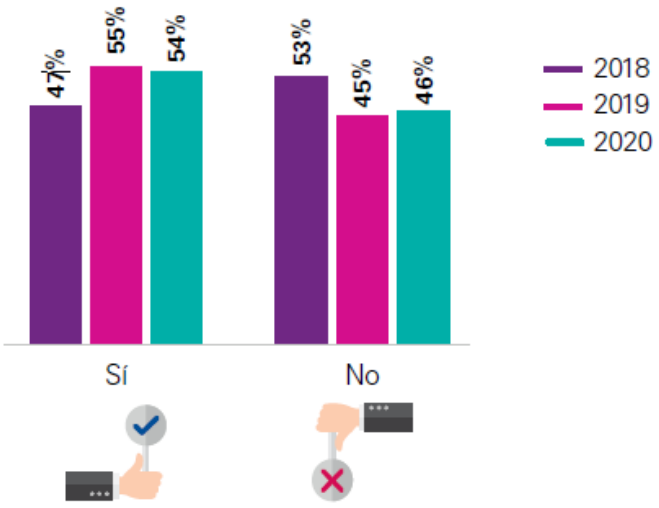
Los grupos criminales pueden aprovecharse de este momento de incertidumbre de diversas maneras, por ejemplo, poniendo a prueba la cultura de seguridad digital y la madurez de individuos y empresas. Es momento de que las compañías se cuestionen y revisen si están preparadas para administrar los riesgos de ciberseguridad.

Trabajo a distancia: desafío para las organizaciones

Diversas empresas han migrado sus operaciones diarias al trabajo a distancia sin saber con exactitud qué implicaciones tendrá esta medida.

De acuerdo con el estudio **Perspectivas de la Alta Dirección en México 2020 de KPMG,** cinco de cada diez directivos aseguraron contar con un modelo estratégico de ciberseguridad.

¿Cuenta con un modelo estratégico para riesgos en ciberseguridad?



Estos datos muestran que los directivos en México aún se encuentran en un proceso de desarrollo en cuanto a la administración de riesgos en ciberseguridad bajo un modelo estratégico, pues 46% aún no cuenta con un modelo con estas características. Aunque no se cuente con un modelo estratégico de ciberseguridad, existen recomendaciones para la gestión de este tema, que pueden servir de base en un momento de crisis.

8 recomendaciones para gestionar la ciberseguridad

Como punto de partida, debemos entender que han aumentado los riesgos solo por el hecho de que se incrementaron las conexiones remotas de la organización. Por ejemplo, hay una mayor necesidad de videollamadas que consumen recursos de VPN y ancho de banda, y las diferentes áreas trabajan mediante herramientas que comparten información. Por ello, es necesario tomar en cuenta las siguientes acciones que minimizarán los riesgos en esta fase:

1. Implementar la autentificación de usuarios remotos al menos con dos factores, por ejemplo: contraseña más *token*
2. Ejecutar procedimientos de actualización continua de antivirus y *firewalls* en las estaciones remotas
3. Abrir una línea de ayuda remota para que los usuarios puedan interactuar rápidamente ante alguna duda o problema que tengan
4. Transferir documentos solo a través de medios configurados y aceptados por la organización, por ejemplo: *e-mail*, herramientas de colaboración, entre otros, y que las mismas se encuentren autorizadas por el CISO (Director de Seguridad Informática o *Chief Information Security Officer*)
5. Apoyarse en un equipo de finanzas independiente, que confirme la viabilidad de pagos en línea al ejecutar grandes transacciones o superando un monto que ponga en riesgo a la organización
6. Revisar los procedimientos de actualizaciones críticas para que estén aplicadas y administradas en los equipos remotos
7. Administrar los respaldos de información crítica (*backups*) de las conexiones remotas, validando su integridad

8. El CISO debe tener un canal de comunicación continua con el equipo de administración de incidentes y crisis, para trabajar de manera cercana en caso de tener algún ataque *ransomware* (ataques que encriptan información y que no permiten el acceso a la misma) que comprometa a la organización

Durante una crisis como la de COVID-19, es necesario que la función de Ciberseguridad vea más allá de lo que se administra como componentes, para anticiparse a los posibles incidentes a los que una empresa está expuesta, por el tipo de operación y tecnología utilizada, así como por la cultura de seguridad de la información que se tenga.

La pandemia de COVID-19 ha impactado los negocios y la vida diaria, poniendo a prueba la capacidad de respuesta de las empresas ante eventos fuera de su alcance. Es crítico evaluar y dar seguimiento adecuado a las prioridades específicas que determine cada organización para afrontar esta crisis.

###

Nota: las ideas y opiniones expresadas en este escrito son del autor y no necesariamente representan las ideas y opiniones de KPMG en México.

Para más información de negocios, síguenos:


KPMG MÉXICO


KPMG MÉXICO


@KPMGMEXICO


KPMGMX