Por Rommel García *

# Ciberseguridad: 5 errores que debemos evitar

> Los ciberatacantes son cada vez más continuos y relevantes, lo cual hace ver que la seguridad en el ciberespacio debe aparecer como prioridad para todas las organizaciones.

Las empresas actualmente cometen 5 errores básicos al tratar de contener a los cibercriminales (individuales, casuísticos o grupos profesionales), que tienen estrategias para robar sistemáticamente propiedad intelectual, o para afectar a los negocios de alguna manera. Los siniestros de los ciberatacantes son cada vez más continuos y relevantes, lo cual hace ver que la seguridad en el ciberespacio debe aparecer como prioridad para todas las organizaciones.

## ENTENDER LAS AMENAZAS PARA PODER CONTRARRESTARLAS

El cibercrimen abarca un rango de actividades ilegales enfocadas a realizar daño a las organizaciones. El término se aplica a diferentes métodos de acción, así como de objetivos. Un "actor" es la persona o grupo que patrocina o conduce ataques y existen cuatro categorías en las que se pueden organizar sus actividades:

- **Hacker:** generalmente actúa solo.
- **Activista:** cuenta con un perfil idealista con una fuerte visión política, a menudo su objetivo es crear temor y caos.
- **Crimen organizado:** enfocado a ganancias financieras a través de diferentes mecanismos tales como el phishing, hasta la venta de datos.
- **Gobiernos:** enfocados a mejorar su posición geopolítica o de intereses comerciales con presupuestos elevados y ambientes de seguridad complejos, que han sufrido ataques cibernéticos.

## ¿EN QUÉ ESTAMOS FALLANDO?

La inversión que las empresas han realizado para protegerse ha sido importante, pero insuficiente. Hoy, existen grandes organizaciones que

han sufrido pérdidas en esta materia (las cuales, al final, se traducen en pérdidas financieras). Si ya estamos conscientes del gran riesgo existente, ¿por qué aún seguimos expuestos? Quizá estamos cometiendo alguno de los 5 errores más comunes en la protección de activos digitales.

### //ERROR 1. "NOSOTROS ESTAMOS SEGUROS AL 100%"

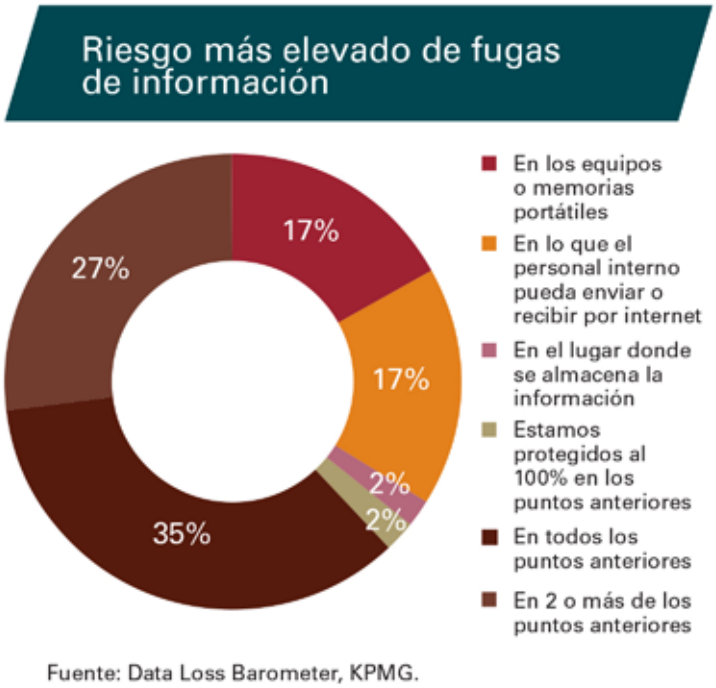
Con datos de una encuesta de KPMG realizada entre los Directores Generales y Directores de Finanzas Chief Financial Officer (CFO) de más de 100 de las organizaciones más importantes de México, pudimos conocer dónde consideraban los directivos que estaban sus principales riesgos de fuga de información.

Lo más impactante de las respuestas fue que un 2% de los encuestados contestó que estaban protegidos al 100%. Una postura de seguridad total es una meta inalcanzable. Hay organizaciones gubernamentales, financieras y tecnológicas, que han sufrido ataques cibernéticos, demostrando a pesar de los presupuestos altos y sistemas de seguridad complejos, que nunca podemos estar seguros a cabalidad.

Una postura de defensa adecuada se basa en entender correctamente las amenazas relativas (Prevención), las vulnerabilidades de la organización (Protección), el establecimiento de mecanismos para detectar brechas inminentes (Detección), y el establecimiento de capacidades de respuesta al incidente (Integración), para minimizar las pérdidas.

### //ERROR 2. "INVERTIMOS EN LAS MEJORES HERRAMIENTAS, ASÍ QUE ESTAMOS PROTEGIDOS"

El mundo de la ciberseguridad está dominado por proveedores que venden productos que ofrecen una rápida




Fuente: Data Loss Barometer, KPMG.


detección de intrusos, en cualquier ambiente o arquitectura tecnológica.

Las herramientas, sin embargo, se complementan con un elemento básico para una estrategia de ciberseguridad holística y robusta: el personal de la organización. Este es el factor más trascendental en la seguridad, ya que las herramientas dependen de una buena administración, así como de diversos procesos de mantenimiento.

### //ERROR 3. "NUESTRAS ARMAS SON MEJORES QUE LAS DE LOS HACKERS"

Los ciberatacantes permanentemente desarrollan nuevos métodos y tecnologías para obtener beneficios o destruir a las organizaciones. En este sentido, las defensas siempre van un paso atrás, por lo que nuestros oficiales de seguridad deben conocer cuál es el tipo de atacantes atraídos por la organización, el tipo de negocio que les parece atractivo y por qué, es decir, las empresas deben conocer la inteligencia de las propias amenazas.

### //ERROR 4. "TODA REGULACIÓN EN CIBERSEGURIDAD IMPLICA MONITOREO EFECTIVO"

Las organizaciones, en mayor o menor grado, están sujetas a regulaciones de ciberseguridad. Una "visión de mero cumplimiento" respecto de la ciberseguridad, nos llevará a pensar que el tema es irrelevante para el negocio, viéndolo más como un estorbo, que como un proceso que aporta valor.

Las organizaciones deben asumir que las amenazas evolucionan, cómo lo hacen, y, sobre todo, cómo pueden anticiparse a ellas, lo cual hará que el monitoreo sea realmente efectivo.

### //ERROR 5. "TENEMOS UN ÁREA DE CIBERSEGURIDAD QUE NOS PROTEGE"

El principal reto que enfrenta el área de Ciberseguridad es hacer a todos los colaboradores de la empresa, partícipes de las iniciativas de protección.

En conclusión, la solución real en términos de ciberseguridad se ubica en todos los espacios de la organización. La ciberseguridad es una actitud, y debe convertirse en parte de la política integral de la empresa. ■

* Rommel García es Socio de Asesoría en Tecnologías de la Información de KPMG en México, y se le puede localizar en asesoria@kpmg.com.mx, o visitando la página www.delineandoestrategias.com