# Más desafíos para el cuidado de los datos

**Tecnología.** La digitalización ha llegado acompañada de crecientes amenazas en seguridad, que ameritan reformular las políticas corporativas.

MARCELA MENDOZA RIOFRÍO

Los ataques cibernéticos crecen todos los años, pero en el 2018 el país presentó niveles fuera de lo ordinario. Solo en simples ataques DoS (negación de servicio distribuido o DDoS, por sus siglas en inglés) el alza fue de 740%. Y el ramsware (secuestro de datos para cobrar un rescate) se elevó mucho y puso en apuros tanto a filiales de grandes multinacionales como a las pymes.

El suceso más significativo, sin duda, se dio en agosto, el día en que varios cajeros dejaron de funcionar, no se podían realizar algunos pagos en línea ni ejecutar transferencias interbancarias. El pánico llegó con una alerta de ataque global y el recuerdo de los US$10 millones que poco antes había perdido el Banco de Chile.

Asbanc salió a declarar que los bancos locales habían resistido todos los ataques del día sin inconvenientes. Y no faltó a la verdad. Sin embargo, los hackers sostienen que eso fue posible porque aquí no recibimos el mismo tipo de ataque dirigido que recibió Chile. De hecho, los delincuentes ya han diseñado hasta manuales para replicarlo acá y si los aplican, los daños serían similares.

¿Estamos a nivel corporativo y Estado reaccionando de la forma que deberíamos ante las amenazas al alza? Un reciente estudio de EY refiere que el 16% de las organizaciones considera regularmente la seguridad de la información en sus planes, pero solo un 3% ha hecho un incremento en el presupuesto en el 2018 y apenas un 7% planea elevarlo este año. En el mundo, en cambio, eso es algo que contempla el 65%.

Franz Erni, gerente país de Fortinet Perú, reconoce que la adquisición de soluciones de seguridad no crece al ritmo que debiera. A diario se reciben miles de asaltos y un promedio de diez intentos de ataques dirigidos (APT) al mes, pero muchos siguen pensando que es un gasto postergable.

Jorge Zeballos, gerente general de ESET Perú, añade que aquí se logra un alza del 30% anual en un mercado de alrededor de US$400 millones, pero eso apenas es la décima parte de lo que se podría estar invirtiendo.

Los problemas de seguridad, advierte, se irán intensificando en la medida en que más empresas se inmiscuyan por completo en la transformación digital y en el uso de los objetos que se conectan a Internet para comunicarse entre ellos (IoT). El camino de conversión se recorrerá con éxito si se incluye una mayor protección, recalca.

### POLÍTICAS CON REDISEÑO

Cuando se piensa en seguridad en medio de un universo lleno de datos digitales, la mayor conciencia empresarial de los riesgos es solo una parte del problema. El marco legal y la eficiente supervisión del cumplimiento de la ley son la otra arista, advierten los consultores de EY, quienes no creen que haya gran déficit normativo ni en la ley de protección de datos ni en la que pena los delitos informáticos.

Óscar Montezuma, socio fundador de Niubox, refiere que el más reciente reporte de ciberseguridad de la OEA y el BID concluyó que en el caso del Perú hay normas importantes, pero se carece de una estrategia y cadena de mando clara que impide fortalecer su control.

Este año, en febrero, se ha dado un avance importante porque nos adherimos al Convenio de Budapest, luego de cinco años de gestionarlo. Ello implicará acceder a una mayor cooperación internacional para controlar y combatir estos delitos.

Montezuma estima que tras la firma es posible que se necesiten modificaciones adicionales a las normas penales existentes, pero sobre todo se requerirá capacitar a los fiscales y jueces penales, lo que podría tomar un año. Los beneficios serán tanto para el sector público como el privado, pues tendrán un derrotero claro para sus políticas de cumplimiento.

Pero es dentro del sector privado en donde existe una urgencia de reforma en términos de políticas internas para el cumplimiento de la ley, sobre todo entre los proveedores de servicios. Los expertos coinciden en que no solo se necesita que un Plaza Vea o un Marriott cuide el servidor, en donde tiene la base de datos de clientes, sino un Google o un Facebook que interiorice acá prácticas como las que le dispone la nueva normativa europea (RGPD), pues ese es el estándar que seguirá la región.

Miguel Morachino, director de Hiperderecho, destaca que una cuota muy importante de responsabilidad recae sobre los operadores de telecomunicaciones. Ellos son quienes trasladan la data por el ciberespacio y están desaprobados en términos de implementación de políticas y cuidados para garantizar un tratamiento idóneo. Se han visto mejoras en los últimos tres años, acepta, pero el camino pendiente aún es largo.

**Indicadores**

## Mejores prácticas de protección

Hiperderecho ha desarrollado el estudio "¿Quién defiende tus derechos?", basado en el modelo de la Electronic Frontier Foundation (EFF), en el que se evalúa si se cumple con las mejores prácticas de protección.

Entre las conclusiones se destaca que los usuarios desconocen las medidas adoptadas para protegerlos. Algunas marcas han mejorado sus políticas superando lo exigido por la ley local, pero el usuario no lo sabe.

**CRITERIOS DE LA EVALUACIÓN**

¿Cumplen las telco con cuidar la privacidad de los datos?

**Políticas de privacidad**

| | Cuenta con políticas de privacidad y protección de datos personales aplicables al servicio de telecomunicaciones que presta. | Comunica en lenguaje simple sus políticas de privacidad y protección de datos personales a través de su página web. | Incluye en sus políticas de privacidad y protección de datos personales la información sobre por cuánto tiempo y para qué almacena la información de sus usuarios. |
|---|---|---|---|
| Bitel | 0,33 | 0,33 | 0,33 |
| Claro | 0,33 | 0 | 0,33 |
| Entel | 0,33 | 0 | 0,33 |
| Movistal | 0,33 | 0,33 | 0,33 |
| Olo | 0 | 0 | 0,33 |
| InkaCel | 0,33 | 0,33 | 0,33 |

**Autorización judicial**

| | Exige la existencia de una orden judicial expresa y previa, antes de entregar datos sobre el contenido de comunicaciones a las autoridades de seguridad y justicia. | La empresa exige la existencia de una orden judicial expresa y previa, antes de entregar metadatos almacenados de sus usuarios. |
|---|---|---|
| Bitel | 0,50 | 0 |
| Claro | 0,50 | 0 |
| Entel | 0 | 0 |
| Movistal | 0,50 | 0,50 |
| Olo | 0 | 0 |
| InkaCel | 0 | 0 |

**Notifiación al usuario**

| | Cuando su información personal o comunicaciones han sido objeto de una solicitud de acceso por parte del Gobierno. |
|---|---|
| Bitel | 0 |
| Claro | 0 |
| Entel | 0 |
| Movistal | 0 |
| Olo | 0 |
| InkaCel | 0 |

**Transparencia**

| | Publica reportes de transparencia que contenga información anonimizada sobre el número de solicitudes de acceso a información personal o comunicaciones de autoridades nacionales o internacionales recibidas y aceptadas. | Incluye en sus reportes de transparencia información sobre bajo qué supuestos y de qué manera puede entregar la información de sus usuarios a una autoridad. | La empresa pone a disposición de sus usuarios información estadística sobre la motivación, tipo de datos solicitados, de los pedidos de acceso a datos de autoridades recibidas y aceptadas. |
|---|---|---|---|
| Bitel | 0 | 0,33 | 0 |
| Claro | 0 | 0,33 | 0 |
| Entel | 0 | 0 | 0 |
| Movistal | 0,33 | 0,33 | 0,33 |
| Olo | 0 | 0 | 0 |
| InkaCel | 0 | 0 | 0 |

**Compromiso con la privacidad**

| | La empresa ha controvertido en sede judicial mandatos o pedidos de acceso a información sobre sus usuarios, que considera indebidamente formulados o sustentados. | Participa enviando comentarios formales a proyectos de ley y de propuestas de reglamentación en favor de la privacidad de sus usuarios. |
|---|---|---|
| Bitel | 0 | 0 |
| Claro | 0 | 0 |
| Entel | 0 | 0 |
| Movistal | 0 | 0 |
| Olo | 0 | 0 |
| InkaCel | 0 | 0 |

Fuente: Hiperderecho