PERIÓDICO	PÁGINA	FECHA	SECCIÓN
EL FINANCIERO	35	05/10/2022	COLUMNAS Y ARTÍCULOS

El problema, el no remedio y el trapito

Hace poco escuché una explicación de lo que hace un banco para mantener a raya a los ciberdelincuentes. Fue detallada, pero partía de una lógica sencilla de ilustrar.

Los funcionarios de ese banco –la reunión fue *off the record*– contaron que, en efecto, tienen muchos recursos y bastante presupuesto dedicado a frustrar *hackeos* de los ciberdelincuentes.

Se trata, me dijeron, de una carrera permanente para hacer más alta, por decirlo de una manera, la barda protectora: los criminales cibernéticos innovan para saltar esa barrera digital, y el banco, de manera preventiva y también de forma reactiva, busca hacer cada vez menos vulnerable ese muro.

En la visión de ese banco, la enorme mayoría de las transacciones está a salvo. Hay *hackeos* y fraudes cibernéticos, sin duda, pero representan una fracción diminuta de las operaciones diarias.

Lo anterior a pesar de que, a menudo, escuchamos o leemos historias de que alguien resultó saqueado. Ahí, aseguraron los del banco, empieza otra historia. Una que no sin sorpresa resulta poco popular.

LA FERIA

Salvador Camarena

Opine usted:
nacional@elfinanciero.com.mx

@salcamarena

Ruidosas denuncias que leemos en redes sociales sobre fraudes cibernéticos muchas veces son –asegura el banco– producto de errores que, de una forma u otra, son achacables a los cuentahabientes. Desde contraseñas increíblemente predecibles hasta candidez del ahorrador al dar, en persona, en línea o vía telefónica, información en trámites no solicitados.

Y también hay, por supuesto, graves casos de suplantación de identidad a partir del robo de datos personales y de complicidad, ni duda cabe, de funcionarios en sucursales bancarias.

De remate, en no pocos casos hay renuencia de los defraudados a levantar una denuncia, cosa que contribuye a la impunidad.

Sirva esta comparación para hablar del *GuacamayaLeaks*, no vaya a ser que confundamos el problema, el remedio y el trapito.

A partir de que se conoció, el jueves, que la Secretaría de la Defensa Nacional había sido *hackeada*, surgieron voces desde el Congreso de que lo que hace falta es hacer nuevas leyes de ciberseguridad. Claro, los legisladores siempre creen que su papel se reduce a hacer leyes, y para nada a llamar a cuentas a quienes no están cumpliendo con las existentes.

En el saqueo a la Sedena el ciudadano podría pagar muchos costos sin haber cometido error alguno

... salvo el de haber depositado su confianza en una institución cuya respetabilidad dependerá de la forma en que expliquen lo que no hicieron

El problema hoy no es la ciberseguridad del futuro de la Defensa Nacional. El problema es que el ataque ya ocurrió, que se desoyeron advertencias de la auditoría, que el gobierno juega al tío lolo en este delicado asunto, que la Sedena hace como si la seguridad nacional y la pública –ya no digamos su imagen– no estuvieran en juego por esta megafiltración y que el Congreso es uno más de los que no están reaccionando bien.

Así que, en vez de haber invertido permanentemente en ciberseguridad para hacer más difícil el éxito de los ataques, en vez de revisar qué falló, en lugar de rendir cuentas en público, el Ejército sigue sobrado en su actitud de a mí no me exige nadie y apruébenme todo lo que pido.

El no remedio son más leyes. No en este momento con una clase política, en su mayoría, capturada, como vimos ayer, por el antipatriotismo.

Y el trapito de ese no remedio es el Congreso: cuya mayoría se pone de tapete a las Fuerzas Armadas y a Palacio Nacional.

Porque, a diferencia de lo que pasa con la banca, en el saqueo a la Sedena el ciudadano podría pagar muchos costos sin haber cometido error alguno, salvo el de haber depositado su confianza en una institución cuya respetabilidad dependerá de la forma en que expliquen lo que no hicieron para prevenir este problema, y lo que harán para remediarlo.