BANCA Y TRANSACCIONES SEGURAS

De acuerdo con el **BID**, los daños económicos de los **ataques cibernéticos** podrían encontrarse **por encima del 1% del PIB** en algunos países y, en el caso de los **ataques a infraestructura crítica**, podría llegar a ser del **6%**. Estas cifras vuelven a poner el foco en la importancia crucial que tienen las políticas e **inversiones** de ciberseguridad para aumentar y consolidar la **confianza de los ciudadanos** en las tecnologías digitales que, ahora más que nunca, hacen parte de sus actividades cotidianas.

Uno de los **sectores de la industria** que debe enfocar sus estrategias y procesos de transformación digital en **garantizar la seguridad de sus productos y servicios,** para mantenerse competitivo en el mercado y para sus clientes, es la banca.

En uno de nuestros Newpter: encuentros digitales, dos expertos de Cisco y Axity pusieron sobre la mesa algunas de las cuestiones que las entidades financieras deben identificar y tener en cuenta para **dirigir mejor los desafíos de ciberseguridad,** sobre todo en un momento como el actual. Acá te compartimos algunas de las conclusiones de esta conversación.

La pandemia aceleró la evolución del mundo financiero y de las amenazas

Aunque **antes del covid-19** las entidades ya estaban replanteando su infraestructura para **responder a la demanda de la digitalización** y, por ejemplo, poder competir con las Fintech, la pandemia generó un efecto catalizador que **aceleró todos los procesos de transformación digital**, moviendo la fuerza laboral hacia lo remoto, exigiendo disponibilidad de recursos, así como adopción y migración a la nube y levantamiento de **mayores instancias y capacidades virtuales.**

De cara a sus usuarios, las **instituciones financieras** tuvieron que moverse a una mayor velocidad para garantizar la disponibilidad de sus servicios, **ofrecer acceso a mejores soluciones**, créditos, medios de pago, costo adecuado, experiencias de los usuarios, etc.
Sumado a estos esfuerzos, **la ciberseguridad ocupó un lugar prioritario,** pues la pandemia también propició el lanzamiento de campañas maliciosas que se aprovechaban de las circunstancias para afectar entidades y clientes.

Ante el panorama, qué pasos seguir: frameworks de referencia

Pese a los avances, el camino de las entidades sigue exigiendo toma ágil de decisiones, de ahí la importancia de establecer **frameworks,** pues guían a las compañías de todos los tamaños a **gestionar y a reducir los riesgos para proteger la información.** Al respecto, los expertos nombran al framework de ciberseguridad de **NIST (el Instituto Nacional de Normas y Tecnología en Estados Unidos)** como uno de los marcos de referencia que abarca una serie de pasos a seguir para poder identificar, recuperar y saber actuar en diferentes puntos del ciclo de una amenaza.

No obstante, uno de los **desafíos** que implica el trabajo con esas líneas guía es poder establecer una conversación que articule el negocio con la tecnología y en la que directores y decisores de las entidades logren ver cómo están, qué hace falta y qué hay que hacer, de modo que se den las inversiones y los presupuestos necesarios. El reto no se trata, entonces, de la adquisición o implementación de una solución, sino en **conectar precisamente las áreas de negocio con las tecnológicas,** tanto dentro como fuera de las entidades, para saber cómo usar qué herramientas. Por lo tanto, lo que permite tener inversiones más asertivas y estratégicas es entender que **más allá de la tecnología, la solución implica tener una visión correcta de dónde están los problemas.**

Productos bancarios seguros desde su concepción

En la actualidad, **la seguridad es un componente que se brinda al final del desarrollo de un producto.** Pero, idealmente, el sector de la banca debería encontrar un equilibrio entre productos y servicios que brinden una **experiencia de usuario óptima**, a la vez que sean lo más seguros posible.
Según el World Economic Forum, la seguridad debe pensarse estratégicamente y ha de darse desde el diseño de un producto, entre otras cosas, para que al nacer seguro reduzca sus huecos de seguridad. Cuando se toma en serio ese concepto de la seguridad se ve que es necesario un cambio organizacional en el que se logre realizar, en la práctica, la seguridad desde el inicio.

No obstante, aunque este **balance entre experiencia óptima y segura** sea un desafío, el objetivo de trabajar en ambos aspectos deberá ser **ofrecer al usuario confianza,** permitiéndole entender cómo y qué hace la entidad para proteger su información, identidad y dinero. **La confianza pasa a ser un recurso competitivo para las entidades financieras: "en la entidad en la que yo confíe más, voy a poner mi dinero".**

La tecnología como factor diferenciador de la seguridad

Uno de los **retos** actuales de las entidades es **brindar confianza a los usuarios** escépticos o que tienen temor de usar productos o servicios financieros digitales. Ahí, las herramientas tecnológicas tendrán un rol facilitador y deberán **aportar visibilidad, simplicidad y eficacia a los usuarios.**

Según nuestros expertos, uno de los diferenciadores es la infraestructura en la nube, pues permite pensar en la **seguridad como un servicio**, convirtiéndose en el gran habilitador tecnológico. De hecho, también mencionan, las entidades que se anticiparon y entendieron la seguridad desde ese concepto, lograron **mejores resultados** a partir de decisiones más adecuadas.

Axity y Cisco: soluciones inteligentes

"La tecnología no hace que pasen cosas, las personas eligen qué hacer con las tecnologías para generar los cambios".

Las entidades deben saber contar con **aliados estratégicos** que comprendan los desafíos, pero también las soluciones de ciberseguridad para poder **evolucionar sus servicios de banca.**

Desde nuestra visión, esta evolución permite, entre otras cosas, **minimizar riesgos, mejorar la detección de amenazas,** contar con sistemas de monitoreo, tener visibilidad continua de vulnerabilidades y riesgos y análisis avanzado; y todo esto, **hecho de forma transparente para el usuario.**
La clave es invitar a las entidades a permitirnos **conocer las necesidades tecnológicas y de negocio** para tomar las decisiones correctas y saber cómo dirigir las tecnologías y abordar los esfuerzos de modo tal que **se transforme en valor para la entidad.**

Si quieres conocer más, te invitamos a acceder al conversatorio completo **aquí**

axity.social
axity_social
axity_social

Si en algún momento deseas contactarnos, no dudes en escribirnos al siguiente correo:
contacto@axity.com

Visita nuestro sitio web
www.axity.com