

DESGRABACIÓN

LUCAS PATANÓ

Gracias Gabriela. Buenas tardes. Mi nombre es Lucas Patanó, trabajo en Gire Soluciones, una empresa del grupo Gire que brinda soluciones de outsourcing para empresas, entidades financieras y entes gubernamentales.

Damos servicios hace más de 25 años en el mercado a empresas de primera línea y también es una de las dueñas de la empresa Rapipago, los invito si quieren visitar www.giresoluciones.com.ar.

Tenemos tres divisiones de servicios, brindamos servicios relacionados a lo que es recaudación y pagos, sumando el expertise de Rapipago nos podemos integrar con cualquier medio de pago y tenemos una división exclusiva de procesamiento de cheques.

El año pasado fuimos una de las primeras empresas que lanzó al mercado la captura de cheques con celular, van a ver que hoy en día hay muchos bancos que lo tienen.

No tenemos la marca final sino que usan quizá nuestra aplicación con la marca propia del banco, pero fuimos uno de los primeros en lanzar en el mercado argentino esa solución.

También tenemos soluciones relacionadas con la digitalización, está relacionado con acompañar a nuestros clientes en esa transformación digital, pasar del mundo papel, esos formularios en papeles y tenerlos todos en un formato digital workflows, documentación nativa digital.

La charla está relacionada con la seguridad informática, cumplir con los procesos e ir más allá tiene que ver con, es decir, ¿le cobro a mis clientes, le mando a hacer débitos automáticos, les pido el número de tarjeta y les cobro? ¿también soy conciente de que estoy guardando un dato sensible para mis clientes?

Cuando planificamos un viaje, ¿qué hacemos?, nos vamos a ir con el auto al sur por ejemplo a Bariloche. Antes de irnos de vacaciones mandamos el auto al mecánico, chequeamos que esté todo bien, revisamos el nivel de aceite, los neumáticos y que los frenos funcionen bien. Antes de emprender el viaje hacemos un control previo: mandarlo al mecánico y después cuando estamos viajando en el auto, seguimos haciendo controles y chequeando cosas.

Si quiero pasar a alguien uso la luz de giro, controlo cuando tengo la próxima estación de servicio, me pongo el cinturón de seguridad, me armo una lista en Spotify para no quedarme dormido, hago un montón de cosas durante el viaje. Me preparo antes y durante el viaje.

Lo mismo tiene que pasar con las tarjetas de crédito, porque hay que ser conciente de los riesgos. Cuando les decía recién antes de hacer el viaje me fijo en un montón de cosas, es porque soy conciente de que si no mando el auto al mecánico se me puede romper en la mitad del viaje.

Si no me armo una buena lista de música en Spotify me puedo quedar dormido, si voy a cruzar la ruta del desierto tengo que saber si me voy a dormir antes de cruzarla o después, eso es planificar. Porque soy conciente del riesgo uso el cinturón de seguridad, también porque soy conciente del riesgo ante un accidente.

Lo mismo pasa con las tarjetas de crédito, tengo que prepararme antes de recibir todos los números de tarjeta de crédito de mis clientes para poder cobrarles. Cosa que me imagino que ya es tarde porque todos si trabajan en una empresa de seguros ya manejan números de tarjeta de crédito, estamos un paso más adelantado pero se puede volver atrás y revisar.

Después en el día a día, cada vez que les cobramos a un nuevo cliente le pedimos el número de tarjeta de crédito también tenemos que ser conscientes de ese número de tarjeta de crédito ¿dónde lo tomamos, a dónde va, dónde queda guardado? Cualquiera de mi empresa puede verlo o puede usarlo, ¿qué tan accesible está ese número de tarjeta de crédito?

Vamos a unos datos para tener y marcar un poco un orden de magnitud de cómo son los pagos electrónicos en la región.

Actualmente en Latinoamérica el 20% de los pagos son pagos electrónicos, este número es de algunos meses, puede ser que haya crecido un poquito más y seguramente va a seguir creciendo.

Argentina aparece en el tercer puesto con el 22% de pagos electrónicos versus efectivo, sin ir más lejos, uno puede ir a Chile y cuando va a un restaurant y cuando quiere pagar con la tarjeta de crédito viene el mozo con el POS no toca nunca tu tarjeta de crédito, haces vos mismo la transacción, firmas y te vas.

Hoy acá si vas a un restaurant y le dan la tarjeta al mozo y esperamos unos minutos hasta que vuelva y no sabemos qué hace con la tarjeta.

Todavía nos falta un poco para llegar a eso pero no estamos tan lejos. Lo importante es que los pagos electrónicos en Argentina van a empezar a crecer, por qué lo estamos viendo en todos lados.

El otro día leí una nota que decía que el Banco Central argentino era uno de los que más estaba impulsando la innovación en Latinoamérica respecto de las tendencias de los medios de pago.

El año pasado sacaron el depósito de cheque con celulares, ahora están impulsando un montón de medios de pagos electrónicos, por ejemplo puede ser el de BIN que creo sale ahora en Agosto, salió PAI que es una billetera, hay un montón de impulso a migrar hacia el pago electrónico.

¿Por qué en Argentina todavía es tan bajo ese número o podemos decirle que es bajo? Creo que por dos situaciones puntualmente.

Una cuestión de la bancarización, ha ayudado muchos años a los negocios como Rapipago de cobrar en efectivo y por otra parte, la cultura. Tengo 29 años y tengo amigos que hoy en día cobran y sacan la plata y se la quedan en la casa y pagan todo en efectivo, no usan las tarjetas. Es un tema cultural.

Pero entendemos que mediante la obligación o como digo siempre mediante la estimulación del efectivo esto va a empezar a crecer y las señales son claras.

El otro día salió que había determinados pagos de la AFIP que no se podían pagar más en efectivo. También por el lado de la desincentivación, le pusieron impuestos al manejo del efectivo, entonces el manejo del efectivo es más costoso, siempre impulsando a ir hacia los medios de pago electrónicos.

Otro dato que está relacionado con esto y es que el 29% de las empresas fue atacada en la Argentina. Recién les hablaba del efectivo versus los pagos electrónicos, esos como un cambio de paradigma en la cobranza, en la forma de cobrar para las empresas.

Hoy cuando alguien te va a pagar en efectivo a una ventanilla bancaria, a un Rapipago o cualquier competidor de Rapipago, la empresa genera un archivo de facturación y se lo manda a los medios de pagos que tiene habilitados para que el cliente lo pueda ir a pagar.

No tiene ningún dato del cliente, a lo sumo tiene el monto de la factura y el número de teléfono o un dato que identifique más el monto que tiene que pagar.

Cuando empezamos a pagar con medios electrónicos el paradigma de la cobranza de voy a pagar cuando quiero, donde quiero y si quiero no pago a lo sumo me cortarían el servicio, cambia. Cuando ustedes cobran con débito automático, el cliente le confía a su compañía un número de tarjeta de crédito.

Cuando vienen mis amigos a casa no ando mostrando la tarjeta de crédito, no tengo la tarjeta de crédito en la mesa. Sus clientes confían en ustedes y le dan ese número para que mensualmente le debiten determinada cantidad de dinero de su cuenta por el servicio que habían acordado. A veces pasa que hacen un doble débito y no le gusta al cliente, tengan eso en cuenta.

El cambio de una cobranza tradicional donde cada uno va paga donde quiere y cuando quiere a tomá te doy un dato mío que es confidencial, guardamelo bien porque te lo doy a vos que confío y cobrame lo que me dijiste que me ibas a cobrar, no me cobres más, mensualmente.

Al cambiar ese paradigma también cambia el paradigma de donde se guarda la información. Imagínense que los números de la tarjeta de crédito no están en formularios, una caja o salón, están guardados en alguna nube de algún sistema hoy en día.

Antiguamente teníamos números de tarjetas de créditos en formularios, podíamos tener un millón de clientes, tener un millón de formularios en una habitación y si nos querían robar la información, había muy pocas opciones.

Una era que un empleado vaya entrando y vaya robando formularios y empezara a hacer fraudes con tus números de tarjeta de crédito, pero no se podía llevar 100 mil cajas con números de tarjeta de créditos. Otra opción era que entre un grupo comando y te robe todas las cajas pero también es muy poco probable.

En cambio al tener los números de tarjetas de crédito en la nube con un solo click te roban toda la información en instantes, la información está en la nube y te pueden robar todos los números de tarjetas de crédito, te los pueden cambiar, borrar, lo que les va a traer un dolor de cabeza en sus compañías.

Ernst&Young hizo hace poquito una conferencia donde juntó a principales directivos de las compañías de la parte comercial y de la parte de seguridad informática, donde hablaron de temas de seguridad, todos hablamos de la seguridad pero a veces no somos conscientes hasta que nos pasa algo.

Voy a mostrarles seis grandes conclusiones que me parecen que son bastante reveladoras. Hay un globito de los que voy a mostrar que es mi favorito pero vamos a ver los seis.

El primero, es que más de un tercio de las empresas no puede prevenir un ataque informático.

¿Vieron cuando les decía que agarramos el auto y lo llevamos al mecánico por si tengo la correa un poco gastada no se me rompa?, estoy previniendo que se me rompa en el viaje. Es importante porque una vez que entra un ataque informático, un hackeo a su base de datos sabemos que puede llegar a pasar.

El segundo dato es que el 57% de las empresas sufrió un ataque informático, ahora todos saben que la información está en la nube y cualquiera de sus empleados quizá pueda entrar a una aplicativa y ver un número de tarjeta de crédito sin ningún problema o tener un formulario con tarjetas de crédito.

Es un dato de que como hoy la información está en la nube, constantemente están los hackers o quien sea buscando la vulnerabilidad a los sistemas para entrar y robar la información, hay que estar atento y cada vez más buscan robarle la información para hacerse base de datos o hacer algún desastre.

El 34% de las empresas tiene poca probabilidad de detectar un ataque a tiempo, si no llegamos a detectar el ataque a tiempo no sabemos qué va a pasar, una vez que entró hay que esperar a ver qué pasa.

Es importante estar preparados antes para lo que va a venir y eso es clave, para saber si un día tienen la desgracia de recibir un ataque informático, que información le pueden llegar a robar o donde puede ser la vulnerabilidad de sus sistemas.

Ahora viene mi loguito favorito. Con este dato es donde uno empieza a caer un poco más en conciencia de guardar al seguro la información. El 89% de las empresas no evalúa el impacto financiero y reputacional de un ataque.

Una famosa empresa que vende video juegos, tiene una consola y para poder jugar por Internet uno tiene que poner la tarjeta de crédito y puede comprar jueguitos. Hace unos años le robaron la base de datos de sus clientes con los números de tarjetas de créditos.

Soy usuario y en un momento me dijeron: tuvimos un problema con la información, te voy a pedir que me des de nuevo tu número de tarjeta de crédito y además te regalamos 10 dólares para hacer la transacción que quieras dentro de nuestra plataforma de juegos.

Después nos enteramos lo que había pasado, le habían robado la base de datos de los usuarios con las tarjetas de crédito, salió en un montón de noticias del mundo de sistemas, en la expo de videojuegos salió publicada esa información. No es un dato menor si un día recibe un ataque cibernético, a nivel reputacional también es negativo no sólo pensemos en la parte de sistemas, pensemos en la marca.

Como les decía, cuando le van a cobrar a un cliente él les da un dato que no se lo da cualquiera y es el número su tarjeta de crédito y tienen que guardar ese dato de forma segura.

El segundo impacto, es el financiero. Imagínense esa consola de videojuegos, esa empresa que no tuvo los números de tarjetas de crédito de sus clientes lo que le costó volver a pedirle a todos sus usuarios los números de tarjetas de crédito; las veces que no pudo cobrar en esos días hasta que recuperó todos los números de tarjetas de crédito, los reclamos que tuvieron y la gente que decide darse de baja por no confiar en esa empresa.

Otro ejemplo más reciente que no tiene que ver con números de tarjetas de crédito pero que tiene que ver con robo de información, fue hace poquito con un hackeo mundial. A uno de los principales servicios de e-mails del mundo le habían robado las claves de todos sus usuarios, no sé si saben pero ahora cada vez que entran a ese correo les piden que cambien la clave o por nuevas medidas de seguridad les pedimos que cambien la clave de usuario.

Esa empresa se acordó tarde, ya le habían robado todo y un dato es que una vez que le robaron todas las claves, después la empresa dijo, por seguridad cambien las claves a todos los usuarios que tienen en el mundo. El 10% las cambió, el resto no usó más el correo electrónico y mantuvo esa clave.

Soy uno de los que mantuvo la clave y casi ni uso más ese correo electrónico porque me generó desconfianza. La seguridad informática es un complemento, no es la parte acorde al negocio pero es un complemento crítico de nuestro negocio.

La parte financiera. Si un día a ustedes le roban los números de tarjetas de sus clientes no le van a poder cobrar por uno, dos, tres o cuatro días; imagínense en el flujo de su compañía no podés tener ese dinero ingresando en sus balances.

El 48% asegura que sus controles de seguridad están desactualizados. ¿Tiene lógica? Sí, tiene lógica esto.

Ahora hay actividades complementarias como los procesos de cobranza que tienen que ser seguros que quizás porque el foco es comercial, el foco es la venta, se olvidan y también son complementarios y son importantes.

Para esas cosas hay empresas como Gire Soluciones que los pueden ayudar y acompañar, nosotros los acompañamos en la actividad complementaria crítica que es la cobranza.

El último dato es que el 50% de los directivos sostiene que la fuga de información es una de sus principales preocupaciones pero los mismos que dicen eso, son los que dicen que sus sistemas están desactualizados.

A veces la agenda del negocio no les permite poner foco en eso. Que le roben la información a una compañía es como que a nosotros nos roben la billetera, se hacen de todas nuestras tarjetas de crédito, del DNI, de nuestra licencia de conducir, es lo mismo.

Seamos conscientes de los riesgos que hay y tratemos de reducirlos, la información que hasta hace un tiempo teníamos en cualquier aplicativo o formulario hay que guardarla; porque el que les roba la información puede estar dentro de la compañía y les puede hacer fraudes o puede venir de afuera y robarle un montón de información que les va a costar muchísima plata.

Dicho todo esto, les venimos hoy a presentar una solución que desarrollamos y que está en funcionamiento desde hace un año y medio, lo que hace es la

administración, captura y procesamiento seguro de números de tarjetas de crédito; los números de tarjetas de crédito que hoy tienen guardados en sus sistemas y sus aplicativos van a ser reemplazados por un token.

Hoy en día tienen números, todos los números de tarjetas se van a reemplazar por token.

Cuando hablamos de estos temas siempre está la puja entre el comercial que quiere ver todo el número de tarjeta de crédito para poder cobrar y hacer las gestiones, el de seguridad informática dice que no puedes ver nada del número de tarjeta de crédito y está a veces el de cobranza, que dice necesito algo para conciliar. Es como un universo muy complejo.

Nuestra solución hace que esas tres personas que siempre se peleaban sean amigas de nuevo, porque nuestro token tiene una característica que hace que se amiguen todos.

El token es de 16 caracteres como un número de tarjeta de crédito para la gente comercial, y los que concilien se pueden quedar tranquilos porque pueden ver los primeros seis números del bin y los últimos cuatro de la tarjeta y lo del medio, es un algoritmo que se genera y hace un token.

Por cada número de tarjeta de crédito que entre a nuestro sistema se le va a generar un token que es unívoco por número de tarjeta de crédito. Este servicio se complementa con la parte de procesamiento y conciliación.

Ahora vamos a ver esos tres grandes procesos que abarcan el servicio y que se los voy a explicar para que entiendan cómo va el servicio de punta a punta.

La idea es que una vez que tienen este servicio implementado nunca más ingrese un número de tarjeta de crédito en sus sistemas, van a estar siempre resguardados en los ámbitos seguros de Gire.

Los tres grandes procesos que abarca nuestros servicios son tres: administración segura de un padrón de números de tarjetas de crédito, captura segura online y por último, procesamiento y conciliación.

Esos 3 grandes procesos están englobados por una llavecita que dice PCI que es Payment Card Industry y es un conjunto de mejores prácticas estipulado por las grandes procesadoras del mundo. Puedo operar en Argentina y Uruguay.

Si ustedes quieren manejar números de tarjetas de crédito de forma segura tiene que cumplir con todo esto y eso requiere una gran inversión en know-how, en infraestructura tecnológica, para pagar las auditorias anuales que te certifican que sean una empresa PCI.

El sello de seguridad que le damos desde Gire Soluciones es que somos una empresa PCI a nivel internacional y no muchas empresas en el país lo son, contratando este servicio están seguros de que Gire les va a dar la seguridad máxima a los datos de sus compañía.

Vamos a repasar cada uno de los procesos. El primero es administración segura. ¿En qué consiste esto?

Una vez que su empresa decide contratar este servicio, un equipo de especialistas de Gire hace un revelamiento y entiende todos los puntos de ingreso de números de tarjetas de crédito de su compañía.

Entonces trabajamos, desarrollamos y decimos el lunes 14 de Agosto arranca a funcionar este servicio, el viernes 11 le dice mándeme toda la base de datos de números de tarjetas de crédito de su compañía; se manda a Gire, tokenisa todos esos números de tarjetas de crédito y le devuelve los tokens. A partir de ese momento ya pueden borrar el número de tarjeta de crédito.

En una de las migraciones que hicimos de este servicio tokenisamos en 5 horas 2 millones de números de tarjetas de crédito, nos mandaron un archivo, se tokenisaron todos, se le devolvió a la empresa, pudo borrar de sus sistemas y los números los manejamos nosotros.

Nos mandan el stock de números de tarjetas de crédito, lo que hacemos es tokenisarlos todos y les devolvemos un archivo con tokens, ese es el día cero.

A partir de ahí cada vez que ingreso un número de tarjeta, le vamos a generar un token en el momento a través de esta solución que desarrollamos, es una

solución multiplataforma para capturar número de tarjetas de crédito y tokenizarlas en el punto de venta.

Hay varias, ahí hay tres nada más. Voy a explicar un par para que entiendan pero pensamos en cada momento de venta, si ustedes tienen un productor que anda vendiendo en oficinas comerciales o va a vender seguros en oficinas y lo que hace comúnmente es completar un formulario en papel te dice: ¿quieres débito automático?, sí, y te completa el número de tarjeta en el formulario y ese formulario después viaja en algún momento a la compañía.

La idea es que eso no suceda más. Para eso desarrollamos una aplicación mobile para que cuando el productor vaya a venderle a alguien y le tiene que completar ese formulario, pueda tokenizar esa tarjeta en el momento y en vez de completar el número de tarjetas de crédito completa el token. Ese token en el momento viaja a Gire y queda guardado en nuestra base.

Otro de los canales que tenemos es una aplicación Web, muchos seguros o empresas venden a través de un call center, la misma funcionalidad, el vendedor que está en el call center puede ingresar los datos en nuestra aplicación y tokenizar en el momento.

También tenemos una solución por IBR llamando por un teléfono, tenemos un web service para que puedan consumir y tokenizar directamente.

Por último también en el mundo de los seguros donde no solamente las empresas venden sino que lo hacen a través de sponsor, por ejemplo bancos que venden seguros, está la posibilidad que esos bancos cuando cierran al final del día le dicen: mira te vendí todo esto y te mando un archivo con número de tarjetas de crédito antes de que llegue a tu empresa pase por Gire y se tokeniza, de esa forma los número de tarjetas de crédito se capturan en el punto de venta y nunca más ingresa un número a sus sistemas. El circuito es: ingresan números de tarjetas de crédito, se tokeniza, devuelve el token y el token queda para la empresa.

Un dato que es importante. Quizá muchos escucharon la palabra token porque se usa muchísimo sobre todo los que entran a interbanking o lo usan en las aplicaciones mobile de los bancos.

Te genera un token de seguridad que es dinámico, dura una determinada cantidad de segundos, nuestro token es único, no cambia nunca, es fijo por cada número de tarjeta de crédito que entra, y este token no es para el tarjetahabiente, para el dueño de la tarjeta, es seguridad para su empresa, el cliente nunca se entera que le generaron un token, el que sabe es la empresa, es seguridad pura y exclusivamente para las empresas.

Y después, ¿cómo hago para cobrarle a mis clientes?, les mando a Visa los token y no podemos cobrarle. Ahí está la última pata, que es la pata de procesamiento y consolidación.

Además de este servicio de tokenización brindamos un servicio donde hacemos de facilitador en la relación entre sus empresas y todos los medios de pagos que tienen habilitados para la cobranza.

Funcionamos como un nodo de integración entre ustedes y cualquier medio de pago: efectivo, banco, lo que sea.

Ustedes se ahorran de dialogar con todos los medios de pago, Gire dialoga con todos. Presenta los débitos, las publicaciones de deuda, las recibimos todas y después hacemos la conciliación de esas transacciones y le damos la información conciliada, es un servicio de procesamiento y conciliación.

Mechado con eso se engancha la última parte que es la presentación de los débitos en las tarjetas. Ustedes no van a tener los números de tarjetas de crédito para mandárselo a Visa, Master a Amex a cualquier medio de pago, tienen los tokens.

Ustedes van a seguir generando la presentación, ahí hay un montón de facilidades que da este servicio de Gire para hacerle el servicio más fácil, más

seguro y más ágil, en vez de tener todos los diseños de todos los medios de pagos, es hacer un solo diseño y hablan directamente con Gire.

Gire va a transformar token por un número de tarjeta de crédito o destokenisar y lo manda a las procesadoras, porque las procesadoras no saben lo que es el token, tienen que mandarle el número de tarjeta.

Nosotros lo volvemos a recibir, lo volvemos a tokenisar y se lo mandamos a ustedes para que puedan imputar la cobranza con los tokens en sus sistemas. No más números de tarjetas de crédito, nosotros nos encargamos del procesamiento y después de la conciliación.

Si hay reintegros, devoluciones, contra cargos, todo eso lo hacemos nosotros que gestionamos directamente con los medios de pago.

Este servicio además de dar seguridad, le da agilidad y facilidad a la gestión de las cobranzas. Es un servicio punta a punta, desde el momento que se contrata esto no ingresa más un número de tarjeta de crédito, se pueden olvidar de ese problema y el problema es nuestro, que sabemos cómo manejar la información.

No sé si hay alguna duda, alguna consulta, si quieren hacer preguntas, sino podemos cerrar ahora.