WHITE PAPER

Un análisis de la industria del control de acceso en América Latina

Luego de una encuesta realizada por HID Global entre usuarios finales en Latinoamérica, una de las conclusiones del estudio es que las corporaciones de la región tienen enormes oportunidades para actualizar sus sistemas, incrementar sus índices de protección y agregar nuevas funciones a los mismos.

RESUMEN EJECUTIVO

Los sistemas de control de acceso ya no son simples herramientas físicas para autorizar o negar el ingreso de una persona a una edificación. Actualmente, estas soluciones integran tecnologías novedosas que, además de incorporar avanzadas tecnologías de seguridad, pueden emplearse para diferentes labores corporativas.

Pese a lo anterior, **aún existen organizaciones que no tienen dentro de sus planes cercanos modernizar sus sistemas de control de acceso, exponiéndose así a las vulnerabilidades presentes en el entorno actual.**

Por otro lado, invertir en un moderno sistema de control de acceso —físico y lógico— es una decisión importante para una empresa, por lo que lo más razonable es aprovechar al máximo el potencial de estas herramientas.

Todos estos aspectos fueron considerados en una encuesta realizada por HID Global®, en donde usuarios finales de distintos mercados verticales en Latinoamérica hablaron de la tecnología que usan para realizar la labor de control de acceso.

Estos resultados fueron considerados en el presente documento, en donde además se evidencia que en muchas organizaciones se mantienen herramientas obsoletas que no ofrecen la protección necesaria.

Al final, encontraremos que **el mercado actual ofrece alternativas de control de acceso modernas (basadas en estándares de alta seguridad)** que están al alcance de cualquier usuario, desvirtuando la idea de que este tipo de soluciones solo pueden ser costeadas por grandes organizaciones.

La información está disponible para aquellas empresas que quieran dar un paso al frente en su seguridad, siendo este un elemento que -además- incide con el rendimiento de cualquier entidad.

INTRODUCCIÓN

En la década de los 70's, una reconocida marca de automóviles lanzó un vehículo con unas características excepcionales para la época. Su confort, rendimiento y parámetros de seguridad sobresalían dentro de la industria. En 2018, dichos automóviles siguen en circulación, cumpliendo con la función básica de transportar pasajeros, pero ¿cumplen con los parámetros de seguridad que demanda el entorno actual? Con seguridad la respuesta es negativa, y por eso los fabricantes de la industria automotriz desarrollan constantemente innovaciones para que los automóviles no solo puedan movilizar personas, sino que también ofrezcan características superiores de confort y seguridad.

Algo similar ocurre en el mercado de soluciones de control de acceso físico en América Latina, en donde se observa una situación particular, toda vez que aún se utilizan herramientas que están quedando desactualizadas y ello lleva a tres situaciones puntuales: **operar con sistemas inseguros, tener soluciones obsoletas y desaprovechar las aplicaciones avanzadas de los mecanismos de control de acceso.**

Dicha situación quedó evidenciada en una encuesta realizada por HID Global® en países de América Latina en la que participaron 648 funcionarios del área de seguridad, dentro de los cuales el 29% eran asesores de seguridad, 22% ejercían el cargo de gerentes o directores de este departamento y 17% oficiaban como gerentes o directores de informática, entre otros. Es decir que el 67% del personal consultado encajan en la categoría de tomadores de decisión sobre los sistemas de control de acceso de sus respectivas corporaciones.

También vale señalar que todos los participantes fueron usuarios finales, pertenecientes a mercados verticales como construcción, servicios generales, información, educación, gobierno y entidades financieras, solo por mencionar algunos de ellos.

A continuación, se hará referencia a los tres efectos referidos previamente.

Confiando la seguridad a soluciones vulnerables

Dentro del estudio en mención, un 37.3% de los participantes aseguró que la principal tecnología de credenciales que emplean actualmente en sus organizaciones para el control de acceso físico es la proximidad en baja frecuencia de 125kHz. Infortunadamente, según expertos de HID Global, esta tecnología entró al mercado hace más de 25 años y aunque ofrece grandes ventajas en términos de longevidad, son credenciales que pueden ser fácilmente clonadas, incluso sin que el portador autorizado lo note. Por supuesto, la tarjeta clonada podría abrir cualquier puerta en la que esté configurada.

Asimismo, no proveen un mecanismo eficiente para determinar si un sistema se ha visto comprometido, lo cual genera un falso sentido de seguridad pues, dado que la credencial clonada es aparentemente legítima, cualquier persona no autorizada podría ingresar a un edificio y hacer uso de los equipos y otros servicios corporativos.

La segunda tecnología más implementada por los encuestados es la de código de barras, con un 20.4%. Este hallazgo es realmente preocupante, más si se tiene en cuenta que —en palabras de los analistas— esta es la herramienta menos segura que existe en el mercado. Pese a que es un sistema muy común en aplicaciones como bibliotecas y supermercados, no es muy funcional para el tema de la seguridad, puesto que el elemento de protección está a la vista y esto hace que pueda ser fácilmente vulnerado... Basta con tomar una foto de la credencial para poder copiar la tarjeta original, y en un mundo en el que la gran mayoría de las personas cuentan con un teléfono inteligente, con cámaras de alta resolución, esto no resulta una tarea difícil.

El tercer lugar en el listado de tecnologías para el control de acceso lo ocupó la banda magnética, con un 20.1%. Lo primero que se puede decir de esta solución es que es actualmente está siendo descartada por las entidades bancarias para darle paso a los chips, precisamente por su falta de seguridad. De acuerdo con el análisis realizado por los expertos, las tarjetas con banda magnética almacenan información sólo en una delgada cinta magnética que tiende a desgastarse con cada uso.

Además, los analistas manifiestan que no hay seguridad relacionada con esta tecnología porque los datos quedan almacenados sin encriptación.

Cabe señalar que, dentro de las respuestas recibidas, un 18.5% manifestó que las credenciales de control de ingreso de sus organizaciones utiliza actualmente la tecnología de acceso móvil, que si bien aún no está en un lugar privilegiado dentro de los funcionarios de la industria de la seguridad, ya está en la mira por sus grandes beneficios de uso y protección ante posibles intrusiones.

Apoyarse en tecnologías obsoletas expone a la empresa a que una persona no autorizada ingrese a sus instalaciones, o a que los empleados clonen sus tarjetas para suplantar a un compañero de trabajo y que aparezca como si estuviera dentro de la oficina, cuando realmente no lo está.

Incluso, en un escenario peor, un empleado puede plagiar una credencial de acceso de un compañero y acceder al sistema para robar información a nombre de su colega.

En este sentido, expertos de HID aseveran que con credenciales de proximidad —por citar un ejemplo— resulta muy sencillo copiar la información allí contenida y luego copiarla en otro plástico; esto incluso puede realizarse con el apoyo de videos tutoriales que están disponibles en YouTube.

Explorando nuevas opciones

Es claro que la función principal de las soluciones de control de acceso físico es garantizar que solo las personas avaladas ingresen a una edificación. Sin embargo, estas herramientas pueden ofrecer otro tipo de beneficios que no están siendo explorados ni aprovechados por la mayoría de los usuarios finales.

Como se determinó en el estudio de HID Global, el uso más frecuente de un sistema de autenticación (con el 75%) es el control de acceso físico. Incluso considerando esta estadística, es importante señalar que dichas soluciones pueden ser aplicadas para otras funciones, las cuales -curiosamente- fueron contempladas por los participantes de la encuesta.

Estas aplicaciones adicionales de las tarjetas de control de acceso dependerán completamente del tipo de usuario. Por ejemplo, en una unidad residencial de un nivel promedio, se esperaría que la solución de seguridad mantenga las puertas del condominio cerradas y que las barras del estacionamiento estén abajo. Pero, en un conjunto de nivel premium, estas credenciales pueden adaptarse para que controlen la piscina, el spa y las zonas comunes; todo esto es posible al vincular la credencial al software de la unidad para que pueda tener servicios integrados.

En el caso de las empresas, la tarjeta de acceso se convierte en el elemento principal de identificación de los empleados dentro de la organización, la cual sugiere unos servicios implícitos. Dicha credencial —dependiendo del software de la empresa— puede utilizarse para emitir vales de alimentos de la organización o administrar el sistema de impresión de la compañía.

Puede decirse que en lo que respecta a estos servicios adicionales, no hay un límite, sino que depende de la creatividad del personal de la corporación, toda vez que con estos dispositivos es posible —por ejemplo— controlar la privacidad de los documentos que se imprimen en la organización, verificar que el área encargada esté pagando por dicha impresión, rastrear transacciones o administrar las máquinas expendedoras.

Toda la información necesaria está incluida en la credencial, la cual encripta datos que son reconocidos por los lectores.

Uso de tecnología de vieja data que deriva en insatisfacción frente a los sistemas de control de acceso instalados

Otro elemento abordado dentro del análisis efectuado por HID Global tiene que ver con la obsolescencia de las soluciones de control de acceso. En este punto es importante señalar que la antigüedad de las herramientas en mención está relacionada con el ciclo de vida de las mismas. Por lo anterior, los usuarios finales deben tener claro cuál es el ciclo de vida de la solución que están implementando, con el fin de garantizar que la herramienta en mención durará por un mayor periodo de tiempo. Además, si una solución tiene una vulnerabilidad conocida o no cuenta con repuestos que se puedan adquirir fácilmente, es necesario que esta herramienta sea reemplazada lo antes posible.

Al respecto, se encontró que el 11% de los encuestados dispone de lectores que fueron implementados hace más de seis años.

Dentro de dicho rango de tiempo también se encuentran los software (9.4%), controladores (11.4%) y las credenciales (9.8%).

Este escenario tiene un impacto directo en la satisfacción de los usuarios finales de estas soluciones. Lo anterior quedó evidenciado en el estudio mencionado previamente, puesto que el 46.4% de los encuestados se ubicó en una posición conformista, al contar con una herramienta de control de acceso que apenas satisface los requerimientos básicos esperados.

Cabe aclarar que —en este punto— es de vital importancia que los profesionales encargados de la seguridad estén al tanto de las tecnologías que existen para el control de acceso. Si bien es cierto que las empresas no siempre tienen los recursos necesarios para actualizar dicha herramienta, sí es necesario que el personal a cargo se mantenga al tanto de las opciones nuevas del mercado.

Pese a esta situación, existen aún usuarios finales que no tienen planes de actualizar los elementos de su sistema de control de acceso. Particularmente, 23.6% de los entrevistados por HID Global aseguraron que no han contemplado la posibilidad de modernizar sus lectores, credenciales, controladores o software.

Obsolescencia en el control de acceso en América Latina

Para nadie es un secreto que la situación de seguridad en esta región es un asunto de gran preocupación para los gobiernos, las empresas y, por supuesto, los ciudadanos. Por ello, ha sido necesario buscar opciones de protección más avanzadas.

Un ejemplo de esto es el hecho que se presentó en el 2018, en la zona de la Recoleta, en la ciudad de Buenos Aires (Argentina), en donde las autoridades trabajaban en la captura de una banda de delincuentes que se dedica a clonar las llaves codificadas (con tecnología de 125 Khz, diseñada en 1990) de los edificios residenciales.

Según medios argentinos[1], en esta localidad, para finales de 2018 se habían presentado más de 50 asaltos a domicilios en aproximadamente seis meses. Y es que, según los expertos, estas llaves pueden clonarse con gran facilidad gracias a un dispositivo digital que puede adquirirse en tiendas virtuales muy reconocidas y que no toma más de cinco segundos en realizar la copia de dichas llaves, cuyo costo promedio es de 1.14USD.

En este caso puntual, la comunidad argentina ha optado por implementar unos dispositivos "anti-hacking"[2] que evitan que la puerta de una edificación se abra con una llave clonada.

Para evitar esta situación, los fabricantes como HID y su red de integradores certificados recomiendan hacer una actualización tecnológica a dispositivos de última generación, los cuales utilizan elementos criptográficos que impiden ser plagiados.

En este mismo sentido, los expertos recomiendan utilizar llaves con encriptación superior, como las ofrecidas por HID Global® que —en sus palabras— son muy difíciles de clonar.[3]

---

[1] América Noticias (2018, septiembre 06). América Noticias nos visita para saber sobre llaveros electrónicos. Recuperado de https://www.youtube.com/watch?v=PaZc9av8gRs

[2] A24 (2018, septiembre 06). ¿Llaveros electrónicos clonables?. Recuperado de https://www.youtube.com/watch?v=Mo5JFpBFxNU

[3] A24(2018, septiembre 06). Entrevista en vivo con América 24 por los llaveros electrónicos. Recuperado de https://www.youtube.com/watch?v=L1_pHAoRTLE

¿CÓMO PUEDE CAMBIARSE ESTE ENTORNO EN AMÉRICA LATINA?

Lamentablemente, el desconocimiento de los usuarios finales en América Latina ha hecho que estos sigan aferrados a tecnologías con más de 20 años de existencia, lo cual les ha generado vacíos de seguridad.

Infortunadamente, la decisión de modernizar el sistema de control de acceso depende de que el directivo que tenga en sus manos esta determinación haya detectado el problema de seguridad, puesto que será este profesional quien decida cómo enfrentarlo.

Por ejemplo, hay usuarios finales que creen que con las cámaras de videovigilancia que tienen instaladas es suficiente para detectar cualquier riesgo que tengan... Este es un pensamiento bastante alejado de la realidad.

En el entorno latinoamericano es común encontrar entornos altamente vulnerables, los cuales provienen de este comportamiento "poco consciente" que tienen los usuarios finales con respecto a sus soluciones de control de acceso.

Así, es muy común que, ante la propuesta de modernizar sus herramientas, la respuesta de los clientes sea:

- "Mi sistema de identificación aún funciona".
- "Mi herramienta tiene garantía de por vida".
- "No tengo tiempo de aprender e implementar mejores prácticas de la industria".
- "Es un proceso muy complejo el tener que cambiar una especificación en mi sistema de compras".
- "Los fabricantes solo buscan su beneficio personal".
- "No tengo presupuesto".

En este camino por protegerse, el mercado latinoamericano se ha apoyado en soluciones que, aunque en su momento fueron adecuadas, actualmente se han quedado rezagadas frente a las necesidades de seguridad que plantea el entorno actual de la región.

Dentro de este abanico de posibilidades se pueden encontrar las tarjetas de 1ª. generación, que son de baja frecuencia (125Khz), cuya creación se dio en la década de los 90's y que tienen altos riesgos de clonación.

En una escala superior de protección, aparecen las tarjetas de 2ª. generación, que salieron al mercado entre 1996 y 2002 y que, aunque incluyen un chip con memoria, están en un alto riesgo de ser plagiadas.

En el año 2011 fueron lanzadas las soluciones de 3ª. generación, que son de alta frecuencia (13.56Mhz) y que incluyen la tecnología SIO (Secure Identity Object), que es un modelo de datos que permite almacenar y transportar información de identidad en un solo objeto, que puede ser utilizada en dispositivos de control de acceso (gafetes, por ejemplo). Por supuesto que, si bien son herramientas mucho más seguras, siguen teniendo un riesgo —aunque bajo— de ser clonadas.

Surgen entonces, en 2014, las tecnologías de última generación, dentro de las cuales está el sistema Seos®. Este se convierte en una solución poderosa e innovadora para la identificación segura, especialmente para las credenciales de control de acceso.

Una de las grandes ventajas de Seos es que permite utilizar cualquier dispositivo de preferencia del usuario final para el acceso seguro a más aplicaciones, con la garantía de una total protección de la privacidad del cliente.

Otras ventajas de este sistema son:

- Flexibilidad de implementación en credenciales físicas o virtuales.
- Precios de tarjetas mucho más bajos que Prox.
- Seguridad a corto y largo plazo.
- Multi-aplicación.
- Soporta el control de acceso móvil.

A partir de 2017, y hasta la fecha, los corporativos han empezado a tomar medidas de actualización, puesto que cuentan con mayores recursos para hacerlo. Infortunadamente, el escenario para las PyMES es diferente, ya que cuentan con menor capital para hacer dichas inversiones.

Pese a que los usuarios finales ya se están percatando de la situación de riesgo en la que están, hasta el momento la inversión es muy poca, y si los proyectos tienen un impacto global (porque afecta a varios países de la región), es necesario asignar un presupuesto importante y que este sea puesto como prioridad para el corporativo.

Se espera que, a partir del año entrante, un mayor número de usuarios finales en América Latina inicien un proceso migratorio de su sistema de control de acceso.

SOLUCIONES MODERNAS: ALTERNATIVAS QUE PUEDEN CAMBIAR EL ENTORNO ACTUAL

Hablar de soluciones modernas de control de acceso es imposible sin hacer referencia a una tecnología que hace que estas novedosas herramientas sean posibles. Se trata de Seos, que está disponible tanto para credenciales físicas como digitales.

Esta tecnología está diseñada para ser altamente portátil, lo que quiere decir que puede incluirse en un gafete físico o en un dispositivo móvil, incluso en relojes inteligentes.

De acuerdo con los expertos, Seos es una plataforma que permite incrementar la seguridad y conveniencia de las soluciones de control de acceso, las cuales están evolucionando constantemente.

Sin embargo, es claro que las condiciones de seguridad planteadas por América Latina representan un reto importante para el sistema de control de acceso móvil, toda vez que el robo de celulares es una problemática que se vive a diario en la región.

Es así como, a pesar de sus grandes ventajas, surge la duda de qué sucede si el teléfono móvil de un empleado se pierde. ¿Cómo desligarlo del sistema para que quien tenga el equipo, no pueda utilizar la credencial digital allí albergada?

Al respecto, profesionales aseguran que dicho gafete virtual solo funciona si el sistema lo autoriza para acceder a un área restringida, tal como sucede con las credenciales físicas. Entonces, con respecto a la solución móvil de HID, y en los casos en los que un empleado pierde su teléfono o simplemente es despedido de la organización, el administrador del sistema retira cualquier tipo de autorización que esta persona pudiera tener.

Es claro que estas tecnologías modernas son muy positivas para las organizaciones, no solo por las prestaciones de seguridad que ofrecen, sino porque su funcionamiento no es costoso, ni complicado. Por ejemplo— para el caso de los lectores Seos- basta con hacer un ajuste muy sencillo en el número de las credenciales y el usuario estará listo para entrar en acción.

Actualización tecnológica al alcance de todos

Con todas estas especificaciones tecnológicas es factible que las Pequeñas y Medianas Empresas piensen que este tipo de soluciones modernas son exclusivas para grandes organizaciones. ¿Qué opción podría tener una compañía con pocos empleados y una operación pequeña que tiene implementada una solución de control de acceso que no es confiable (como una llave) y que quiere cambiar por una más confiable, eficiente y que por supuesto, sea segura, difícil de clonar y sin tener que pagar una gran cantidad de dinero?

La respuesta a esta necesidad son las soluciones modernas de control de acceso, algunas de las cuales no requieren una inversión cuantiosa y de las que tampoco se espera la máxima calidad posible, con lo cual es fácil superar las herramientas convencionales.

Otra preocupación que va en este mismo sentido es el Retorno de la Inversión (ROI) y las ganancias que puedan obtenerse a partir de esta implementación. Frente a este tema, los expertos de HID establecen que en aquellas soluciones que se basan estrictamente en credenciales —puntualmente en la actualización de las mismas— el ROI no puede calcularse con tanta precisión, porque es necesario determinar si se trata de un reajuste de las tarjetas o si se están introduciendo nuevos distintivos que probablemente tendrán un costo adicional.

En este caso, los precios son similares y no representa un cambio significativo porque basta con revisar los detalles de cada aplicación para ver si hay alguna diferencia. Entonces, desde la perspectiva del ROI, la variación estaría en la diferencia de costos que pueda existir entre las aplicaciones.

Ahora bien, lo que realmente podría resultar difícil de computar es lo que sucede si una persona no autorizada logra copiar la información de acceso de una credencial corporativa. En este caso, el plagiador podría entrar a donde quisiera y cuando quisiera. Imagine si esto ocurre en una empresa donde se maneje inventario o información altamente confidencial. ¿Cuánto podría costarle este impase a dicha organización? ¿Cuál es el precio de asegurarse de que nadie entrará a la edificación a atentar, por ejemplo, contra el personal? Todas estas son situaciones que pueden evitarse a través de herramientas como las credenciales móviles.

Por otro lado, manejar credenciales físicas también implica otros sobrecostos relacionados con labores como impresión y distribución de las mismas. Existen empresas que, por ejemplo, pueden llegar a invertir hasta US$75 en el envío de gafetes a los empleados que tienen en otras zonas. Al hacer las cuentas de lo que podrían ahorrarse con estas nuevas tecnologías, es fácil darse cuenta que estas herramientas modernas de control de acceso son altamente eficientes en términos financieros. ¿Qué pasa si una empresa quiere tener credenciales físicas y digitales? Esta es una opción que también es posible con este novedoso sistema.

Seguridad más allá de lo físico

Contrario a lo que muchos usuarios finales piensan, el control de acceso no se limita únicamente al ámbito físico; esto obedece a que no se toman en consideración las vulnerabilidades a las que se puede exponer una organización que no adopte las medidas necesarias y se deja de lado que la experiencia de usuario en sí ha cambiado. De hecho, las soluciones móviles han cambiado este escenario porque han puesto en evidencia las vulnerabilidades de las herramientas anteriores. Es así como la persona a cargo del área de IT tiene la enorme responsabilidad de manejar no solo los computadores de escritorio, sino aplicaciones basadas en el servidor y en la nube; esto quiere decir que debe garantizar la seguridad del acceso, el video, la guardia física y posibles intrusiones.

Por lo anterior es que los profesionales de seguridad deben considerar todas las vulnerabilidades posibles, físicas y de IT, pensando —por ejemplo— en casos en los que la credencial impresa tenga el número de usuario a la vista y que una persona inescrupulosa lo anote y, haciendo un ejercicio de deducción, logre descifrar los códigos de personas de más alto rango en dicha empresa.

De esta manera, basta con que imprima esa información en una tarjeta para que pueda no solo entrar a la edificación, sino al sistema de la organización y cometer cualquier tipo de fraude, y esto representará pérdidas económicas importantes para la compañía.

CONCLUSIONES

En el pasado, antes de la Internet, era posible contar con tecnología relativamente segura, pues no mucha gente sabía cómo vulnerar los sistemas y no existía un medio de transmisión de información eficiente como la Internet; era la época de "seguridad a través de la oscuridad". Hoy, con los diferentes medios de acceso a la información de la red y con los recursos disponibles, a un costo relativamente bajo, personas malintencionadas pueden vulnerar la seguridad física y lógica de una empresa.

Entonces, ¿por qué correr el riesgo? La información y la tecnología para hacer las empresas más seguras ya está disponible, al alcance de todos. Los riesgos son una realidad, y clonar las credenciales físicas es algo que puede realizarse fácilmente, utilizando herramientas que pueden adquirirse incluso en tiendas departamentales y grandes superficies. Entre más grande sea el peligro, mayores serán las consecuencias que el usuario final tendrá que asumir.

Finalmente, la protección no puede limitarse al ámbito de la intrusión física, sino que es necesario extenderla al espectro informático; desconocer este hecho sería como operar una compañía utilizando Windows 3.11 (el primer sistema operativo de la familia Windows, lanzado a comienzos de la década de los 90).

Obviamente la seguridad y la privacidad son muy importantes para los usuarios actuales. Por eso las organizaciones—sin importar su tamaño— deben estar al día en lo concerniente a control de acceso físico y lógico. Para ello existen alternativas como las herramientas móviles, que están disponibles incluso para aquellas empresas que consideran que no pueden costearlas y, por ende, no tienen planeada la modernización de estas soluciones.

© 2019 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

2019-04-23-hid-pacs-lam-acc-crtl-ind-lam-wp-es

PLT-04381