Cambios en los enfoques actuales:

Una mirada al papel cada vez más preponderante de la Tecnología de Información en el control de acceso físico

2018

Articulo elaborado por **HID Global** y traducido por **Luis R Castellanos**, para efectos de instrucción.

https://www.hidglobal.com/

Documento original se puede descargar en la URL:

https://www.hidglobal.com/sites/default/files/resource_files/the_rising_role_of_it_in_physical_access_control_-_final.pdf

luiscastellanos@yahoo.com
http://luiscastellanos.org
@lrcastellanos

Imagen de portada tomada de Teleskop

http://www.teleskop.es/wp-content/uploads/2018/04/shutterstock_582347923FILEminimizer.jpg

Los presupuestos y responsabilidades dinámicas requieren equipos de seguridad física y equipos de TI para evaluar los cambios fundamentales en las operaciones del día a día.

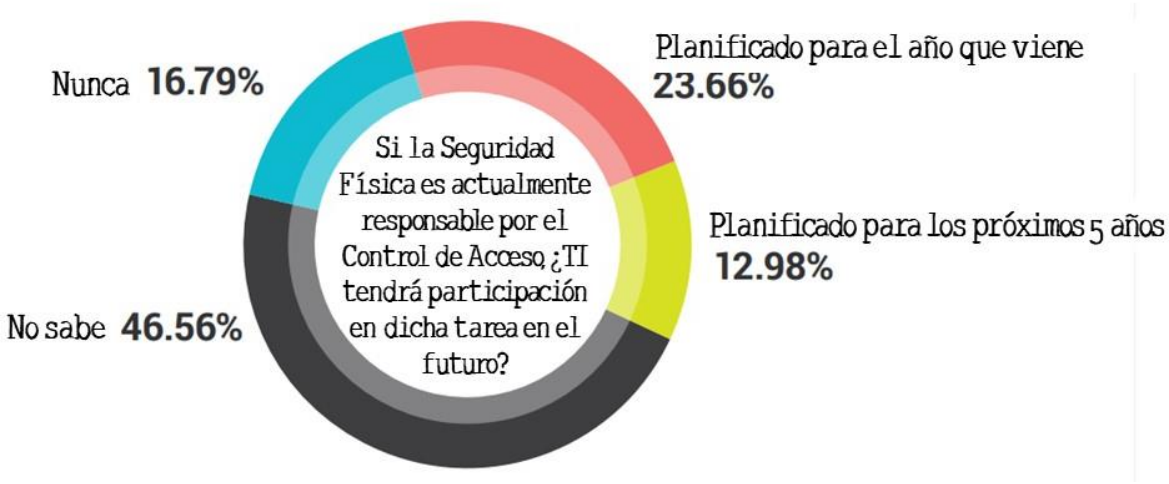
Los profesionales de seguridad física han sospechado que existe en la actualidad una tendencia hacia una mayor participación del departamento de TI en las actividades de control de acceso físico, y las investigaciones recientes han demostrado que esto es cierto. Una encuesta realizada por el Grupo 05[1] a más de 1.500 gerentes, directores y personal de TI, así como también a Directores de Información y Directores de Tecnología, encontró que los departamentos de TI ahora están más involucrados que nunca en las decisiones de control de acceso físico de una organización y en su implementación[2].

Los departamentos de TI ahora están más involucrados que nunca en las decisiones de control de acceso físico de una organización y en su implementación.

Según la encuesta, más de la mitad (55%) de los encuestados informaron que TI era el principal responsable o compartió la responsabilidad en el control de acceso dentro de su organización. Como resultado, los líderes de TI son encargados de encabezar no solo la protección de la red de su empresa e iniciativas de seguridad cibernética, sino también son encargados de aquellas tareas establecidas por el departamento de Seguridad Física para proteger a empleados, visitantes y activos de las amenazas internas y externas. Del mismo modo, el estudio mostró que el

[1] https://the05group.com/Home.aspx
[2] Nota del traductor: Metodología empleada se presenta al final de este documento.

departamento de TI jugará cada vez más un papel más preponderante en la seguridad física para influir sobre las decisiones de tecnología (76%) a través de la integración del control de acceso dentro del ecosistema (72%), al implementar tecnología para el control de acceso (59%), y a través de la gestión de sistemas de control de acceso (39%).



Junto con la responsabilidad adicional de ayudar a implementar proyectos con soluciones de seguridad basadas en TI, los líderes de TI también son cada vez más responsables de las decisiones de presupuesto para la seguridad. Según la encuesta, más del 85% de los encuestados informó que TI estaba involucrada en decisiones acerca de las inversiones en tecnología para el control de acceso físico.

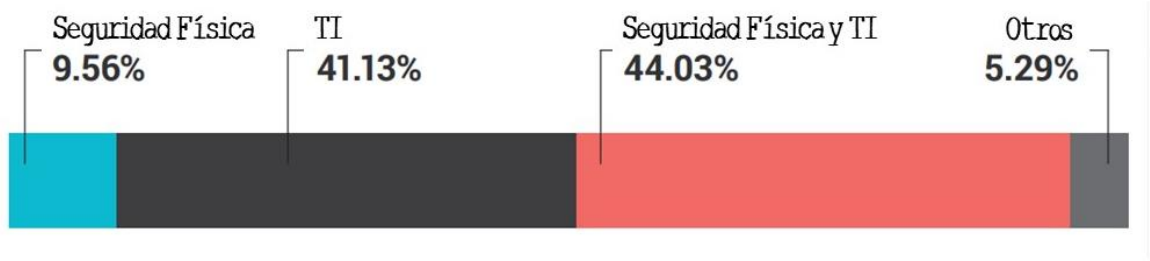
"Los números hablan de una tendencia que hemos visto en los últimos años acerca de cómo las soluciones de control de acceso y las soluciones de seguridad física pasan de un enfoque predominantemente aislado[3] a un método de gestión más colaborativo", dijo Luc Merredew, Director de Mercadeo de Productos, en HID Global.

[3] Nota del Traductor: en compartimientos estancos

"En este entorno organizativo es frecuente hacer preguntas acerca de la conectividad, alojamiento en la nube vs hospedaje *in situ*, e inversión de capital vs gastos operativos".

El propósito de la encuesta fue obtener información sobre la relación entre los departamentos de seguridad física y de TI de las organizaciones, cómo trabajan juntos y cómo se hacen las inversiones en nuevas tecnologías. En este documento, se exploran estos resultados y cómo se pueden aplicar en el mundo cada vez más colaborativo de las organizaciones de hoy en día.

¿Qué departamento decide principalmente acerca de las inversiones en control de acceso físico?



Responsabilidad del control de acceso físico cambiando rápidamente a TI

Mientras que el 67% de los encuestados informó tener una persona, departamento o equipo de seguridad física dedicado al control de acceso, la mayoría de los encuestados (55%) informaron que TI era al menos parcialmente responsable de control de acceso físico dentro de la organización. De hecho, el 26% informó que TI era principalmente responsable, y el 29% dijo que TI y los departamentos de seguridad física compartían la responsabilidad. Ello significa que desde que TI y seguridad física empezaron a compartir responsabilidades, también están

comenzando a compartir decisiones de compra y recursos, incluyendo presupuestos.

De los encuestados que respondieron que TI todavía no participa en el control de acceso físico, el 36% informó que TI desempeñará un papel importante el año que viene o dentro de los próximos cinco años. Esto indica un cambio fundamental en cómo las organizaciones gestionan la seguridad física.

“Este resultado muestra el crecimiento de la colaboración entre los departamentos de seguridad física y TI, lo que requiere mejores relaciones entre las dos entidades ", dijo Merredew. "Este es un cambio bien significativo en la forma en que la seguridad física ha operado históricamente – como un departamento que es capaz de tomar decisiones unilateralmente. La colaboración ya no es una recomendación; es un requisito para la seguridad organizacional".

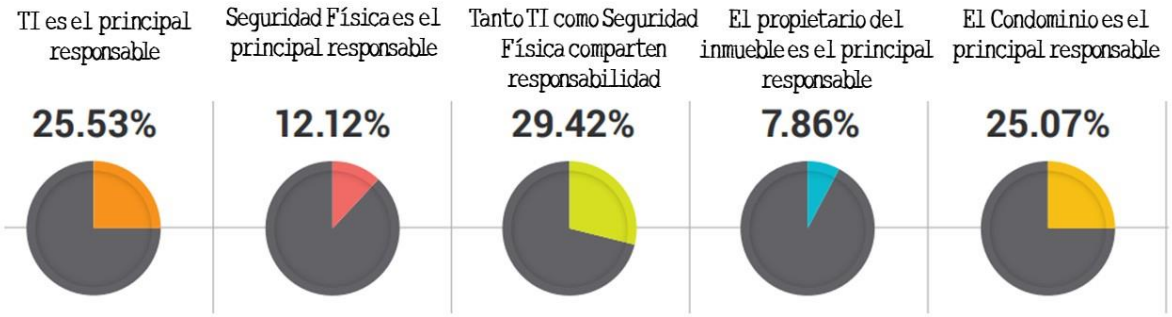
Yendo más lejos, cuando los resultados se desglosan de acuerdo al tamaño de la empresa, en las empresas más grandes (más de 1.000 empleados) es más probable que tanto TI como Seguridad física compartan la responsabilidad del control de acceso físico (36%). Las empresas más pequeñas informan que TI tienen un papel aún mayor en el control de acceso físico, con el 37% de los encuestados informando que TI tiene la responsabilidad exclusiva vs el 14% de las empresas con más de 1.000 empleados.

A medida que este cambio fundamental se produce en todas las organizaciones, muchos líderes tienen la tarea de construir o fortalecer las relaciones entre departamentos. Esto significa incorporar las mejores prácticas para la comunicación, así como establecer un énfasis en la influencia de crear un enfoque holístico de seguridad para la toma de

decisiones. En este enfoque, el énfasis está en toda la amplitud de la solución de seguridad, no solo el potencial del sistema de control de acceso para ser el eslabón más débil en una sofisticada estrategia de seguridad de red.

Según la encuesta, el 76% de los encuestados dijo que TI tendrá influencia en las decisiones tecnológicas como resultado de la colaboración entre los dos departamentos; mientras que el 72% dijo que TI desempeñará un papel en la integración del control de acceso en el ecosistema general de la organización. Cerca del 60% dijo que TI será responsable de la implementación de la tecnología para el control de acceso en toda la empresa, mientras que el 39% dijo que TI deberá administrar el sistema de control de acceso implementado.

¿Quién es el principal responsable del control de acceso físico en su organización?

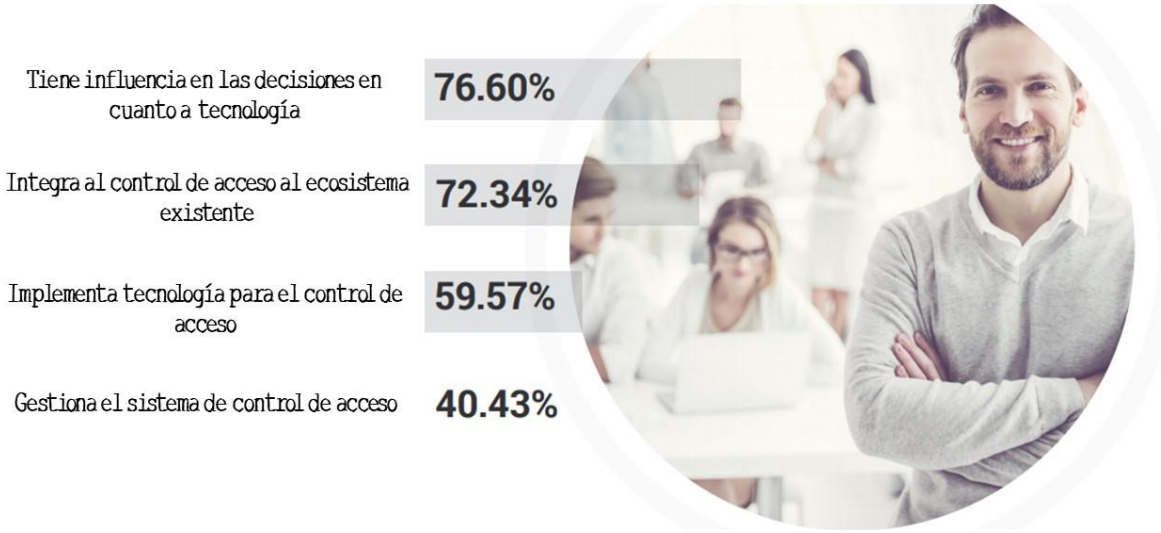


Si bien esto parece ser un fenómeno relativamente nuevo, de quienes informaron que TI y seguridad física compartieron responsabilidades, el 34% dijo que siempre ha sido así, mientras que el 39% dijo que el cambio ocurrió en los últimos cinco años. Para los que informaron que la

responsabilidad principal es de TI, el 29% informó que este cambio también tuvo lugar en los últimos cinco años. Muchas de estas organizaciones han aprendido a comprender mejor los desafíos que enfrenta cada departamento con respecto a la seguridad – ya sea proteger a las personas y a los activos críticos, o proteger la información que se transmite dentro de una organización – los cuales son importantes para la organización en general.

¿Qué papel jugará la TI en la seguridad física?

Seleccione todas las que correspondan



La investigación muestra que TI absorbe los presupuestos para la seguridad física

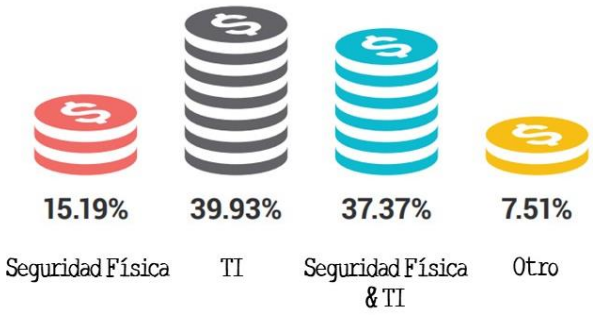
En ninguna parte es este cambio tan crítico como en el proceso de establecer presupuestos y asignar dinero para inversiones de capital en infraestructura de TI y de seguridad física. A medida que el rol de TI se expande, también la parte del presupuesto que controla este departamento,

lo que hace necesaria una comunicación abierta acerca de las necesidades de seguridad de una organización.

Casi el 44% de los participantes informó que tanto TI como seguridad física comparten las decisiones de inversión relacionadas con el control de acceso físico, mientras que el 41% informó que TI es el principal tomador de decisiones sobre estas inversiones.

De dónde proviene el dinero también está en línea con este razonamiento, con un 40% que informa que las inversiones en control de acceso provienen del presupuesto del departamento de TI, mientras que otro 37% dijo que provienen tanto de TI como de fondos correspondientes a seguridad física.

¿De qué departamento provienen las inversiones en los sistemas de control de acceso?



Este cambio es lógico, ya que los sistemas de control de acceso físico se involucran cada vez más con redes más grandes y estrategias de ciberseguridad. Con esta creciente interdependencia viene el marco para establecer dispositivos de control de acceso físico a la par de otras plataformas de hardware y software conectadas. Los sistemas de control de acceso antiguos que no otorgan una importancia superior a los protocolos de seguridad más reciente deben reemplazarse de inmediato para proteger

la seguridad general de una organización. “Los sistemas de control de acceso físico no pueden ser el eslabón más débil en la seguridad de la organización en general. Sin un enfoque adecuado centrado en la TI, se arriesgan a serlo", dijo Merredew. "Los resultados de esta encuesta son claros que a lo largo de los escenarios en general, las organizaciones de hoy deben tratar a la seguridad física con el mismo enfoque y diligencia ejercidos en las redes informáticas. La buena noticia es que muchas organizaciones lo reconocen y está evolucionando para satisfacer esta necesidad ".

Sin embargo, los niveles de comodidad del departamento de TI pueden ser un problema cuando se les asigna la tarea de tomar decisiones. Solo el 27% de los encuestados afirmó estar "muy cómodo" con la toma de decisiones con respecto a los sistemas de control de acceso físico, mientras que el 38% dijo sentirse "cómodo" con la toma de estas decisiones. Esto parece indicar que, si bien las decisiones están cambiando, todavía hay trabajo por hacer para educar a estas personas sobre los méritos de los diversos sistemas y soluciones en el mercado. Esto demuestra una oportunidad para que los equipos de seguridad física colaboren y muestren su experiencia a los líderes de TI cuando se toman las decisiones de compra y se implementen las soluciones.

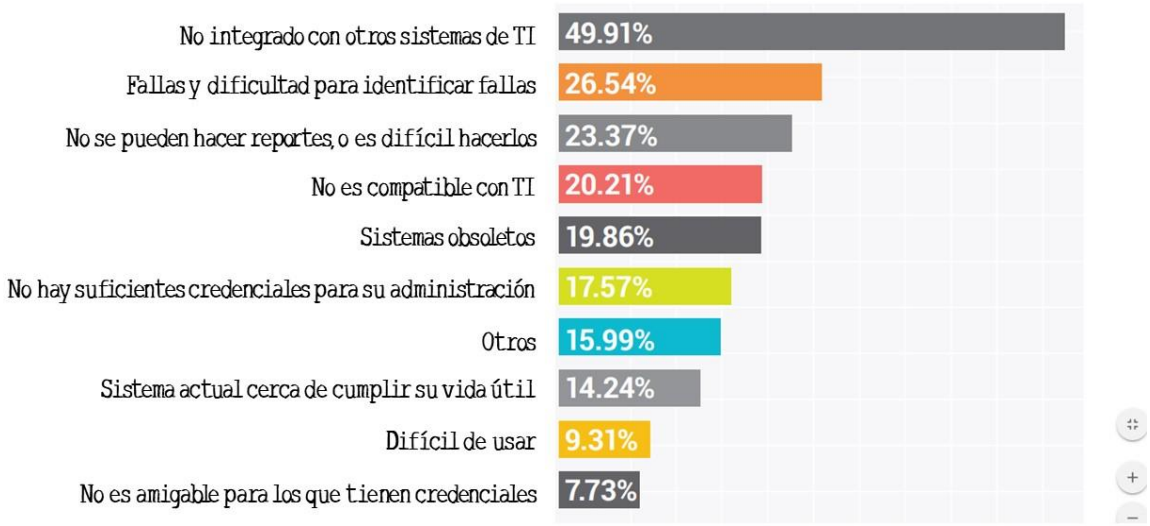
En muchas organizaciones, las inversiones en cámaras y sistemas de tarjetas se consideran que cubrirían sus necesidades por muchos años. Sin embargo, a medida que la tecnología evoluciona y las vulnerabilidades se revelan públicamente, se vuelve imperativo que los equipos de seguridad física se actualicen en un ciclo equivalente al de la TI. Como tal, los sistemas de control de acceso físico deben actualizarse continuamente a medida que las necesidades cambian y las amenazas evolucionan.

Abordar los puntos débiles de los sistemas de control de acceso de hoy

En general, los encuestados tanto en empresas grandes (> 1.000) como en empresas pequeñas (<1.000 empleados) reportaron puntos débiles similares relacionados con sus soluciones de control de acceso actuales, con un 50% reportando que la falta de integración con los sistemas de TI encabezó su lista. Otro 26% informó que sus soluciones de control de acceso son difíciles para hacerle mantenimiento o son propensas a fallas; el 23% dijo que reportar es difícil o no se puede hacer; el 20% informó que su sistema está desactualizado; y otro 20% dijo que los sistemas no son compatibles con la tecnología existente en la organización.

¿Qué puntos débiles existen en sus sistemas actuales?

Seleccione todos los que apliquen



Es importante tener en cuenta que a medida que se produce este cambio, la investigación muestra que todavía hay desafíos que enfrenta TI al gestionar

sistemas de control de acceso físico. Casi el 39% de los encuestados afirman que están "cómodos" con las características individuales en su sistema de control de acceso, mientras que solo el 16% están "muy cómodos". Del mismo modo, solo el 34% está "cómodo" solucionando problemas o fallas, mientras que solo el 17% está "muy cómodo" con la tarea. Esto deja espacio a líderes de seguridad física, así como a proveedores e integradores, para aumentar el nivel de capacitación y educación ofrecida cuando se implementa una nueva solución de control de acceso dentro de una organización.

Independientemente del tamaño, los resultados muestran la importancia de desarrollar una relación más sólida y compartir iniciativas de capacitación entre los dos departamentos para racionalizar y comprender mejor la sinergia entre TI y control de acceso físico. TI también debe hacer el esfuerzo de familiarizarse y sentirse más cómodo con los sistemas de control de acceso físico para servir mejor los objetivos de la organización.

La tecnología emergente y las características que hacen que el control de acceso sea coherente con la TI

Un factor crítico para el éxito de una solución moderna de control de acceso físico es la capacidad de prevenir que individuos no autorizados accedan al hardware relacionado con la red, y al mismo tiempo presentan a los directores de seguridad con la capacidad de agregar fácilmente opciones para la tecnología emergente, como dispositivos móviles o biométricos. Más del 68% de los encuestados estuvieron de acuerdo, diciendo que uno de los principales requisitos de características en una nueva solución es la capacidad de agregar o admitir nuevas tecnologías en el futuro.

¿Cuál de las siguientes funciones necesitaría en un nuevo sistema de control de acceso físico?

Seleccione todas las que correspondan

La facilidad de uso es otro componente crítico, con el 71% de los encuestados nombrando esto como un requisito de un nuevo sistema de control de acceso físico. La facilidad de uso ahorra tiempo, esfuerzo y recursos en todos los departamentos, lo que permite un mayor enfoque en proyectos de mayor prioridad. Otros requisitos enumerados por los encuestados incluyeron: integración con plataformas de seguridad existentes (54%); soporte para características más avanzadas de seguridad (53%); tecnología abierta para una fácil integración (52%); y garantía de alta calidad y servicios de soporte extendido (46%).

Estas respuestas apoyan el argumento de que los líderes de TI prefieren una tecnología que se integre más fácilmente con las soluciones existentes y futuras. Esto también es una indicación de la necesidad de que las organizaciones puedan escalar su tecnología de la manera más apropiada; cuanto más antigua sea la tecnología, menos probabilidades hay de poder integrarse con las soluciones de seguridad existentes y alinearse con las

necesidades de red. Las organizaciones de hoy deben invertir en soluciones que cumplan con los requisitos de los líderes de TI y seguridad física.

Más del 58% de los encuestados mencionaron el acceso móvil como una de las funciones que más requieren en un nuevo sistema de control de acceso físico, lo que indica un cambio hacia la movilidad y flexibilidad para las soluciones entrantes. El "acceso móvil" incluye el uso de teléfonos inteligentes, tabletas y/o dispositivos vestibles para el control de acceso. Esto también indica una creciente aceptación de las credenciales móviles para el control de acceso, lo que permite a las organizaciones tener más flexibilidad para decidir qué factores de forma son mejores para sus necesidades únicas de control de acceso.

Conclusión

Las organizaciones de hoy deben ser internamente más colaborativas que nunca, especialmente en el ámbito de seguridad. Las decisiones y responsabilidades en cuanto al control de acceso físico están viendo un cambio fundamental hacia el departamento de TI, lo que requiere que ambos departamentos trabajen juntos para lograr una verdadera seguridad en toda la empresa. Está claro que el cambio en cuanto a la colaboración entre TI y seguridad física está dando como resultado un enfoque más unificado de la seguridad, lo que resulta en una mayor frente unido para combatir los problemas que se presenten.

Como resultado, los profesionales de TI deben confiar en los equipos de seguridad física por su experiencia y soporte cuando se implementa nueva tecnología, mientras que los equipos de seguridad física deben hacer lo mismo con respecto a decisiones centradas en la TI. Además, es fundamental que los equipos de seguridad física demuestren su valor a la política general

de seguridad de la organización. Al centrarse en la colaboración entre los dos departamentos, los equipos de seguridad física pueden mantener el control sobre las decisiones en sus presupuestos e inversiones, así como la capacidad de priorizar la seguridad de la organización.

Al igual que las amenazas que enfrentan las organizaciones de hoy, las necesidades de estas organizaciones están constantemente cambiando, llevando a las empresas de todos los tamaños a darse cuenta que las soluciones de control de acceso físico deben estar alineadas con los estándares que el departamento de TI ha establecido para proteger los activos y las personas. A medida que se introduce una nueva tecnología en el ecosistema de una organización, es imperativo que la colaboración cercana entre seguridad física y TI continúe creciendo y prosperando para cumplir y superar las expectativas de seguridad y protección trazadas.

Metodología empleada

El Grupo 05 encuestó a 1.576 personas, que representan a más de una docena de industrias diferentes, incluyendo Educación (19%), Información (16%), Gobierno (11%), Manufactura (8%), Servicios de salud (8%) y Seguridad, Servicios profesionales y de negocios (8%). De los encuestados, el 35% eran gerentes de TI, el 26% eran directores de TI, el 13% era personal de TI, el 8% eran CIO/CTO y el 3% eran vicepresidentes de Tecnología.

El desglose del tamaño del negocio es el siguiente: el 24% tiene menos de 100 empleados, el 22% tiene 101-500 empleados, el 11% tiene 501-1.000 empleados, el 17% tiene 1.001-5.000, el 6% tiene 5.001-9.999 y el 6% tiene 10.000-24.999 empleados.

HID

Con sede principal en Austin, Texas, HID Global tiene más de 3.000 empleados en todo el mundo y cuenta con oficinas internacionales que brindan soporte a más de 100 países. HID Global® es una marca del Grupo ASSA ABLOY.

Luis R Castellanos

Experto en eLearning, Tecnologia y Seguridad.
Director Académico en Total Risk, empresa de larga trayectoria en Seguridad, y coordinador del Diplomado en Seguridad. Gerente de eLearning en Nebusis Cloud Services.