Inversión en seguridad empresarial crece en pandemia

El sector empresarial invierte cada vez más en temas relacionados con la seguridad. El aumento se ha dado sobre todo durante esta pandemia, no solo para reducir los riesgos de robos, sabotajes y defraudaciones, etc, sino para la detección de delitos cibernéticos.

Security & Safety

El mercado de seguridad en el Perú mueve en promedio US$ 400 millones anuales. Así, existe una tendencia marcada sobre el perfil security & safety (riesgos asociados a robos y delitos cometidos por terceros, así como incendios o peligros como la pandemia), la cual alcanza en promedio US$ 250 millones en el Perú, y que ha crecido unos US$ 100 millones por la pandemia.

“Ahora casi el 84% del mercado requiere de este tipo de servicio, más enfocado a la personalización de la seguridad”, anota el gerente de Seguridad del Grupo EULEN Perú, Santiago Barranzuela.

▶ Avances del plan nacional de infraestructura para la competitividad

▶ Infracciones y sanciones laborales vigentes

 Venta de casas alcanza cifras pre pandemia

Además, explica que las empresas también necesitan la detección de potenciales riesgos sobre todo en torno a la gestión SSOMA (seguridad, salud ocupacional y medio ambiente), es decir, salud en el trabajo, detección de zonas inseguras y protocolos de acceso para combatir la **COVID-19**.

Cabe resaltar que, según el Instituto Nacional de Estadística e Informática (INEI), la tasa de percepción de inseguridad ciudadana al 2020 llegó hasta el 90%.

Incluso, de acuerdo al Banco Interamericano de Desarrollo (BID), el costo de la delincuencia en el Perú equivale al 2,77% del PBI, es decir, más de US$ 10.000 millones, señala el presidente de la Comisión de Seguridad Ciudadana y Empresarial de la Cámara de Comercio de Lima (CCL), Vicente Romero.

Asimismo, añade que en la región el gasto en seguridad se descompone en 42% en gasto público (sobre todo en servicios policiales), 37% en gastos privados y 21% en los costos sociales de la delincuencia.

“El principal riesgo (para las empresas) es la distribución de productos o mercaderías. Se han reportado múltiples asaltos en diferentes partes del país a empresas de alimentos, bienes, servicios etc. Por tanto, se deben tomar modelos donde el Estado y el sector privado trabajen de manera conjunta para combatir la delincuencia y la inseguridad ciudadana”, recalca

Romero.

Mayor inversión

Santiago Barranzuela, del Grupo EULEN Perú, añade que el presupuesto que se suele destinar para seguridad depende mucho del perfil de la empresa, la cantidad de colaboradores y los equipos que la compañía requiera.

Por ello, advierte que, en promedio, una compañía puede llegar a invertir S/ 90.000 al año por una posición 24×7 (dos agentes más un descansero, incluyendo accesorios).

“En el sector alimentario el porcentaje destinado a seguridad del total puede llegar al 10%, sobre todo por los protocolos de inocuidad. En el sector educación puede alcanzar el 8% o 9%. Y en promedio, en todas las industrias gira en torno al 13% o 14%. Lo destinado a ciberseguridad es adicional, pues esto depende mucho de lo que el cliente requiera resguardar”, refiere Barranzuela.

Priorizando ciberseguridad

Sobre ciberseguridad, el gerente general de ESET Perú, Jorge Zeballos, destaca que la mayor inversión en el rubro ha sido para hardware, donde muchas empresas han privilegiado la adquisición de equipos portátiles para sus empleados con la

intención de controlarlos mejor.

“También han invertido en sistemas de autenticación (claves de una sola vez), sistemas de prevención de fuga de datos y medición de uso/ acceso a los sistemas, y licenciamiento de software de seguridad para las computadoras destinadas al home office. Estas ‘nuevas’ inversiones han requerido que la seguridad de la información y acceso a sistemas claves sea incrementado en un promedio de 30%”, indica.

Riesgos informáticos

La mayoría de los riesgos cibernéticos para las empresas están ligados a casos de phishing, que se distribuyen a través del correo electrónico, y ransomware, ataque a través del cual los ciberdelincuentes secuestran información de la empresa para luego pedir un rescate en efectivo o Bitcoins.

Jorge Zeballos, de ESET Perú, destaca que, en el 2020, en el Perú se dio el 20% de los ataques de ransomware de toda la región. Según la herramienta ESET Virus Radar, nuestro país registró el mayor nivel de infección con 11,69%.

“Estos resultados nos alertan sobre la situación vulnerable en que vivimos y nos motivan a concientizar a las empresas y usuarios sobre la importancia de la ciberseguridad y el uso de las herramientas de prevención”, asevera Zeballos.

Cabe señalar que, durante los meses de cuarentena, de mayo a julio 2020, se observó un incremento en la actividad de phishing, con casi 2.500 detecciones diarias. En los primeros meses del año los registros oscilaban en alrededor de 2.000.

“En un ataque ransomware, el costo es difícil de calcular, porque esta en función de cuanto daño podría producir la publicación de dicha información secuestrada. Ello implica no solo las multas por infringir las normas de protección de datos personales, que pueden ser sumas de hasta S/ 540.000, sino hasta la pérdida de reputación y cierre de la compañía”, detalla Zeballos.

Según el reciente ESET Security Report (2020), los principales controles de seguridad implementados en las empresas son las soluciones antimalware (86%), firewalls (75%), soluciones de respaldo de información (68%), y el uso de soluciones de doble factor de autenticación (22%).

Por ello, Zeballos asegura que las empresas también deberían implementar soluciones de seguridad en smartphones o tablets, sobre todo porque en el teletrabajo estos son muy utilizados para actividades laborales y personales, y pueden ser la puerta de entrada a la información sensible de la empresa.

Video vigilancia

Uno de los requerimientos más frecuentes, a causa de la transformación digital, son los sistemas y aplicativos

enfocados al monitoreo de puestos, colocación de agentes y seguimiento de las operaciones durante todo el día mediante video vigilancia.

Por ello, compañías del sector han migrado a las plataformas virtuales para conocer en tiempo real el estado de sus agentes de vigilancia privados (AVP).

En esa línea, el director general de la empresa de vigilancia GOES Perú, Miguel Castro, subraya que hay dos tendencias muy marcadas en el sector.

“Anteriormente las empresas encargadas de seguridad instalaban y vendían los equipos, hoy una persona natural puede comprar cámaras de video e instalarlas en su casa o empresa. Esto no es efectivo si no está conectado a una central de monitoreo. Este servicio ha crecido, especialmente en condominios y empresas”, apunta.

Se puede empezar con una inversión de US$ 2.000 hasta US$ 100.000. Este último incluye un centro de control in house, especial para empresas mineras, o agroindustriales, por ejemplo.

“Muchas empresas adquieren los equipos por renting o leasing que hace la propia proveedora, la cual hace mantenimiento del sistema. Por eso, al final es un negocio eficiente y rentable para la empresa”, dice Castro y adelanta que en el 2022 se incorporarán al mercado las cámaras de reconocimiento facial, pues ya no son muy costosas.