Año 6 Nº 36 Septiembre 2022

Revista SEGURIDAD .Online
& DEFENSA
LA PRINCIPAL PLATAFORMA DE INFORMACIÓN DE SEGURIDAD EN LATINOAMÉRICA

CASO DE ESTUDIO
Masacres en colegios
¿Cómo abordar este riesgo potencial?

HARP
Protección efectiva contra grabaciones clandestinas

DEEPFAKE
Una amenaza creciente

CIBERSEGURIDAD
CHILE BAJO ATAQUE

REDSEG

RED LATINOAMERICANA DE EMPRESAS Y PROFESIONALES EN SEGURIDAD TECNOLÓGICA

REGÍSTRESE, ES GRATIS.

www.redseg.org

- Patrocinador
- Corporativo
- Empresa
- Academia
- Profesional
- Colaborador

SOLICITE SU MEMBRESÍA OFICIAL

planes.redseg.org

PATROCINANTES OFICIALES

Revista SEGURIDAD

DIGITALX C.A
INNOVACIÓN AL LÍMITE
RIF: J40985476-0

GRUPO RAM´S
Seguridad Integral

Asistencia Telefónica: +58 412 4980135 info@redseg.org

EDITORIAL

Nº36 Septiembre 2022

La ciberseguridad vuelve a retomar su protagonismo a raíz de los últimos hackeos que afectaron tanto, al Estado Mayor Conjunto, como al Poder Judicial.

Este tipo de situaciones nos debe llevar a replantearnos la manera que estamos abordando la temática de la ciberseguridad, independientemente que se trate de una institución, una corporación o incluso un individuo.

Los ciberataques constituyen un problema global, por lo anterior no podríamos pensar que Chile podría ser la excepción.

Como dato ilustrativo podemos señalar el segmento de la telefonía celular, en Chile en agosto de 2022 ya contaba con más de 33 millones de dispositivos, sin embargo, solo un ínfimo porcentaje cuenta con un sistema adecuado de antivirus. En términos simples un hacker puede acceder a nuestros contactos, nuestras claves cuentas bancarias, activar nuestras cámaras, neutralizar alarmas y sistema de domótica asociados a nuestros celulares, neutralizar sistemas de rastreo GPS entre otros.

La seguridad constituye la principal prioridad nacional, donde encerronas, portonazos y asaltos concentran nuestra atención, sin embargo, la evolución del delito siempre buscará aquellas instancias que generen mayores beneficios, con el menor riesgo asociado; por lo anterior frente a la escalada delincuencial debemos considerar todos los flancos, pues en definitiva un alto porcentaje de los delitos busca generar ganancia a costa del patrimonio de la víctima.

Robert Gutter Boim
Director

CONTENIDO

Editorial 1

Ciberseguridad 3
¿Estramos bajo ataque?

Leyendas Urbanas de Ciberseguridad 5

Proteja hoy su dispositivo celular 8

CIBERSEG 9
Un nuevo referente para el área de la ciberseguridad

Actualizar nuestra legislación 10
Una necesidad frente al escenario actual

Principios prácticos 13
para reclutar, enseñar y liderar escoltas

REDSEG 17
Materializa su llegada a Chile

Caso de estudio y recomendaciones 18
Masacres en escuelas en Estados Unidos

HARP 20
Protección efectiva contra grabaciones clandestinas

Pantallas interactivas 28
Una nueva forma de informarse y aprender

Tecnologías biométricas de ZKTeco 33
Permiten reconocimientos seguros, efectivos y rápidos

Deepfake 38
Una amenaza creciente

Policiamiento predictivo 40
En la era de los algotitmos y la justicia criminal inteligente

Eventos 44

Informaciones
www.revistaseguridad.cl
E mail: info@revistaseguridad.cl - revseguridad@gmail.com

AÑO 6 N° 36 Edición SEPTIEMBRE 2022

Prohibida toda reproducción total o parcial de esta revista.

Revista Seguridad Online es una edición de Producciones Gótica Ltda.

Las opiniones incorporadas en esta revistas son de exclusiva responsabilidad de quienes las emiten y no representan necesariamente el pensamiento del editor.

Revista Seguridad Online

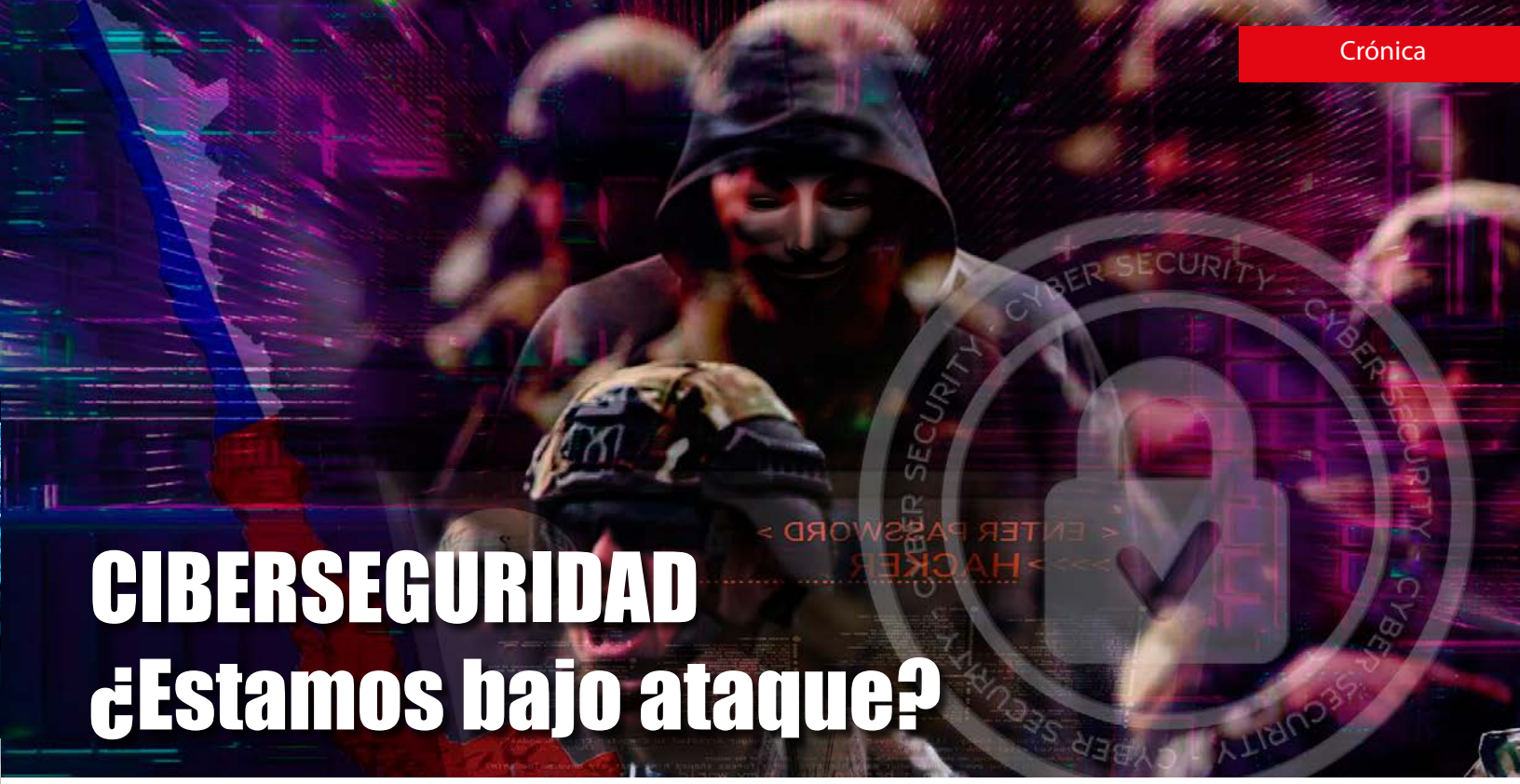
Director: **Robert Gutter Boim**
CEO: **Cristián Fonseca**

Fotografía General: Archivo

Portada : Demidov Armor en Unsplash

Dirección Creativa: **Gótica Ltda**

Ventas de Publicidad: **+56 9 98246696**



CIBERSEGURIDAD ¿Estamos bajo ataque?

En diversas oportunidades, tanto empresas como bancos han sido víctimas de hackeos. Si bien se desconoce la real dimensión de los daños causados, los recientes hackeos sufridos por el Estado Mayor Conjunto (EMCO) de la Defensa de Chile y por el Poder Judicial han evidenciado una falta de prolijidad en materia de Ciberseguridad. En virtud de nuestro rol de medio de difusión en materia de seguridad, quisimos abordar este importante tema, para lo cual conversamos con Félix Miranda, del departamento de Ciberseguridad de REDSEG, entidad internacional de reconocida trayectoria y prestigio en el ámbito de la ciberseguridad.

¿Qué nos puede comentar con respecto a los niveles de incremento en los ataques parte de hackers?

Pueden deberse a causas tan diversas como un parcheado mal ejecutado (o incluso, desestimado o postergado), o que la actualidad política y socioeconómica haya causado un olvido en materia de Ciberseguridad (tanto a nivel de prioridades estratégicas como de destinación de recursos), e incluso con fines de intereses y desestabilización política.

Es probable que otras instituciones, también de otros sectores, se vean afectados en la reciente oleada, o que eventualmente las técnicas y vulnerabilidades empleadas puedan replicarse, y por un efecto de entusiasmo puedan surgir otros ciberatacantes o candidatos a serlo.

¿Con qué velocidad aparecen nuevas amenazas en materia de ciberseguridad?

Me atrevería a decir que son de carácter diario, o al menos esta es la frecuencia tienen los ciberatacantes y amenazas ya existentes, para desarrollar más o robustecer sus técnicas y recursos; sin embargo, el impacto que una nueva amenaza pueda tener, variará según lo que pueda explotar, lo desastrosa que resulte, lo sigilosa que sea, o mas importante, lo indetenible que resulte.

Al hablar de protección en materia de ciberseguridad se suele mencionar el término "capas". En términos sencillos, ¿cómo podríamos definir qué es lo que es una capa?

Podemos decir que una capa es cada control de seguridad que se implemente en materia de cioberseguridad. No debemos confiarnos sólo en una capa, sino en proteger tanto como sea posible y factible, para buscar defender (o al menos complicar) el acceso a la información, a los activos, e inclusive a las personas.

Para ser mas específico, suelen asociarse como capas a los factores humanos, perimetrales, de red, de aplicación y de datos. Recomiendo ver el modelo de Defensa en profundidad (Defense in deep), en donde se compara con las múltiples zonas y defensas de un castillo, pero recomiendo aún más el de Confianza Cero (Zero Thrust), que viene a combatir la noción de que desconfiemos sólo de lo que está afuera, cuando también debemos verificar lo interno (tanto en red como a personas).

¿Cuáles son los niveles de protección en términos de capas aconsejados actualmente para instituciones gubernamentales o armadas?

No recomendaría un mínimo, sino considerar tantas como sean posibles, de un modo inteligente que no cause inoperatividad. Por mencionar algunas:

- Contar con un Sistema de Gestión de Seguridad de la Información (SGSI) adecuado.
- Contar con un enfoque de gestión de riesgos.
- Entender que la efectividad de ambos debe ser verificada periódicamente.
- Adaptar el máximo rigor en sus medidas de seguridad técnicas y administrativas.
- Contemplar a las ciberguerras como otro escenario posible.
- Buscar actores referentes y asesorías que puedan encaminarlas de la mejor manera posible.
- Conocer qué adversarios podrían atacarle y saber cómo defenderse de sus técnicas usuales.

Como organización dedicada al tema de la ciberseguridad, ¿poseen alguna teoría respecto de la modalidad utilizada por el grupo Guacamaya para, materializar este hackeo a distintas instituciones a nivel continental?

Guacamaya publicó un video en donde muestra cómo realizaron su ataque al EMCO, a Equiborax y a la Fiscalía de Colombia:

En resumen, luego de escanear y encontrar una vulnerabilidad de Microsoft Exchange, procedieron a explotarla, descargando la cantidad de

correos electrónicos que ya sabemos.

¿Y en cuanto al Poder Judicial?

En cuanto a los hechos, primero se afectaron alrededor de 150 equipos, y se presentó al público que habían caído por tener tanto Windows 7 (sistema operativo obsoleto) como antivirus McAfee (pasándole, con o sin razón, parte de la responsabilidad); sin embargo, al día siguiente también se vieron afectados equipos con Windows 10, esta vez sin hacer alusión al antivirus. No se tienen tantos antecedentes para este caso, salvo que el ataque se llevó a cabo con un ransomware (software malicioso que cifra archivos, para luego extorsionar a la víctima pidiéndole un pago para que vuelva a tenerlos disponibles, pudiendo también eliminarlos progresivamente), en específico LockBit 3.0, posiblemente usando correos electrónicos como vector de ataque, ingeniería social, disposición de dispositivos USB infectados, o habiéndolos ubicado gracias a un acceso previo.

¿Cuáles son los errores y omisiones más comunes en las que incurren entidades gubernamentales en materia de ciberseguridad?

Sin necesariamente hablar en específico de Chile las omisiones más frecuentes son:

- Tener dispositivos y sistemas obsoletos.

- Creer que nunca serán afectadas.

- Creer que son lo suficientemente maduras a nivel de Ciberseguridad (y si en verdad lo son, creer que el trabajo ya está hecho).

- Destinar recursos insuficientes.

- Ver a la seguridad en general como un gasto y actuar más de forma reactiva, por miedo o por cumplimiento que de forma proactiva y preventiva.

- No contar con una adecuada gestión de parches.

- Dejarse llevar por política más que por capacidad técnica, muchas veces desoyendo a las voces tanto internas como externas, e incluso fijando cargos por demostrada lealtad política antes que por competencias idóneas.

¿Puede un dispositivo externo como un teléfono inteligente vulnerar un sistema Cibernético de alta complejidad al cual se encuentra vinculado mediante correo electrónico?

Es posible, pero más siendo un medio de acceso que un ejecutor de ataques (lo cual sigue siendo factible). Muchas veces, los dispositivos móviles en general no son adecuadamente securitizados antes de su ingreso a una red o a su uso de forma laboral (por no decir que incluso podría ser implementado sin ser securitizados en lo absoluto), por lo que ampliarían la superficie de ataque, siendo un caballo de troya.

Para lo anterior, lo ideal sería primero definir si la organización los empleará o no, según su naturaleza y necesidades (puede prohibirlos, optar por brindar sus dispositivos ya securitizados, o adecuar a los que tengan sus colaboradores y proveedores), documentar y difundir sus políticas, implementar MDM (Mobile Device Management), llevar un inventario vivo de sus activos, contar con software de seguridad en ellos, así como medios que le otorguen la capacidad para identificar, detectar, contener y recuperar de incidentes relacionados.

Para cerrar, ¿cuáles son sus comentarios finales?

Dado que nada es eternamente invulnerable, se debe disponer de acciones de detección proactivas y contar con medidas de prevención y respuesta probadas. Asimismo, se hubiese evitado el ataque al EMCO (al menos en la forma que lo sufrió) de haber contado con sus parches aplicados de forma oportuna.

Destaco la importancia de que las entidades conozcan su perfil de riesgo, qué los hace atractivos ante un ataque, quiénes podrían ser sus adversarios y factores de amenazas, y entender sus motivaciones (por ejemplo: los hacktivistas, tienen motivaciones políticas e incluso sociales, lo que puede volverlos más determinados por sus convicciones que por su beneficio económico).

Por último, aunque estas líneas abordan principalmente lo que ha venido sucediendo a grandes entidades, principalmente gubernamentales, el resto de los sectores, las organizaciones de menor tamaño y la sociedad en general también deben tomar cartas en su ciberseguridad, ya que quizás sea menos vistoso atacar a una entidad pequeña, pero puede ser más rentable al requerir menos esfuerzos, pasar más desapercibido y hasta servir para amplificar ataques (DDoS, redes zombi) o usar sus recursos para beneficio propio (como minar criptomonedas, reduciendo la potencia para su uso previsto).

CIBERSEG

Félix Miranda
Integrante del departamento
de Ciberseguridad de REDSEG

Leyendas Urbanas de Ciberseguridad

Imagen de kalhh en Pixabay

En muchas ocasiones como profesional de la seguridad de la información, me he topado con situaciones donde las personas expresan desconocimiento en mi área, esto hasta cierto punto es normal ya que lo que para mí es habitual para otra persona no lo será, esta situación se podría replicar o trasladar a cualquier profesión o circunstancia, lo que me hace pensar que muchas de las personas, entre su desconocimiento, se dejan llevar por leyendas urbanas. En este caso leyendas urbanas de ciberseguridad.

Lo interesante es que esas mismas personas que creen fielmente en esto no reconocen o piensan que son leyendas, sino que es sabiduría popular, la intención de esta columna es llegar a todos aquellos que aún creen en esto, que no tienen controles de ciberseguridad, en generar conciencia, apoyar a las organizaciones, decirles y demostrarles que la ciberseguridad no es solo tecnología, sino que es un tema de negocio, es un habilitador que puede hacer que una empresa crezca, como que desaparezca.

Considero que como usuarios nos falta educarnos y no solo en ciberseguridad, sino en todos los aspectos, ejemplo hay personas que no saben utilizar una tarjeta de crédito pensando que ese es su dinero y no comprenden que se lo están prestando por lo cual necesitan educación financiera, así mismo ocurre con los sistemas informáticos, si en el mundo físico alquilamos una oficina, le ponemos puertas, candados y demás dispositivos de seguridad, lo mismo, se debe hacer en la parte tecnológica.

Establecido esto les diré lo que considero son las leyendas urbanas más comunes y como debemos cambiar esos paradigmas:

Solo Windows puede tener virus: Han ocurrido ataques en IOS y Linux lo que dejo demostrado que esto es falso, quiero decirle que no hay una seguridad 100% segura ni siquiera en nuestra casa, les explico: estando en nuestro hogar si nuestro hijo esta en su habitación navegando por la internet puede sufrir ataques informáticos, estando acostados en nuestra cama se nos puede caer el techo encima, se nos puede ir la saliva por otro lado, en fin muchas situaciones imprevistas si lo trasladamos al mundo cibernético.

Si yo soy un cibercriminal me voy a interesar más en una plataforma que tiene 100 millones de usuarios, que en una que solo tiene 10 millones. Los cibercriminales siempre le van a buscar la vuelta al sistema operativo, es como la estafa del rey nigeriano o de la señora que quiere dar su fortuna, su herencia, a un desconocido.

Si un proveedor de servicios dice que con la solución que nos ofrece tendremos un sistema 100% seguro, debemos tener la capacidad de reconocer que esto es totalmente falso por lo cual no debemos dejarnos llevar de buenas a primeras ante la inmediatez o las ofertas de soluciones tecnológicas.

Mis datos no son importantes: ¿Ni soy millonario, ni soy famoso, no tengo dinero porque un ciberdelincuente se interesaría en mí? Quiero decirles que las bases de datos se trafican, que se ha generado una economía del clic a nivel mundial, por eso la suplantación de datos y cualquier robo de información está a la orden del día, en muchas ocasiones descargamos e instalamos aplicaciones y no vemos que datos o que permisos le estamos entregando lo que hace que nos roben o que se filtre nuestra información.

Quizás mi información por sí sola no vale mucho, pero créanme que el conjunto de datos de la población es muy valioso, aunque una red social sea gratis nosotros estamos pagando con nuestros datos. ¿Cuantas organizaciones piensan que son pequeñas y que nunca le han robado información o que no son importantes? Mientras una empresa siga viendo la ciberseguridad como algo tecnológico y no como una parte del negocio estará totalmente expuesta, ya que tienen los datos, nómina y cualquier información de las otras empresas, filiales, clientes y proveedores.

En la pandemia se vio un aumento en los ataques a los dispositivos de trabajo remoto por esta misma situación, ya que muchas personas pensaban que no los podían atacar por ser un ciudadano de a pie, un ciudadano común y corriente. Así tengas un negocio que venda tomates y no tengas mucha tecnología eres vulnerable.

Estoy blindado porque tengo un servicio de seguridad: Parece irónico pero muchas personas pecan de petulantes, de arrogantes porque se confían ante esto, desde el nivel usuario hasta las grandes organizaciones, quedó demostrado cuando países enteros han sido hackeados, no se puede perder de vista esta situación, existen dos tipos de empresas las que ya han sido hackeadas y las que no saben que han sido hackeadas, son el medio para llegar a esas grandes empresas.

Los ciberdelincuentes pueden colocar enlaces para sitios maliciosos, pornografía, o cualquier otro virus por lo tanto hay que tener mucho ojo para evitar esta situación, quizás tengan un equipo de ciberseguridad, pero no se pueden confiar

en esto, se debe tener una constante formación y evaluación de los sistemas informáticos de la empresa o negocio.

Posiblemente no seas el fin, pero si el medio, que quiero decir con esto que si tu empresa es vulnerada a través de ti pueden llegar a tus clientes, proveedores o empresas filiales, todos estamos interconectados en una eterna y entera cadena de suministro.

Muchas empresas piensan que si su personal contratado tiene estudios en informática o sistemas saben de todo, hay poca claridad en esto y consideran que pueden resolverlo todo, es como el doctor que estudia medicina, primero comienza con la medicina general para luego especializarse, lo mismo sucede con quien estudia y se emplea en sistemas, le dan muchas responsabilidades y no están preparados y las organizaciones deben saber que tiene que contratar especialistas dedicados en cada área.

Hacker y cibercriminal es lo mismo: Esto nace de un verbo irrumpir, muchas personas piensan que es lo mismo, pero realmente un hacker busca vulnerabilidades dentro de las organizaciones e instituciones, mientras que un ciberdelincuente tiene como intención dañar y lucrarse a través de esta acción, ambos tienen las capacidades y las habilidades para lograr adentrarse en un sistema informático. Es casi un personaje mítico.

Pero no solo con habilidades informáticas se puede hacer esto, con habilidades sociales también pueden acceder a los mismos aplicando ingeniera social, en la mayoría de los casos las amenazas o las peores amenazas están dentro de la organización, la mayoría de las personas piensan que se deben cuidar del hacker, pero un gran porcentaje de los delitos se realizan de manera interna por lo tanto para evitar esta situación se deben hacer auditorias, evoluciones, aplicar la confianza cero, crear el filtro de acuerdo a la jerarquía de cada empleado, ya no se ataca a la infraestructura tecnológica se ataca al usuario sobre todo por medio del phishing.

Solo los ataques vienen de amenazas externas: El mismo usuario tiene la iniciativa, puede ser amenazado desde afuera, las amenazas pueden ser de ambos lados como se explicó anteriormente, por eso debemos estar al tanto de todas estas situaciones, recuerdan aquel personaje, aquel vendedor ambulante que ofrecía una panacea, una medicina que quitaba todo tipo de malestares, aquel que tenía un brebaje que lo curaba todo, cuando en realidad tenía un cómplice que tomaba del líquido y se curaba milagrosamente y simulaba que todo estaba bien.

Pues esta simulación se está llevando al mundo tecnológico, ¿ya todas estas estafas se enfocan en las personas debido a que es más fácil engañar y dejar que sea el usuario final haga el trabajo difícil, antes que sea el mismo ciberdelincuente que invierta tiempo y recursos en estos intentos, como se mejora esto?

Creando cultura de ciberseguridad dentro de las organizaciones, son los hábitos, las creencias lo que nos ayudara a solventar todas estos problemas, tomo como ejemplo de lo que pensamos sobre el ejército, pensamos que tienen una jerga, una etiqueta, una cultura distinta, lo mismo sucede dentro de la organización que tienen cultura de seguridad, de prevención, identificando riesgos, pero no solo que los pueden identificar sino que también sepan actuar ante un problema, porque también suele suceder que no saben a quién llamar, a quien informar, ante una situación adversa, compartir la cultura de seguridad es importante.

No necesito un especialista yo lo puedo hacer: Lo poco o mucho que puedas invertir o hacer por ahorrarte algo de dinero, te saldrá más caro al delegar toda tu ciberseguridad en el personal de soporte técnico pensando que este lo puede hacer todo a la vez, he visto que inventan y crean políticas de seguridad, pero no hacen análisis de riesgo previos lo cual es un error garrafal.

Hoy es muy fácil atacar a una empresa, hay recursos como contratar servicios para dañar la reputación o la estructura de una organización, quiero hacer un ataque de denegación de servicio pues lo contrato, con esto daño una de los principios de la seguridad informática la disponibilidad de los recursos.

Ya hay software para hacer vectores de ataque, los cuales se compran en la Deep web o en la Dark web, las personas son el eslabón más débil, en muchos casos las empresas invierten en tecnología, pero no en su capacitación, también sucede que en algunos casos capacitan, pero contratan a alguien con léxico muy tecnológico y este no trasmite el mensaje de forma adecuada.

Muchas empresas no invierten en tecnología o en capacitar a su personal, pero una organización delictiva si lo hace y más, habiendo tanto dinero de por medio, es una reflexión que les dejo ya que ellos, los chicos malos, nos llevan una ventaja con relación a eso.

Mi antivirus me protege: Mas que no querer invertir muchas veces las empresas no saben que quieren contratar o solucionar, en ocasiones contratan a un supuesto experto y este llega diciendo que deben invertir en una solución tecnológica sin hacer un informe de vulnerabilidades, revisar si fue el becario quien instalo ese antivirus gratuito, o simplemente hacer el estudio previo antes de ofrecer programas o paquetes de soluciones.

Foto de Mark Harrison en Unsplash

El elemento humano nada podrá hacer si no existe una metodología en la tecnología y los procesos, si tengo un antivirus o firewall gratuito, si no lo tengo configurado adecuadamente, si tengo las claves de fábrica, si no se gobierna el sistema estamos fallando, esto es de vital importancia ya que a la tecnología se le deben crear procedimientos y procesos, no le van a salir brazos para impedir algo que dañe o interfiera con el sistema.

Como profesional de la seguridad informática pienso que las personas que utilizan los sistemas diariamente tienden a cuidarse, ya que usan de manera habitual gestores de contraseñas o cualquier medida de seguridad, pero lamentablemente no es así, me he dado cuenta que debemos hacer más accesibles nuestro discurso, hacerlo más digerible ya que hay una brecha digital por ese mismo lenguaje, si logramos esto el usuario final por ejemplo, podrá determinar porque su aplicación le está pidiendo permisos que no tiene nada que ver con su función y así se podrá comenzar a corregir todo el sistema ocasionado por el desconocimiento.

Las mujeres no forman parte dinámica de la ciberseguridad: No solo en la ciberseguridad se aplica esto, sino en muchas más instituciones lo cual es un viejo paradigma, esto se debe comenzar a corregir ya que se ha determinado que las empresas donde trabajan más mujeres son de las organizaciones más exitosas, más allá del machismo, debemos educarnos, informarnos, no ver la ciberseguridad como algo tecnológico, debido a que como consultor he observado que los mismos directores por falta de entendimiento, de claridad incluso hasta de miedo, son los principales responsables de detener el empoderamiento de las mujeres dentro de las organizaciones.

Si un CEO es garante de las inversiones, contratos y afines debe saber que nuestra vida está inmersa en la tecnología y que las mujeres son parte activa de este desarrollo. Si no asumen esto, el problema será mayor en algún momento, es como cuando invierten 100 dólares en ciberseguridad, pero cuando les ocurre algo quieren ante la necesidad invertir 1000 dólares de inmediato, no se adelantan a los hechos, no ven más allá, no ven el futuro.

Dejar de creer en novelas de fantasía, pensar que lo que uso es totalmente seguro tanto en el mundo físico como en el digital es falso, este es mi granito de arena para seguir contribuyendo el fomento de una cultura de prevención y de seguridad, lamentablemente estas leyendas tenemos años escuchándolas, pero la intención con este escrito es dejar una enseñanza y comenzar a cerrar dichas brechas, debemos tener en cuenta que los datos son el nuevo petróleo.

Evite ser victima

Adolfo M. Gelder
@adogel
t.me/seguridadintegral

Proteja hoy su dispositivo celular

En diversas oportunidades en nuestro portal web nos hemos referido a la preocupante vulnerabilidad de los dispositivos celulares. Con más de 33 millones de dispositivos en uso en Chile, estos representan un segmento de alto riesgo. Contactos, claves de acceso, control de nuestros sistemas de domótica, cámaras de vídeo vigilancia, claves bancarias entre otros, son los incentivos para ser victimas de un ataque cibernético. A nivel mundial existe una empresa poco conocida en Chile, denominada Dr. Web, la cual cuenta con una trayectoria de 30 años y con presencia a nivel global y que se encuentra a la vanguardia en el área de las soluciones en ciberseguridad, la cual dispone de excelentes soluciones para brindar protección a nuestros dispositivos móviles.

¿Qué podemos comentar respecto d elos principales antecedentes de Dr. Web?

En el año 1993, Dr.Web fue el primer programa en la historia de la industria antivirus, capaz de detectar y desinfectar los equipos contra los virus polimórficos sofisticados. Esta propiedad tecnológica del antivirus Dr.Web le hizo internacionalmente famoso en el ámbito profesional, este reconocimiento lo distinguió y marcó una clara diferencia entre los antivirus que protegen de verdad.

También es notorio destacar que Dr.Web fue pionero en el desarrollo de soluciones orientadas a detección de los primeros virus desarrollados para atacar equipos macOS

¿Cómo ha sido la evolución de los ciberataques en dispositivos como los Smartphones a nivel mundial?

Durante el último trimestre de este año los analistas de virus de la empresa Doctor Web han detectado un aumento de amenazas en el catálogo Google Play con decenas de aplicaciones con malware (troyanos de publicidad y programas falsificados) insertados por actores malintencionados con la finalidad de robar información privada. Esto nos muestra que incluso en plataformas supuestamente "seguras y confiables", nuestros dispositivos están expuestos, al igual que los datos, privacidad y hasta la intimidad.

La empresa Doctor Web comunicó la información de las amenazas detectadas a la corporación Google y ya han sido tomado en cuenta los correctivos. No obstante, los crímenes digitales seguirán buscando nuevos y sofisticados métodos para atacar a sus víctimas.

Qué nos puede comentar con respecto al nivel de protección que nos brinda Dr. Web?

Doctor Web es uno de los pocos vendedores antivirus en el mundo que tiene sus propias tecnologías únicas para detectar y desinfectar los programas malintencionados. La protección antivirus Dr.Web permite a los clientes afrontar cualquier amenaza, incluidas las desconocidas, gracias a la implementación de:

- Tecnologías de protección preventiva
- Tecnologías de detección no basada en firmas
- Tecnologías de detección a base de los algoritmos de aprendizaje automático
- Tecnologías antispam
- Base de virus
- Sistema global de actualizaciones

Todos estos componentes fusionados nos permiten manejar información útil sobre troyanos, virus, programas nocivos, spam y otras amenazas en la Internet, brindando así una seguridad 360 a nuestros clientes.

DESCARGUE LA VERSIÓN GRATUITA DE Dr. Web

Gracias a un acuerdo logrado entre nuestro medio y Dr. Web nuestros lectores podrán acceder a una versión gratuita del antivirus para dispositivos celulares escaneando el código Q adjunto, o realizando click sobre él..

CIBERSEG
Un nuevo referente para el área de la Ciberseguridad

Los recientes ataques cibernéticos sufridos tanto por el Estado Mayor conjunto como el Poder Judicial no se ven llevar a reflexionar respecto de la forma en que hemos abordado la temática de la ciberseguridad ya que sin duda y de acuerdo a todas las opiniones, lo que trasciende a los medios constituye sólo un porcentaje mínimo del volumen real de ataques cibernéticos. Por lo anterior Revista Seguridad Online se contactó con Denny Rodríguez, Director de CIBERSEG, la unidad de ciberseguridad de la reconocida Red Latinoamericana de Profesionales de Seguridad Tecnológica (REDSEG)

¿Cómo surge la idea de generar esta unidad de Ciberseguridad al interior de REDSEG?

REDSEG fue concebida como una organización gremial que tendría como prioridad estar adaptada a la nueva era de la seguridad y actualizada constantemente con las técnicas y métodos del crimen y delincuencia de alta tecnología.

Esto implicó conformar una unidad orientada a ofrecer apoyo, capacitación y servicios para nuestros agremiados entorno a temas vinculados con seguridad cibernética, ciberseguridad, delitos digitales y amenazas virtuales.

¿A nivel latinoamericano cuál es la real situación de vulnerabilidad en términos de ciberseguridad?

Latinoamérica en los últimos años se ha convertido en un territorio "sin ley" en sentido virtual, donde grupos ligados al cibercrimen, ciberespionaje y ciberterrorismo opera a sus anchas debido a las deficientes políticas de los gobiernos en cómo abordar los actuales retos, amenazas y riesgos dentro del ciberespacio.

Un problema que en los últimos meses se ha acrecentado y convertido en tema de prioridad nacional para muchos países.

¿Qué nos indica la tendencia en cuanto a los volúmenes de ataques?

Durante el período 2020-2021 (pandemia) se incrementó a niveles preocupantes y nunca antes vistos, ataques dirigidos a gobiernos, organizaciones internacionales, corporaciones, empresas y ciudadanos en las distintas plataformas de interacción social a escala mundial. Estos incidentes encendieron las alertas en todo el mundo sobre la necesidad imperante que representa la seguridad digital en la sociedad actual.

¿Existe una estimación porcentual entre los ataques efectivamente perpetrados y aquellos de los cuales la comunidad llega a tener conocimiento?

Los estudios e informes estadísticos con frecuencia son presentados a la comunidad mundial por reconocidas entidades internacionales de gran credibilidad dentro del sector. Por ejemplo, durante el año 2021 se manejó la cifra oficial del 300% en el aumento del cibercrimen a nivel global.

¿Cuales son las principales recomendaciones qué tanto personas, empresas o autoridades al contratar asesoría en materia de ciberseguridad?

Podemos poner en práctica sencillos consejos:

- Mantenga al día sus sistemas (Parches y actualizaciones de seguridad)
- Cuente con software especializado en sus dis - positivos para protegerse y defenderse de las ac tuales amenazas cibernéticas
- Utilice contraseñas complejas y métodos de autenticación robustos.
- Tenga precaución al revisar su buzón de correo
- Precaución al conectar su dispositivo en redes públicas libres o gratuitas con acceso a internet.
- Evite visitar enlaces de dudosa procedencia y responder a personas desconocidas en redes so ciales con propuestas atractivas de negocio.

Aplicando estos sencillos tips podrá mantener a raya a los ciberdelincuentes.

¿Cómo contactarlos?

Visitenos: ciberseg.redseg.org
Escribanos: ciberseg@redseg.org

Denny Rodríguez, Director de CIBERSEG,

Actualizar nuestra legislación Una necesidad frente al escenario actual

Image by Daniel Bone from Pixabay

La necesidad de que la persecución penal disponga de las herramientas e instrumentos que den cuenta del actual escenario en materia de delincuencia, constituye una prioridad Revista Seguridad Online entrevistó al abogado penalista y fiscal Jefe de la Fiscalía de Análisis Criminal y Focos de la Región de Antofagasta, Juan Castro Bekios, con quién para abordar distintas materias referentes a los cambios qué la vigencia requiere la realidad actual y materia delincuencia

La contingencia que existía al momento de implementar la Reforma Procesal Penal dista enormemente respecto del contexto que el sistema afronta hoy, en especial en lo que se refiere a temas como el crimen organizado y el narcotráfico. ¿Cree que las actuales herramientas legales permiten abordar adecuadamente esta nueva realidad?

Antes que todo aclara, que las opiniones que se verterán enseguida son personales fruto de la experiencia al haber ingresado al Ministerio Publico el año 2003 y de casi 15 años dedicado a la persecución penal del tráfico de drogas y por tanto no corresponden necesariamente a la postura institucional del Ministerio Público.

Dicho lo anterior, efectivamente cuando se implementa la reforma procesal, la que por lo demás fue de forma gradual y que culminó con la entrada en vigor en junio de 2005 en la Región Metropolitana, los fenómenos criminales que se enfrentaban en aquella época y sobre todo las formas, modalidades y tecnologías existentes para la comisión de muchos delitos distan mucho tanto en lo cuantitativo como en lo cualitativo, si se comparan con la realidad que actualmente enfrentamos.

Sólo en términos cuantitativos la cantidad de delitos, las nuevas formas de criminalidad y los nuevos tipos penales que se han incorporado a nuestra legislación penal han aumentado notoriamente.

Por otra parte, sumado a lo anterior tanto los delitos como las formas de criminalidad se han tornado más complejos tendiendo muchos de ellos a cometerse por agrupaciones criminales de personas de manera organizada, en otras palabras, lo que se conoce como crimen organizado o delincuencia organizada.

Frente a esta nueva realidad urge la necesidad de actualizar nuestra legislación tanto en materia de tipos penales, es decir delitos, de procedimiento penal y de técnicas de investigación que permitan enfrentar de forma eficiente la actual realidad delictual. En consecuencia, las actual legislación, debe no sólo revisarse, sino que también incorporar nuevas herramientas legales.

Como forma de graficar la situación que enfrentamos, por ejemplo hoy no existe para los delitos de la ley de control de armas y particularmente el tráfico de armas la posibilidad de ampliar la detención por el plazo de 5 días y sin que se realice audiencia ante un Tribunal de Garantía de un imputado que sea sorprendido con un número importante de armas o derechamente un cargamento de armas.

Este vacío dificulta o impide la posibilidad de realizar entregas controladas de armas con el objeto de permitir la circulación por el territorio nacional de forma controlada del cargamento manteniéndose el imputado detenido hasta por cinco días con el objeto de llegar a materializar la entrega de las armas y lograr la detención del destinatario de las mismas en nuestro país. En otras palabras, actualmente si uno o más imputados fueran sorprendidos en alguna ruta del norte del país con un cargamento de armas automáticas con destino a la región metropolitana o más al sur y este quisiera cooperar para seguir el viaje, hacer la entrega al destinatario y detenerlo, no sería posible hacerlo ya que la ley obliga a poner a disposición al detenido dentro de las 24 horas siguientes de su detención, lo cual frustraría la diligencia, ya que las organizaciones criminales están pendientes de los tiempos y ubicaciones de sus envíos ilícitos y monitorean permanentemente a sus transportistas. Hoy tenemos que conformarnos con la detención del transportista a pesar que este tuviera la voluntad de cooperar con la investigación, llevar y entregar las armas bajo la supervisión, control de las policías y autorización de un fiscal del Ministerio Público. Este es solo un ejemplo de la necesidad urgente de actualizar nuestra legislación.

¿Dispone Chile de niveles de penas o sanciones que permitan incrementar la capacidad disuasiva del sistema penal?

Si consideramos que la finalidad de la pena tiene por objeto disuadir al delincuente de cometer nuevos delitos, es necesario poner atención en la aplicación que de las penas se hace con la normativa ya existente. En este sentido, conviene mencionar la aplicación que se ha venido realizando al tipo penal del tráfico de pequeñas cantidades de droga o microtrotráfico, también conocido en otras latitudes como narcomenudeo.

Nuestra legislación contempla esta figura penal

de aplicación excepcional para aquellos casos de tenencia, posesión, guarda entre otras hipótesis de droga. Esta figura legal, que luego de 15 años de vigencia de la ley penal aún sigue siendo una materia de debate respecto de la intelección de la expresión "Pequeñas cantidades de droga", la que luego del periodo antes señalado no ha logrado una interpretación medianamente uniforme en los tribunales de Justicia en el país, así como tampoco en los criterios de actuación que utilizan los fiscales a lo largo del país, lo que además de hacer cada vez más lejano el principio de certeza jurídica, en algunos casos es y ha sido objeto de interpretaciones contradictorias. En efecto, en nuestra opinión se debería volver a la intención original del legislador de la ley N°20.000 y que están plasmada en la historia de la ley, en el sentido que el tráfico de pequeñas cantidades de droga sólo debe ser beneficiado con una pena menor cuando se trate efectivamente de aquellos denominados dealers callejeros independientes que no forman parte de ninguna agrupación delictiva (es decir no son vendedores de otro traficante como los denominados "pilotos") y para aquellos casos de vendedores de droga que lo hacen solamente para satisfacer su propio consuno derivado de la adicción a la que han llegado producto del consumo de drogas. Estimamos que sólo en estos casos se justifica un tratamiento punitivo más benévolo.

Es necesario mencionar que con la actual norma del artículo 4° de la ley N° 20.000, se ha dificultado la persecución penal del denominado tráfico urbano sobre todo en las ciudades donde hay más consumo de droga. Por esta razón urge una modificación legal que establezca un parámetro objetivo de lo que debe entenderse una pequeña cantidad de droga o derechamente eliminar la figura del denominado microtráfico y ser absorbida por al Tráfico de Drogas del Artículo 3° de la Ley N° 20.000. De este modo en el contexto de la persecución penal del tráfico en contexto barrial o poblacional, o tráfico urbano de drogas, se generaría un desincentivo al traficante final para cometer este ilícito, dado que se enfrentaría a un castigo más severo lo que aumentaría la relación costo-beneficio en cuanto al riesgo de persistir en esta actividad, haciendo que el costo punitivo de más años de privación de libertad obligue al traficante a reconsiderar involucrarse en este tipo de actividad delictiva y, sobre todo a reincidir en la misma.

Por otra parte, en este mismo ámbito de delitos también resulta necesario adecuar algunas penas conforme a la ofensa que para la sociedad implica la comisión de algunos delitos. En este sentido, debe existir un adecuado equilibrio valorativo entre la intensidad de la ofensa al o los bienes jurídicos ofendidos por el delito, en el caso del tráfico de drogas la salud pública y la libertad individua en relación a las penas asignadas a las diversas situaciones.

Así por ejemplo, nuestra ley de drogas establece como figura general el tráfico de drogas regulado en el Art. 3° de la ley de drogas que posee una pena que va desde los cinco años y un día de privación de libertad hasta los 15 años de privación de libertad, que por la extensión de estas penas deben cumplirse de forma efectiva. Sin embargo nuestra legislación no contempla ninguna diferencia en cuanto a la gravedad de la pena a aplicar tratándose de tráficos de grandes cantidades de droga. Por ejemplo, de acuerdo a nuestra legislación actual tendrían la misma pena el caso de correo humano que lleva oculto en sus vestimentas un kilo de clorhidrato de cocaína, que el de un transportista que lleva oculto en un camión 400 kilos de la misma sustancia.

El explosivo incremento en la implementación de sistemas de seguridad electrónica, en especial cámaras, no pareciera traducirse en una disminución de los delitos ¿dispone la actual legislación de una postura definida con respecto a la capacidad probatoria de los sistemas de seguridad electrónica (cámaras) de forma tal que el sistema penal oriente al mercado hacia la implementación de soluciones que en definitiva permitan materializar una sanción efectiva con mayor capacidad de disuasión?

Sobre este punto la legislación actual en materia procesal penal no ha tenido una modificación sustancial con la misma velocidad que han tenido las nuevas tecnologías de seguridad y sobre todo de televigilancia. Por esta razón surge la necesidad en nuestra opinión de que exista una regulación en el ámbito procesal penal que reconozca la existencia de estas nuevas tecnologías y que pueda dirimir de forma más precisa aquellas hipótesis que requieren autorización judicial y cuales podrían ser facultades del Ministerio Público a través de sus fiscales.

¿Qué importancia otorga usted a la reforma a las policías para apoyar la gestión de los fiscales?

Conforme a la actual realidad criminal resulta capital evaluar reformas para mejorar particularmente las investigaciones complejas. Es decir, fortalecer en todas las policías y aquellas otras instituciones que por su normativa cumplen fun-

Image by Thomas Rüdesheim from Pixabay

ciones de tal, como lo son Gendarmería de Chile y DIRECTEMAR de la Armada de Chile en áreas que actualmente requieren mayor especialización como lo son los actuales fenómenos de crimen organizado que han ido apareciendo en nuestro país. Lo anterior hace necesario fortalecer las unidades especializadas de investigación que se dedican a fenómenos como el tráfico de drogas, el lavado de activos, la trata de personas, tráfico de migrantes, cibercriminalidad, entre otras. Asimismo, y para la investigación de delitos complejos actualmente se hace necesario incorporar en las policías profesionales especializados en ciertas áreas de la delincuencia en donde los conocimientos de ciertas materias son imprescindibles para hacer frente a fenómenos como el lavado de activos, donde muchas veces las organizaciones criminales cuentan ya sea como asesores o entre sus propias filas a profesionales del área contable, financiera y legal, lo mismo puede replicarse de fenómenos como la cibercriminalidad.

¿Cómo abordar el problema generado por el explosivo incremento de los delitos considerando que el Ministerio Público mantiene en términos generales la misma dotación de personal?

Sin duda cuando se implementó la reforma procesal penal, la dotación de fiscales fue pensada para enfrentan un número de delitos que ha sido desde hace años sobrepasado y que cada vez se incrementa. Por otro lado, en los años de los inicios de la reforma procesal penal no enfrentábamos como país los fenómenos de criminalidad compleja y organizada que hoy nos aqueja como país.

Sin duda alguna esta nueva realidad no prevista hace urgente un aumento numérico significativo de la planta de fiscales en relación a la actualmente existente, pero también una modificación legal que otorgue mayor flexibilidad cuando surja la necesidad de realizar otras modificaciones a la planta de fiscales. Por otra parte, además del aumento cuantitativo es imperativo contar con procesos de perfeccionamiento formales que permita ir preparando a los nuevos fiscales para la investigación de delitos complejos y de las formas de delincuencia que vayan surgiendo con el tiempo.

Sumado a lo anterior, y en base a la experiencia que ha significado la creación de los sistemas de análisis criminal y focos investigativos (SACFI) con la incorporación de profesionales analistas criminales provenientes de distintas áreas del conocimiento como las ciencias de la ingeniería o ciencias sociales que han resultado ser un sustantivo aporte para la metodología de investigación que utilizan los SACFI a nivel nacional que han permitido pasar de la investigación tradicional del caso a caso a la investigación mediante focos que se ocupan ahora de fenómenos criminales y mercados delictuales. Este innegable aporte que han hechos los sistemas de análisis criminal en nuestro país han permitido la obtención de resultados más eficientes en la investigación de delitos que en muchos casos eran objeto de archivo por no contar con una metodología que permitiera vincular casos aparentemente inconexos, en casos totalmente relacionados y que muchas veces eran cometidos por una misma agrupación criminal.

La inmigración ilegal unida a la dificultad de acceder a un adecuado control de antecedentes se traduce en un preocupante incentivo para el crimen organizado ¿Cómo se puede avanzar hacia la generación de una estructura de Seguridad nacional que permita neutralizar oportunamente este peligro, permitiendo descongestionar el creciente flujo a afronta el Ministerio Público?

Al menos en la macrozona norte, no puede desconocerse que algunas de las nuevas formas de criminalidad obedecen, entre otros factores al incremento de la inmigración ilegal. Sólo a modo de ejemplo podemos mencionar que el porcentaje de participación de extranjeros en la comisión de algunos delitos se ha ido incrementando al menos en la Región de Antofagasta.

Las actuales cifras nos periten afirmar que por ejemplo tratándose del robo de vehículos notoriamente la mayoría de los imputados conocidos son nacionales y desde otra vereda en el caso del tráfico de drogas y particularmente tratándose del tráfico de drogas del Art. 3° de la ley de drogas, figura delictiva central de la ley de drogas, la participación de extranjeros como imputados conocidos en estos delitos ha ido en constante incremento en relación a la participación de nacionales.

La constatación de esta realidad impone grandes desafíos para evitar que esta situación se mantenga o incremente. Entre ellas el control de las fronteras es un factor de suma relevancia sobre todo en el norte del país que por sus condiciones geográficas ha permitido la existencia de numerosos pasos no habilitados de personas y vehículos que ingresan sin control. Si a ello se añade que este importante número de ingresos no controlados tiene por objeto la comisión de delitos la situación se torna mucho más preocupante. Por esta razón debe avanzarse de forma urgente en convenios efectivos, expeditos, exentos de burocracia que permitan entre nuestros países vecinos contar de forma rápida con los antecedentes de identidad y prontuáriales de las personas que sean sorprendidas ingresando al país por pasos no controlados. Actualmente dicho proceso es tremendamente lento y ha permitido por la demora en obtener la información que personas que cuentan con antecedentes penales en otros países hayan sido condenados en Chile como autores de su primer delito lo que les ha permitido optar a beneficios que están vedados para personas que poseen antecedentes previos por la comisión de algún delito.

Sostenemos que efectivamente estos factores, entre otros, inciden de forma negativa facilitando el ingreso de personas que están vinculadas a organizaciones criminales extranjeras.

Juan Castro Bekios ,Jefe de la Fiscalía de Análisis Criminal y Focos de la Región de Antofagasta

Principios prácticos para reclutar, enseñar y liderar escoltas,

Después de muchos años y experiencia en el campo, en varias unidades de protección ejecutiva en el mercado Institucional y privado, puedo apoyar a mis compañeros con una visión y pensamiento fuera del servicio. Estoy enfocado en diez principios prácticos de liderazgo de campo, que personalmente he encontrado muy útiles para las operaciones de seguridad en los sectores que menciona. Estos principios provienen de más de dieciocho años de mi propia experiencia de liderazgo, comenzando en el IDF, y luego En el ministerio de defensa de Israel, abarcando además al sector privado.

Plan para adaptación 1

La planificación operativa es la que debe brindar una plataforma desde la cual adaptarse y cambiar cuando las cosas no resultan como se pensó que lo harían. Un buen plan debe adaptarse a la situación, no al revés.

Cuando los hechos sobre el terreno comienzan a cambiar; su plan debe ajustarse en consecuencia. No digo que se deba abandonar inmediatamente el plan tan pronto como las cosas cambien, solo que un plan debe ser una plataforma para operar, en lugar de una secuencia de comandos de eventos futuros.

Las realidades en el campo tienen una forma curiosa de jugar con las expectativas previas. Un líder en la área de escoltas, tiene que levantarse en la mañana y prepararse para una guerra, es decir, a la situación más extrema que puede pasar, y su plan debe reflejar eso.

2. ¡Mantenlo simple

Tan pronto como tenga en cuenta que la realidad en el campo casi siempre diferirá de las expectativas, y que los planes originales a menudo tendrán que modificarse, debe darse cuenta de que los planes deben ser simples.

Si un plan es demasiado complejo, será muy difícil modificarlo y ajustarlo sobre la marcha. Usted mismo puede estar de acuerdo con eso, pero el plan no es solo para usted: tiene que liderar todo un equipo de seguridad.

Si ya tienen que lidiar con un plan complejo, es muy probable que este se pierda tan pronto como empieces a hacer ajustes en él.

3. Cómo realizar un buen briefing inicial antes del comienzo del trabajo

Muchos líderes de seguridad prácticamente no saben qué y cómo pasar un brief operativo relacionado a la operación.

Un resumen del brief efectivo debe cubrir la misión estratégica de lo que el cliente necesita.

1- Nuestra misión táctica: para qué estamos aquí y cómo sirve a la misión estratégica más amplia.
2- Métodos y herramientas para lograr nuestra misión táctica.
3-Parámetros, avanzadas y límites de nuestra misión táctica.
4- Posiciones.
5- Métodos de comunicación.
6- Quién hace qué.
7- Casos y respuestas que pueden ocurrir en la operación en cada posición y cada lugar específico que hay en la rutina y no.

Estos siete puntos deben aplicarse en general a la misión en su conjunto y específicamente a cada puesto individual.

4. Trabaja para tus subordinados

Muchas personas no entienden que el liderazgo es un tipo de relación y, al igual que cualquier otra relación, es una vía de doble sentido. Los miembros del equipo trabajan para su líder, pero un líder también trabaja para los miembros de su equipo.

En muchos sentidos, un líder necesita a sus subordinados, más de lo que ellos lo necesitan a él.

Una cosa interesante que sucede cuando cuidas bien a tu equipo y es que los clientes lo notan, y tienden a apreciarlo y respetarlo.

La mayoría de la gente piensa que un proveedor de servicios solo necesita cuidar a su cliente, pero he recibido muchos elogios a lo largo de los años por lo bien que cuido a mis equipos, y por lo bien que tienden a desempeñarse los equipos Debido a esto, una vez más, cuida muy bien a tu equipo.

5. Liderazgo tipo todo o nada

Un error común de liderazgo en seguridad que he

visto a lo largo de los años es el estilo de gestión de "estás dentro o fuera", "a mi manera o la carretera". A primera vista, esto podría parecer un tipo de liderazgo sólido y sensible, pero no estoy de acuerdo.

No estoy diciendo que no haya situaciones en las que las cosas simplemente deban hacerse de cierta manera, sin argumentos, estoy diciendo que si estás en esto a largo plazo, este tipo de liderazgo no es realmente sostenible, o bueno.

Todo o nada es demasiado simple, demasiado simplista en realidad, y los líderes que intentan decirle que este es solo su estilo, en realidad le están diciendo que realmente no saben cómo hacerlo correctamente.

El liderazgo se trata de motivar a las personas y hacer que se inscriban voluntariamente en la misión. No siempre es simple, y tampoco es tomarse de la mano, es solo un buen liderazgo.

6. Cómo manejar a los miembros débiles del equipo

Casi cualquier líder de seguridad tiene que enfrentar el hecho de que no siempre tendrá un equipo de similar rendimiento debajo de usted y que no siempre puede prescindir de los miembros más débiles del equipo.

Desde mi experiencia, la mejor manera de manejar a la gente de bajo rendimiento es apartarlos, decirles lo importantes que son para la misión y cómo se los necesita personalmente para implementar el conjunto de habilidades de primer nivel que usted sabe que tienen. Es posible que aún sean débiles, pero al menos se esforzará más y le facilitarán el cumplimiento de la misión.

Ahora bien, ¿este tipo de motivación siempre funciona? Por supuesto que no, y eventualmente podría ser necesario tomar medidas más estrictas con un miembro del equipo más débil, Pero reserve esas opciones desafortunadas para más adelante, después de haber probado el enfoque positivo. Recuerde, el liderazgo se trata principalmente de guiar y motivar.

Un error común y que querrás evitar, es enviar a miembros del equipo débiles o poco confiables fuera de la vista, para que se ocupen de una entrada trasera tranquila.

Probablemente sea una buena idea darles un trabajo menos crítico, pero es importante tener en cuenta que la idea aparentemente atractiva deponerlos fuera de la vista podría hacer más daño que beneficio.

Por lo general, se requiere de escoltas sólidos para las esquinas aburridas y lentas, donde éstos no son observados ni administrados de cerca.

Mantén a tus amigos cerca y a tus enemigos más cerca. Si está atrapado con un escolta que no es de confianza, ubícalo donde pueda vigilarlo.

7. Liderazgo en todas las áreas.

He hablado de liderar la cadena de mando hacia abajo, motivar a sus subordinados, pero también debe intentar liderar la cadena de mando, hasta los clientes que lo contrataron.

Obviamente, debe tener mucho tacto; es muy importante infundir calma, control y una sensación de seguridad en su cliente; al fin y al cabo, para eso te contrataron.

Mucha gente a veces no consideran esta ¨recomendación¨ y olvidan que, en esencia, bajo todas las capas de operaciones físicas, sistemas y protocolos, la seguridad es un sentimiento para el que estamos contratados, no para nosotros sino que para nuestros clientes.

Y un buen líder de seguridad sabe cómo inculcar este sentimiento en su cliente.

8. Autocontrol

En pocas palabras, si no puede controlarse a si mismo, ¿cómo controlará o guiará a los demás? Piénselo desde su perspectiva: ¿por qué querría un subordinado seguir a alguien que no puede controlarse a él mismo?. No es que no puedan seguirle, es que probable que no querrán hacerlo. Lograr que la gente quiera seguirle es de lo que se trata el liderazgo.

El mayor problema para mantener el autocontrol es que a menudo no se da cuenta de cuándo y cómo tienden a perderlo. La clave para solucionar esto es desarrollar una buena autoconciencia y empatía; una buena recomendación es mirarse a si mismo como si se tratara de una tercera persona.

¿Cómo se ve ante los demás? ¿Cómo se encuentras? ¿Cómo afecta su tono de voz a las personas a las que te dirige? ¿Cómo le afectaría si se dirigieran a usted de esa manera?

La clave del autocontrol es la autoconciencia.

9. Cálmese y desacelere [tranquilidad]

Ahora que tiene el autocontrol en marcha, úselo para calmarse y reducir la velocidad.

Mucha gente tiende a olvidar lo importante que es esto, especialmente durante los momentos cruciales y estresantes.

Una disposición más tranquila tiene dos funciones importantes: Primero, le ayudará a tomar mejores decisiones.Es como ser un Quarterback, incluso cuando todo está colapsando a su alrededor y está a punto de ser abordado, cálmese, mire a su alrededor y tome una decisión.

Independientemente de si usted personalmente puede manejar un ritmo alto para correr y gritar órdenes, ¿cómo cree que se relaciona con sus subordinados y clientes cuando hace esto?.

Lo entiendo, quiere dar un buen ejemplo, y crear un buen ritmo, pero la línea entre eso y parecer confundido es bastante delgada y se cruza fácilmente.

Por lo general, es más importante para un líder infundir calma y control, y comenzar con calmarse y controlarse a sí mismo primero

10. ¡ Conócete a ti mismo !

El liderazgo tiene que ver con las personas, y comprender a las personas comienza con la comprensión de uno mismo.

Más allá de comprender cómo funciona el liderazgo en principio, si desea aprender cómo usted mismo puede ser un buen líder, deberá descubrir qué tipo de líder eres tu.

El liderazgo viene en muchas formas y de muchos tipos de personas. Trate de no emular demasiado a los líderes que son muy diferentes a usted.

Conoce quién eres, y sé tú.
Algunas personas tienen una disposición de liderazgo permanente, que se manifiesta tanto dentro como fuera del trabajo, Mientras que otras tienen que activarla cuando surge la necesidad.

Algunos líderes son mayores y más distinguidos, mientras que otros son más jóvenes y enérgicos.

Algunos lideran con mucho entusiasmo, mientras que otros tienen una intensidad más tranquila. Cualquiera que sea el caso, sepa quién es usted y descubra su estilo personal de liderazgo...

Autor: Guy Sadeh
Profesional con 22 años de experiencia en el campo de la Seguridad Física y en el ejército Israelí.
Consultor de Seguridad, Especialista en Protección Ejecutiva Oficina de miniterio de defensa interior de Israel , Jefe de operaciones en unidad especial,
Responsable de la elaboracion de los planes y operaciones de misiones oficiales israelies de seguridad en todo el mundo,asi como en las misiones diplomáticas.
Experiencia en:
1. Analisis de datos vinculado a los objetivos estratégicos de las tareas.
2. Orientación global desarrollado a través del empleo en todo el mundo.
Adquisición de conocimiento y experiencia en tecnologías avanzadas de seguridad y vigilancia.
3. Creación de procedimientos de seguridad y estrategias a largo plazo, conducir y facilitar protocolos para la misión diplomática en la ciudad de Lima-peru, incluyendo eventos oficiales en Bolivia.
4. Asumir la responsabilidad de todo contacto con el Ministerio de seguridad domestica local;
5. Instruir al personal, a través de presentaciones y sesiones informativas semanales, en la responsabilidad de proteger datos sensibles; Participación como miembro activo en los comites locales de lucha contra el terrorismo, prestando su experiencia en varios proyectos e inicio de nuevos esquemas.

Experiencia académica respaldada por tres diplomas otorgados por una de las Escuelas de Seguridad Gubernamental más importantes del mundo. Proyecto Maccabiada (Juegos olímpicos judíos) , 2019: Autor del plan de planificación de seguridad para todos los eventos, incluidos los eventos de apertura y cierre.

Guy Sadeh

Teledyne FLIR
Presenta el videoscopio de alto rendimiento VS80 con 7 opciones de sonda, incluida la termográfica

El videoscopio industrial resistente ayuda a los profesionales a detectar de forma rápida y segura problemas ocultos en lugares de difícil acceso. Teledyne FLIR, parte de Teledyne Technologies Incorporated, ha lanzado hoy la serie de videoscopios de altas prestaciones FLIR VS80, una herramienta de inspección profesional apta para una amplia variedad de aplicaciones comerciales e industriales.

Para permitir la gama más amplia de inspecciones visuales, el FLIR VS80 está diseñado como el videoscopio más versátil y potente de su clase.

El VS80 está equipado con una pantalla táctil de siete pulgadas de alta resolución (HD) de 1024×600 y está disponible para su compra en siete kits diferentes, con la opción de comprar sondas ultradelgadas resistentes al agua (impermeables) que se pueden cambiar dentro y fuera en segundos.

Las opciones de sonda incluyen una sonda articulada bidireccional de 4,5 mm de diámetro; una sonda articulada de cuatro vías; un tramo de cañería con sonda de cámara y un cable de 25 metros; sondas de cámara visible de alta definición HD simple y HD doble; una sonda de definición estándar; y una sonda de cámara térmica de propósito general.

"Los comerciantes y los técnicos necesitan inspeccionar objetos en espacios reducidos, sin necesidad de desmontarlos, lo que requiere mucho tiempo en algunas industrias, incluidas la fabricación, la construcción y el mantenimiento en automoción", ha dicho Rob Milner, director de desarrollo comercial de Teledyne FLIR.

»El nuevo FLIR VS80 satisface todas estas necesidades al mismo tiempo que proporciona una versatilidad de diagnóstico impresionante en los espectros de imágenes visibles e infrarrojas.

Los profesionales están mejor equipados para detectar peligros ocultos y daños en lugares que son difíciles de acceder o inaccesibles. En total, el VS80 da al personal de inspección y reparación la capacidad de reducir los costos de mantenimiento y los costos de capital de reemplazo a la vez que mejora la productividad y la seguridad en el trabajo.»

Live Reference simplifica el diagnóstico y la confirmación de reparación

Teledyne FLIR ofrece una comparación única de imágenes de referencia en vivo en la pantalla, para facilitar las comparaciones de imágenes históricas o estándar. Los inspectores simplemente agregan una imagen de referencia en paralelo con las imágenes del videoscopio en vivo. Luego pueden comparar rápidamente las imágenes para ver si un componente ha cambiado desde la inspección anterior o si necesita reparación o reemplazo. La información también se puede agregar a un informe posterior a la inspección con múltiples opciones, para que los inspectores capturen información detallada, incluso a través de texto, voz, imágenes y videos grabados con visualización de marca de tiempo.

El dispositivo también es compatible con la aplicación FLIR Tools Mobile disponible para dispositivos iOS y Android. Desde un dispositivo móvil, vea imágenes guardadas y videos capturados desde el VS80, descargue archivos y compártalos fácilmente con clientes o colegas.

REDSEG | RED LATINOAMERICANA DE EMPRESAS Y PROFESIONALES EN SEGURIDAD TECNOLÓGICA

REDSEG constituye una organización internacional de reconocida trayectoria en el ámbito de los profesionales ligados a la seguridad electrónica y a la ciberseguridad. Este viernes 23 de Septiembre, esta organización dio comienzo oficial a sus actividades en Chile. Conversamos con Elio Caballero, Sub director de esta organización quien a su vez está a cargo de la delegación en chile de REDSEG.

¿Cuál es la relevancia que otorga REDSEG a la apertura de actividades en Chile?

Como organización deseamos brindar al gremio de empresas y profesionales chilenos dedicados a sector seguridad, un puente comercial a nuevas oportunidades de negocios dentro del país con el apoyo de fabricantes tecnológicos de amplia experiencia. Así mismo, el factor formación y la transferencia de conocimiento es uno de los principales ejes dentro de nuestra gestión. La realización frecuente de capacitaciones, charlas y conversatorios serán oportunidades para actualizar conocimientos, así como tambien, mantenerlos a la vanguardia en las distintas disciplinas y áreas del saber que fomentamos.

¿En qué áreas puede aportar REDSEG a los profesionales locales?

Los ejes del conocimiento donde contamos con amplia y sólida experiencia para aportar a los profesionales chilenos son por lo general áreas comúnmente conocidas: seguridad electrónica, ciberseguridad, aerovigilancia, centros de comando y monitoreo, vigilancia inteligencia analitica, tecnologías anti-fuego, defensa electrónica, ethical hacking, entre muchas otras.

No obstante, constantemente nos alineamos a las tendencias del mercado y lo que demanda la industria de la seguridad en la actualidad:

- Inteligencia Artificial- Internet de las Cosas- Ciberespacio- Metaverso - Computación Cuántica. Esto tal vez es un elemento diferenciador que nos permite no sólo mantenernos al día, sino tambiem abarcar a un amplio espectro de audiencia y potenciales miembros agremiados a la organización.

¿Con que alianzas comerciales cuenta REDSEG?

A lo largo de casi 3 años operando oficialmente, hemos establecido importantes alianzas con fabricantes y marcas de talla internacional. Les listamos algunas: TRASSIR (Rusia) Vídeo Inteligencia Analítica Neuronal. DR.WEB (Rusia) Soluciones en Seguridad Cibernética EBS (Polonia) Productos Orientados a Comunicación Crítica TECNAVIX (México) Soluciones en Aerovigilancia Persistente Y muchos otros más...

¿Cómo puede una entidad como REDSEG aportar en áreas con altos niveles de requerimientos, como por ejemplo la Ciberseguridad?

El crimen cibernético ya representa uno de los puntos a tratar dentro de la agenda de gobierno en muchos países. Como entidad Gremial no podemos dejarlo como algo opcional; por ello, REDSEG a dado el primer paso.

Hemos conformado una unidad de ciberseguridad exclusiva para nuestros agremiados, con la finalidad que puedan recibir atención y apoyo entorno a Incidentes Cibernéticos y delincuencia tecnologica avanzada. También hemos creado un programa interno para la acreditación de empresas y profesionales que cumplan con las normativas internacionales en cuanto al aseguramiento de los sistemas y protección de sus clientes.

¿Cuáles son las vías de contactos para aquellos profesionales o entidades que deseen incorporarse a REDSEG?

Si desean conocer más sobre las actividades que organiza REDSEG, puede suscribirse sucribirse a nuestro portal informativo:Telegram.redseg.org

Si desea afiliarse como miembro: registro.redseg.org

Conocer sobre nuestros planes oficiales: planes.redseg.org

Si desea una atención personalizada puede escribirnos a la delegación chile: chile@redseg.org

Elio Caballero Sub director de REDSEG
Director delegación en chile

Caso de estudio y recomendaciones

Masacres en escuelas en Estados Unidos por ex estudiantes.

Me asiste la certeza de que la masacre ocurrida en una escuela primaria en el pueblo de Uvalde en Texas donde fueron asesinados 19 niños y dos docentes, cuenta con responsables en materia de seguridad. No hay duda de que se trata de una amenaza extrema con una probabilidad de recurrencia cada vez mayor de alta gravedad, la cual debe ser abordada bajo la óptica de la gestión de riesgos.

Las impactantes masacres que suceden en Estados Unidos pueden ayudar a comprender mejor la amenaza y las características de su ocurrencia desde la perspectiva del atacante.

El atacante de 18 años que hizo la masacre en la escuela se mudó en marzo pasado a la casa de su abuela en la localidad de Uvalde.

El asesino solía asistir a esta escuela primaria y, regresó con un rifle comprado legalmente al día siguiente de que sus compañeros se graduaran.

Los vecinos que lo conocen dijeron que se burlaban de él por su ropa y por la difícil situación financiera de su familia y que se lo consideraba un estudiante fracasado, que finalmente abandonó la escuela.

La masacre comenzó la mañana del martes cuando el asesino disparó en el rostro a su abuela y la hirió de gravedad, tomó su camioneta, se dirigió a la escuela, a las 11:28 abandonó la camioneta luego de salir armado con un rifle, y cerca de 1000 balas.

Comenzó a avanzar hacia la escuela a pie mientras disparaba a los ciudadanos que iban en su camino (algunos de ellos querían ayudarlo porque pensaban que había tenido un accidente automovilístico), a las 11:40 ingresó a la escuela sin interrupción, ingresando a una de las aulas donde se encontraban maestros y estudiantes inocentes en ese momento, y simplemente comenzó a dispararles sin piedad y sin emoción.

Alrededor de las 13:00 horas, un equipo de policías logró disparar al asesino y neutralizarlo.

En todo el tiempo entre las 11:40 y las 13:00 algunos de los estudiantes lograron esconderse de los ojos del asesino, algunos resultaron heridos por los disparos e hicieron todo lo posible para que el asesino pensara que estaban muertos, y algunos se acostaron encima de sus amigos heridos, para tratar de salvarlos de la muerte.

Niños de 8 a 10 años se encontraron en la escena de un brutal asesinato mientras veían a sus amigos muertos o heridos.

La policía de Texas informó que la escuela tiene un plan de seguridad, algunos de cuyos principios no se implementaron durante el período de tiempo que el asesino llevó a cabo la masacre, por ejemplo una puerta trasera quedó abierta y un guardia de seguridad no estaba de turno.

¿Puede ocurrir una masacre similar en nuestras escuelas?

La suposición del trabajo de la Secretaría de Educación de cada país debería ser que este tipo de masacres se pueden llevar a cabo en escuelas en cualquier país del mundo (es posible que este supuesto de trabajo ya exista).

Los hechos de la masacre en Estados Unidos, y en especial la masacre en Texas, deben servir como una alarma de alerta muy fuerte, que no se puede ignorar, y no se debe cometer el error de pensar de que, tal masacre no pueda que ocurrir en otro país.

Ya sera a nivel mundial, como en Estados Unidos, e independientemente de la política de venta de armas a civiles, un ex alumno frustrado puede decidir regresar a la escuela para vengarse mediante el asesinato de maestros y alumnos. Tal escenario considera suponer que un alumno local si podría llegar a una situación tan extrema.

Las instrucciones que tienen que llegar por parte de la división de seguridad del Estado relacionado con el ministerio de educación incluye los medios físicos y tecnológicos, la seguridad física, el método de seguridad y el método de supervisión y control, necesarios para verificar que la implementación en el campo cumple con la directiva.

¿Dónde está la amenaza de una masacre en la lista de amenazas relevantes para las escuelas?

La gestión de riesgos incluye dos parámetros para medir el nivel de disuasión:

1. La probabilidad de que se cumpla la amenaza y el nivel de daño si ocurriera.

El nivel de daño en el ataque a niños y estu-

diantes jóvenes e inocentes es muy claro, esto constituye un desastre a nivel nacional que sin duda causará una gran ¨shock¨ y muchos cambios inmediatos.

2. La probabilidad de realización se puede dar a diferentes interpretaciones - si bien se trata de una amenaza que se define como extrema y tal que muchos pensarán y dirán que "una masacre como ésta no sucederá en nuestro país", la probabilidad de su realización es más alto, que cualquier otro evento de masacre que ocurre en los Estados Unidos, por lo que sería correcto colocarlo en la parte superior de la lista de amenazas a las escuelas.

La posición de la amenaza en la lista de amenazas relevantes afecta el nivel de respuesta que se dará para enfrentarla.

¿Cuál es el daño en caso de una masacre escolar?

Nuestros hijos son lo más preciado que existe para nosotros en este mundo y no se pueden comparar con nada más preciado que ya hayamos logrado o que aspiremos a lograr. Por ejemplo las empresas financieras y información invierten sumas muy altas para asegurar el dinero, con la ayuda de medios tecnológicos avanzados y personal calificado: ¡los niños son mucho más "preciados" que el dinero!.

¿Cuáles son las acciones que se deben tomar en el marco de tiempo inmediato?

1. Una escuela debe definirse como una instalación segura: Un objetivo de protección único.

Dado que hay muchos tipos diferentes de escuelas, es importante realizar un análisis profesional que finalmente determinará la clasificación de cada escuela. La clasificación se define sobre la base de una serie de parámetros fijos, cuyo nivel varía según los datos y características de cada escuela individual.

2. Paquete de seguridad para cada clasificación:

Determinar con anticipación un paquete de seguridad de acuerdo al nivel de clasificación establecido para cada escuela.

Se debe determinar un paquete de seguridad básico para todas las escuelas y un paquete de seguridad extendido para aquellas que serán altamente clasificadas.

En una situación en la que los estudiantes corren el riesgo de sufrir daños, soy de la opinión de que una escuela primaria es más sensible que una escuela secundaria, principalmente debido al nivel de capacidad de reacción contra un agresor.

3. Un paquete básico para cada escuela:

A. Elaboración de un plan de seguridad.
B. Un fuerte cerco de metal de forma y altura que dificulte el paso de personas.
C. Colocación de señalización de seguridad en el cerco perimetral, complejo de entrada y salida con puertas que puedan cerrarse con llave y ser atendidos por un guardia de seguridad entrenado, en los diversos escenarios de amenaza y en varias ocasiones también armado.

4. Paquete de seguridad extendido: Consedera el paquete básico y adicionalmente:
A. Aumentar el equipo de seguridad con mínimo 2 guardias más.
B. Colocación de cámaras incluyendo cámaras de que pueden alertarnos.
C. Botones de emergencia-pánico.
D. Puertas de conexión entre aulas para permitir el paso en caso de emergencia.
5. Crear un centro de mando - observación:
Que tendrá la capacidad de observar cámaras y la capacidad de controlar, monitorear, y responder en una situación de emergencia.

Cooperación con las fuerzas de rescate: definición de la cooperación en seguridad con los distintos cuerpos y realización de ejercicios periódicos conjuntos, con el fin de practicar y mejorar el nivel de respuesta en caso de emergencia.

Como se mencionó, la masacre en Texas debe servir como una llamada de atención muy fuerte que no se puede ignorar y continuar como de costumbre.

Los tomadores de decisiones en el campo de la seguridad escolar deben darse prisa y tomar decisiones y revisar los supuestos de trabajo relacionados con la lista de amenazas y poder dar una imagen rápida y confiable del nivel de seguridad en las diversas escuelas del mundo.

Hay que implementar ahora todas las medidas necesarias para que niños y profesores no sean atacados en la escuela.

Nota: Esta crónica representa mi opinión, con la que, por supuesto, se puede estar de acuerdo o en desacuerdo, y además es posible que parte las acciones ya se haya implementado.

Guy Sadeh- Profesional con 22 años de experiencia en el campo de la Seguridad física y en el ejército Israelí, Jefe de operaciones en varias unidades del seguridad del estado Israelí. Consultor de Seguridad, especialista en protección -visible y encubierta, análisis de seguridad, seguridad escolar, etc.

HARP, una protección efectiva contra las grabaciones clandestinas

Ya sea empresas, corporaciones e incluso gobiernos, deben prestar especial cuidado a la posibilidad de que cualquier conversación privada o confidencial pudiera ser grabada de forma maliciosa. Hoy gracias a la tecnología disponemos de soluciones efectivas para neutralizar este tipo de riesgos. Presentamos a continuación una interesante crónica referida al sistema HARP, fabricado por la empresa Canadiense SANTOR, el cual nos ofrece una solución efectiva para afrontar este peligro potencial.

¿Cuál es la verdadera dimensión del problema de las grabaciones clandestinas?

Las empresas pierden billones por el espionaje industrial, según el FBI, cada año se pierden miles de millones de dólares, debido a casos de espionaje corporativo.

De estos incidentes, las grabaciones de audio son las más peligrosas, ya que son una prueba tangible de lo que alguien realmente dijo.

¿Se trata de un problema que ha ido en aumento?

Si, ya que hoy en día todo es un dispositivo de grabación: relojes inteligentes, teléfonos celulares, computadoras, dispositivos intelientes para el hogar (Alexa), grabadoras de voz, dispositivos ocultos… están por todas partes. Siempre le comentamos a nuestros prospectos que actualmente, si alguien quisiera grabar sus conversaciones confidenciales sin que elos lo supieran… podría hacerlo. Todos son 100% vulnerables a las grabaciones.

¿En qué porcentaje este tipo de situaciones afecta a empresas, corporaciones y gobiernos?

Es prácticamente imposible saber a ciencia cierta en que porcentaje estos se ven afectados por grabaciones de voz mal intencionadas, ya que muchas veces ellos no lo sabrán. Sin embargo, si sabemos que los operadores internos, empleados o personas de confianza, son responsables del 85% de los delitos cometidos, algunas veces de manera inintencional. Por esta razón, hace sentido agregar protección de voz a las otras capas de protección existentes como lo son las políticas y procedimientos, el control de accesos, detectores de metales y seguridad cibernética.

El HARP es la mejor manera que existe hoy en día para protegerse de grabaciones de voz clandestinas.

¿Todos los sistemas inhibidores son básicamente similares o existen diferencias notables en cuanto a su tecnología y capacidad?

HARP es la única solución que es actualmente considerada para gobiernos. Santor tiene años de experiencia ayudando a Gobiernos, presidentes de países y primeros ministros, presidentes de empresas y clientes corporativos a proteger sus secretos de estado, inteligencia empresarial, confidencialidad de reuniones, reputación de personas, a través de la reducción significativa de riesgos de grabaciones indeseadas y, de fuga de información.

Algunas personas pueden pensar que maquinas generadoras de ruido blanco pueden ayudar, pero realmente resulta contraproducente por que crean un falso sentido de protección.

Otro tipo de dispositivos en el mercado son poco efectivos, son muy ruidosos, poco estéticos y muy poco discretos. En cambio el HARP ofrece un nivel de protección muy alto a través de dos modos de protección.

¿Cuál es el factor diferenciador de estos sistemas?

Que son muy fáciles de usar e instalar. Puede ser utilizado para proteger conversaciones uno a uno en oficinas: reuniones entre miembros, conversaciones de cabildo, negociaciones internas debates entre socios, entrevistas de contratación y despido, negociaciones salariales, presentaciones de ventas, negociaciones de acuerdos confidenciales.

En salas de reuniones: conversaciones secretas o ultrasecretas, temas de seguridad nacional, reuniones de manejo de crisis..

¿Cuáles son los sectores con mayor demanda en esta materia?

El modelo con el que contamos actualmente con-

ocido como HARP https://santor.com/es/pages/harp-speech-protector-system es para uso exclusivo de gobiernos, militares, policías, grandes compañías.

Próximamente saldrá al mercado un modelo para consumidores HARP mini https://santor.com/es/pages/harp-mini-portable-protector-system

Después de años de proporcionar soluciones de contra-vigilancia a sus clientes, los profesionales de Santor reconocen que un barrido electrónico en busca de micrófonos escondidos, puede ser vulnerado inmediatamente por alguien con un dispositivo de grabación oculta.

Santor a través de HARP proporciona a los gobiernos, agencias, instituciones públicas y privadas y empresas vigilantes de todo el mundo una solución que reduce significativamente el riesgo de escuchas ilegales y grabaciones malévolas.

Mayores informaciones:
https://harp.santor.com/es/

El dispositivo HARP funciona para proteger no solo de micrófonos sino también de la escucha humana usando dos modos de protección:

(Modo Acústico) que produce una mezcla personalizada de voces audible, la cual, al ser más alta que la conversación sostenida, protege la misma contra escucha humana y grabaciones de diversos dispositivos. Esta protegida por una patente.

Modo Discreto (Ultrasónico), que emite un ruido apenas perceptible por el oído humano que afecta a los micrófonos que se encuentran dentro del área de protección impidiendo que estos puedan grabar las conversaciones.

Tribunal de Justicia implementa el VMS de Milestone Systems con análisis de vídeo

El Tribunal de Justicia del Distrito Federal de Brasilia, está utilizando su nuevo sistema de seguridad para prevenir que se escapen los acusados durante las audiencias,e identificar los posibles delincuentes que merodeen por sus instalaciones. Las analíticas de video inteligente tienen la capacidad de alertar rápidamente a las autoridades sobre posibles disturbios, para que la policía local pueda actuar e impedir una insurrección.

Desafío: garantizar la seguridad de los empleados y visitantes en los diferentes edificios

Revueltas, insurrecciones y fugas de acusados son riesgos que el Tribunal de Justicia del Distrito siempre ha considerado en sus planes de seguridad. Pero necesitaban de una solución más eficaz para monitorear los 30 edificios distribuidos en la capital federal, para proteger a los empleados y visitantes, y así garantizar la seguridad de miles de ciudadanos brasileños que utilizan los servicios de este órgano judicial. Asimismo, el Tribunal necesitaba de un sistema que ayudara con la identificación de delincuentes y la prevención de fugas.

Solución: sistema de videovigilancia escalable con análisis de video inteligente

El Tribunal de Justicia expandió y actualizó su infraestructura de seguridad existente con una solución integral, utilizando cámaras equipadas con analíticas de video inteligente (protección de perímetro, merodeo y búsqueda forense) de Axis Communications y Bosch, integradas al software de gestión de video (VMS) XProtect Expert de plataforma abierta de Milestone Systems, para facilitar el seguimiento, la prevención y la investigación de incidentes. Durante eventuales emergencias, la policía local ahora tiene acceso directo al VMS y a las cámaras.

Resultado: el monitoreo eficaz de los tribunales y otros edificios aumentó la eficiencia en las acciones de seguridad

El VMS de plataforma abierta de Milestone fue seleccionado en razón de una amplia gama de recursos disponibles, como la integración con cámaras de múltiples fabricantes, los dispositivos soportados, el soporte técnico y su excelente desempeño. El nuevo sistema de videovigilancia ayuda al personal de seguridad a mejorar tanto la prevención, como la optimización de las acciones frente a posibles situaciones de fuga de acusados, así como insurrecciones y la seguridad en las instalaciones.

Proporcionando justicia criminal para todo el Distrito Federal

El Tribunal de Justicia del Distrito Federal y Territorios (TJDFT), órgano federal perteneciente al Poder Judicial de la Unión, fue fundado en abril de 1960.

La institución atiende a todos los municipios del Distrito Federal, que actualmente cuenta con una población cercana a los 3 millones de habitantes. Su misión es proporcionarle a la comunidad acceso a la justicia y a la resolución pacífica de conflictos. El conglomerado reúne foros de las 33 regiones administrativas que componen el Distrito Federal, incluyendo Brasilia. Otros edificios también hacen parte del complejo judicial, como el almacén público, el área central de custodia para guardar armas y objetos de delitos, un museo, áreas médicas y una zona comercial.

Disuadiendo el crimen de manera proactiva con análisis de video inteligente

El TJDFT necesitaba un sistema de gestión de vídeo moderno que pudiera integrar los 30 edificios de los distritos judiciales de la capital federal, algunos de ellos localizados en áreas remotas. Además, el tribunal precisaba monitorear todas las unidades desde una ubicación centralizada. Era esencial garantizar la seguridad de las personas, los bienes y el propio sistema. Solo en el edificio principal, circulan alrededor de 5000 ciudadanos cada mes.

"Estábamos enfrentando diferentes incidentes como acceso no autorizado, personas con órdenes de arresto pendientes y hurtos", dijo Igor Martins da Silva, gerente titular responsable del proyecto en TJDFT. "La capacidad de visualizar imágenes y reaccionar al instante, o incluso antes de que ocurra un incidente, es una gran ventaja para contrarrestar estos desafíos", resaltó.

El sistema de vigilancia anterior del TJDFT c onsistía en cámaras analógicas conectadas a grabadores DVR independientes. El sistema desactualizado ,utilizaba equipos obsoletos y no proporcionaba integración entre los diferentes edificios.

La solución fue implementar un sistema moderno que cubriera todas las necesidades de seguridad del tribunal. El integrador del proyecto inicial fue el responsable de ofrecer el VMS de plataforma de Milestone, porque cumplía con los requisitos del TJDFT, además de ofrecer más libertad de elección, entre las tecnologías asociadas. También recomendaron cámaras con analíticas de vídeo de

Axis (modelos M1125, P1435, M3046, P5534-E) y de Bosch (modelos NBE-3502-AL, NDV-3503-F02) porque ofrecían los mejores recursos visuales y rendimiento. Ahora los 30 edificios se monitorean tanto desde su ubicación única, como desde un centro de comando centralizado.

La implementación de análisis de video inteligente ha optimizado enormemente la vigilancia en los tribunales y otras áreas internas. Según Martins da Silva, los análisis de perímetro, merodeo y búsqueda forense de Axis y Bosch son los que más se utilizan en el TJDFT. Con el sensor de movimiento habilitado en las cámaras y la respectiva configuración de filtros de movimiento, encontrar actividad sospechosa se hizo mucho más rápido. Si el sistema detecta algo inusual en las salas del tribunal, activa una alerta de "disturbios", para que la policía pueda tomar las medidas necesarias.

En los tribunales se juzgan toda clase de delitos, y existe el riesgo de intentos de fuga por parte de los acusados involucrados en estos juicios. El vídeo inteligente permite identificar rápidamente este tipo de situaciones y hacer que la policía intervenga para evitar una insurrección. El magistrado también puede activar un botón de pánico para activar la alarma en la central de monitoreo.

De igual manera los objetos que se dejan en las salas de los tribunales se pueden identificar de manera más eficiente, lo que reduce las situaciones peligrosas, como una bomba escondida en una bolsa, por ejemplo.

Las alarmas y la búsqueda forense brindan mayor agilidad en la respuesta a incidentes

La instalación del VMS de Milestone generó ahorros significativos para el TJDFT. Hoy es posible monitorear áreas mucho más grandes con menos cámaras y menos operadores.

En el pasado, las alarmas se activaban por teléfono, un proceso lento y complicado que exponía a empleados y visitantes. Con el nuevo sistema, es posible incluir analíticos integrados con los botones de pánico de la sala de audiencias. Estos pueden activarse inmediatamente a través del VMS de forma ágil y sencilla para una respuesta más rápida en casos de incidentes.

Cada edificio de TJDFT tiene su propio centro de monitoreo. La policía local realiza un seguimiento en tiempo real y responde a las emergencias. A su vez, todas las unidades de monitoreo están integradas en el centro de comando central, ubicado en la sede principal, que tiene acceso a imágenes y alarmas de todos los edificios.

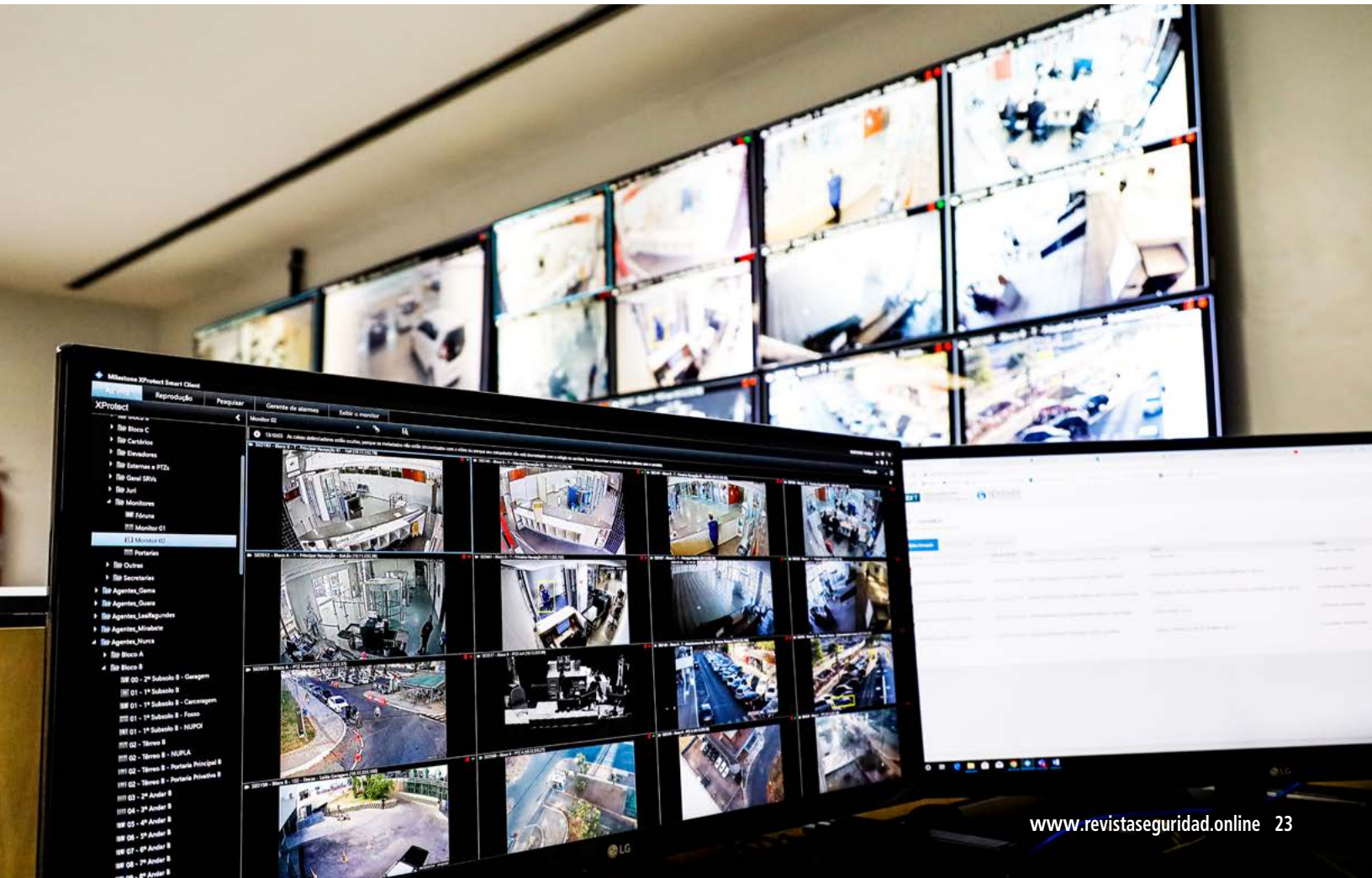
Al momento de ejecutar el control de acceso a los edificios, cuando una persona utiliza su número de identificación (CPF) para ingresar, el sistema indica si existe una orden de arresto en su contra. Si se encuentra una orden judicial, se activa una alarma en el sistema, y el equipo sigue el camino de esta persona en el edificio. La búsqueda forense analiza las características físicas y la ropa de la persona, para que las cámaras puedan encontrarla y rastrearla por al interior del complejo.

Mientras esta persona está siendo monitoreada, la policía se comunica con la agencia que emitió la orden de arresto, para determinar si aún es válida y si requiere acción. Desde la implementación del proyecto, esta función ha ayudado a las agencias del orden público a identificar, ubicar y arrestar a personas con una orden de arresto vigente.

Un sistema más eficiente, escalable y preparado para el crecimiento futuro

La implementación del sistema se llevó a cabo por etapas. Dado que el TJDFT es un órgano público, cada fase requirió un proceso de licitación. La policía judicial se encargó de elaborar la descripción del proyecto para realizar la licitación, los servicios y productos contratados.

Según Martins da Silva, la primera etapa se realizó en 2015. "Elegimos los edificios más críticos, grandes y con mayor flujo de personas para recibir



la nueva tecnología primero. En ese momento, actualizamos nueve edificios con la nueva solución de videovigilancia".

En 2017, el proyecto se expandió al resto de los edificios en la segunda fase. Para entonces, el contrato ya requería el uso del VMS de Milestone. Para la tercera etapa, en 2020, el TJDFT actualizó todas las licencias y amplió el servicio Milestone Care Plus, que brinda mantenimiento y soporte completo del producto.

Aproximadamente 1.174 cámaras, están instaladas en las áreas comunes, exteriores e interiores, especialmente en los espacios donde están retenidos los criminales.

El 80 por ciento de las cámaras son de Axis. Por ser el de mayor tamaño y con el mayor número de salas de audiencias, el edificio principal recibió la mayor cantidad de cámaras, con un total de 450. Los otros 29 edificios tienen entre 40 y 110 cámaras cada uno, dependiendo de su tamaño y necesidades específicas. El sistema es escalable y abierto, listo para manejar nuevas instalaciones e integraciones adicionales.

"Compramos nuestras cámaras en diferentes momentos según el costo, la funcionalidad y la garantía", dijo Martins da Silva. "Teníamos 30 edificios que usaban cámaras diferentes, por lo que necesitábamos estar seguros de que todas se integrarían en el sistema de gestión de video sin problemas".

La gestión de todos los foros del Distrito Federal se realiza en una máquina virtual, instalada sobre un servidor SQL. Sin embargo, las grabaciones de las imágenes se siguen haciendo localmente en cada edificio para evitar sobrecargar el almacenamiento.

Ubicada en el edificio principal, la sala de monitoreo cuenta con servidores más robustos y un videowall con 10 monitores de 47 pulgadas para visualización de imágenes. Los oficiales de policía monitorean el sistema las 24 horas del día con el apoyo del equipo de TI, si es necesario.

El personal que opera el sistema recibió capacitación sobre las funciones más utilizadas a diario: recuperación de imágenes, búsqueda, configuración de mosaicos y verificación de alarmas del sistema.

Actualmente, todos los edificios de TJDFT tienen instalado el VMS de Milestone y todos los edificios nuevos que se construyan en el futuro también recibirán la solución.

UTU

Simplifying Your Community Life

/utulatam

Plataforma de control de acceso inteligente

para empresas y comunidades

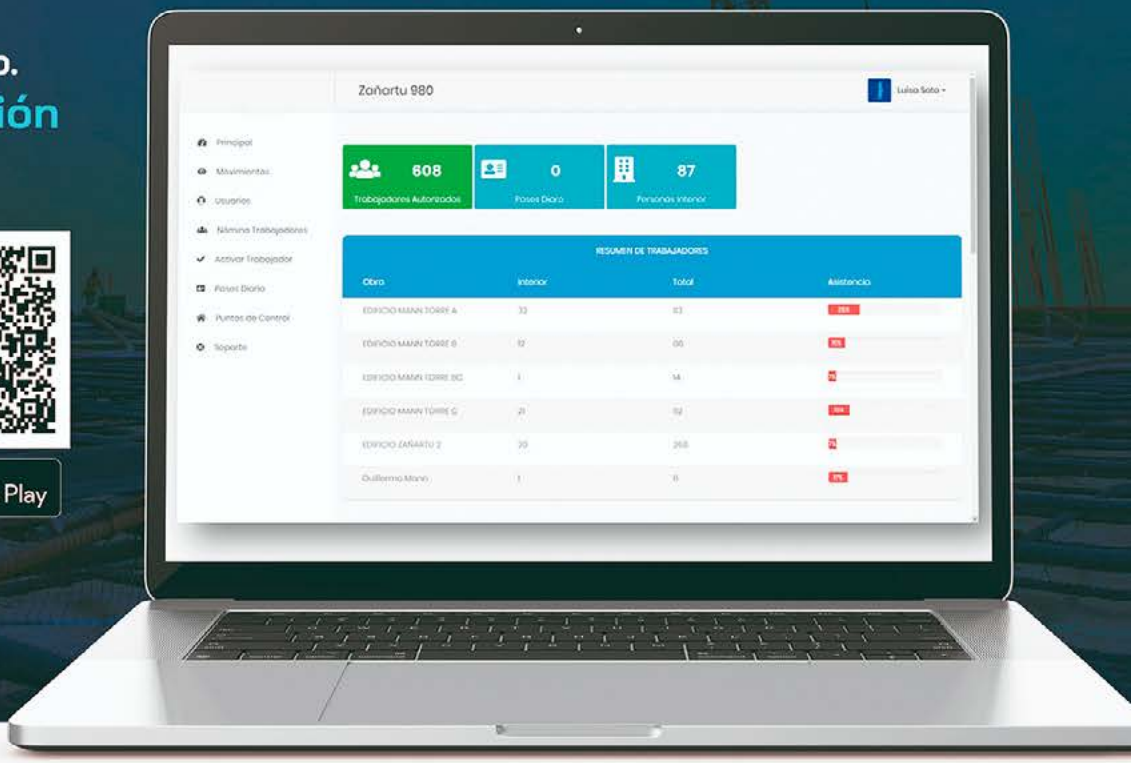
Utu es un sistema de gestión de control inteligente, que permite incrementar la productividad y el nivel de seguridad.

Escanee el código y descargue nuestra app.

Solicite su cotización y demo.

Available on the App Store

GET IT ON Google Play



Es seguro, es ágil, es simple.

utulatam.com

info@utulatam.com

Teléfono: +56 9 6618 0142

ZKTeco

Te esperamos en EDIFICA 2022

PABELLON 2 - STAND 2-E532

Teletrabajo

La importancia de implementar medidas de seguridad informática

Imagen de Ildefonso Linares en Pixabay

El teletrabajo se ha convertido en una práctica útil, eficiente y, sumamente necesaria para algunas empresas en el contexto actual. Si su compañía opera o planea operar de esta forma, debemos advertirle que hay reglas de seguridad informática que debe implementar, para evitar poner en riesgo su información personal, la de sus clientes o la de su empresa.

En las redes empresariales se almacena y distribuye información importante y confidencial relacionada con el negocio, como datos de clientes, contratos, y otra información sensible.

Las personas que accedan a esta red deben realizarlo desde dispositivos seguros y siguiendo protocolos de seguridad establecidos para poder garantizar la privacidad, seguridad e integridad de la información.

Cuando se teletrabaja los usuarios suelen acceder desde sus propios dispositivos desde casa, o ubicaciones externas a la empresa. En estos casos, si la empresa no controla la seguridad de estos dispositivos (ordenadores, portátiles, Smartphones o Tablets) se producirá una situación grave que pondrá en riesgo la seguridad.

Los principales riesgos de no controlar los dispositivos que utilizan los teletrabajadores son:

Robos de identidad (phishing), que permiten acceder a las plataformas y sistemas de la empresa a terceros no autorizados, que utilizan las credenciales robadas de los usuarios.

Infecciones por ransomware, un tipo de malware que encripta los datos de los sistemas informáticos impidiendo su funcionamiento (pidiendo un rescate en criptomonedas para liberarlos).

Robo de información. La fuga de información o robo de datos es otra de las mayores amenazas si no se cuenta con sistemas y normas para la seguridad informática.

Medidas de seguridad informática en teletrabajo
Para poder garantizar la seguridad del teletrabajo en informática, es importante establecer una serie de normas de seguridad informática y utilizar herramientas y protocolos seguros de acceso.

Las principales medidas de seguridad para el teletrabajo son:

Protección de los equipos de los usuarios

Los usuarios deben contar en sus equipos con sistemas de protección como antivirus o antimalware, que ayuden a evitar que este tipo de infecciones lleguen a producirse en sus equipos.

Los equipos y dispositivos de los usuarios deben estar siempre actualizados con la última versión del sistema operativo, incluyendo sus parches de seguridad. De esa forma se evitan vulnerabilidades que puedan ser aprovechadas por terceros.

Utilizar contraseñas seguras

La empresa debe implantar un sistema de creación de contraseñas sólidas y seguras para sus usuarios. Este tipo de contraseñas impedirá que sean averiguadas por terceros con el uso de herramientas específicas.

Acceso mediante conexiones seguras

El acceso a la red empresarial debe hacerse por parte de los usuarios desde una red segura. En este aspecto las redes VPN son una gran solución para controlar los usuarios que pueden acceder a las plataformas de la empresa, minimizando el riesgo de que acceda alguien no autorizado.

Otras medidas de seguridad informática para el teletrabajo:

También es importante que la empresa tome otra serie de medidas de seguridad para poder garantizar que el teletrabajo no ponga en riesgo la seguridad de la información los sistemas, como formación de los empleados en materia de seguridad, publicación de protocolos y políticas de ciberseguridad o proporcionar los dispositivos de acceso a los empleados, entre otras.

Para poder llevar a cabo el trabajo remoto desde casa o teletrabajo es importante priorizar la seguridad. Los usuarios que acceden a las plataformas de la empresa para realizar su trabajo representan uno de los mayores riesgos en ciberseguridad. Por eso es importante tomar una serie de medidas de seguridad informática para el teletrabajo que minimice riesgos y de las garantías suficientes para crear un entorno de trabajo seguro. Trabajar desde casa no debe significar que sus datos no estén protegidos de la misma forma que sucede cuando está en una oficina.

Entre las principales recomendaciones para mantener su información segura destacan:

Asegure las redes a las que se conecta

Navegar en una red de wifi pública desde un parque o una cafetería puede ser un riesgo para su información privada, desde sus cuentas en el banco hasta las fotografías que envía a sus amigos. En este sentido, le resulta útil una Red Privada Virtual (VPN por sus siglas en inglés), que crea una red privada partiendo de una red pública.

Esto significa que sus actividades en línea son encriptadas y su información personal o la de su empresa, no queda vulnerable.

Mantenga sus dispositivos actualizados

Las ventanillas y los avisos de actualizaciones a veces pueden ser molestas, y aun más cuando está en medio de algo importante desde su ordenador. En esos casos, aunque es tentador dar clic en la opción de "Recordar más tarde", no es lo mejor.

Posponer la actualización de sus aplicaciones puede provocarle problemas a largo plazo. Es importante que lo haga inmediatamente, como una forma de prevenir ataques informáticos en sus dispositivos.

Las actualizaciones se encargan de corregir errores en sus dispositivos, agregar nuevas características y, entre otras cosas, arreglar los huecos y debilidades en la seguridad informática que los hackers suelen aprovechar.

Tome las medidas necesarias en caso de robos o pérdidas

Estas situaciones pueden poner en riesgo su información y la de la empresa. Tras denunciar el robo ante las autoridades policiales, para aumentar su probabilidad de recuperar lo perdido, informe también a sus contactos y a su empresa sobre la pérdida.

Siempre que pueda hacerlo, trate de rastrear el dispositivo a través de las opciones que las diferentes marcas ofrecen. Esta información de seguimiento es vital para la policía. En caso de que el ladrón burle el sistema de bloqueo del dispositivo, usted debe entrar a los sitios web de las aplicaciones que usa, para cerrar las sesiones y cambiar las contraseñas.

Finalmente, si el dispositivo es irrecuperable, desactívelo. Aunque perderá contacto con él, evitará que el ladrón pueda acceder a sus cuentas o reutilizarlo.

Virtualice las aplicaciones

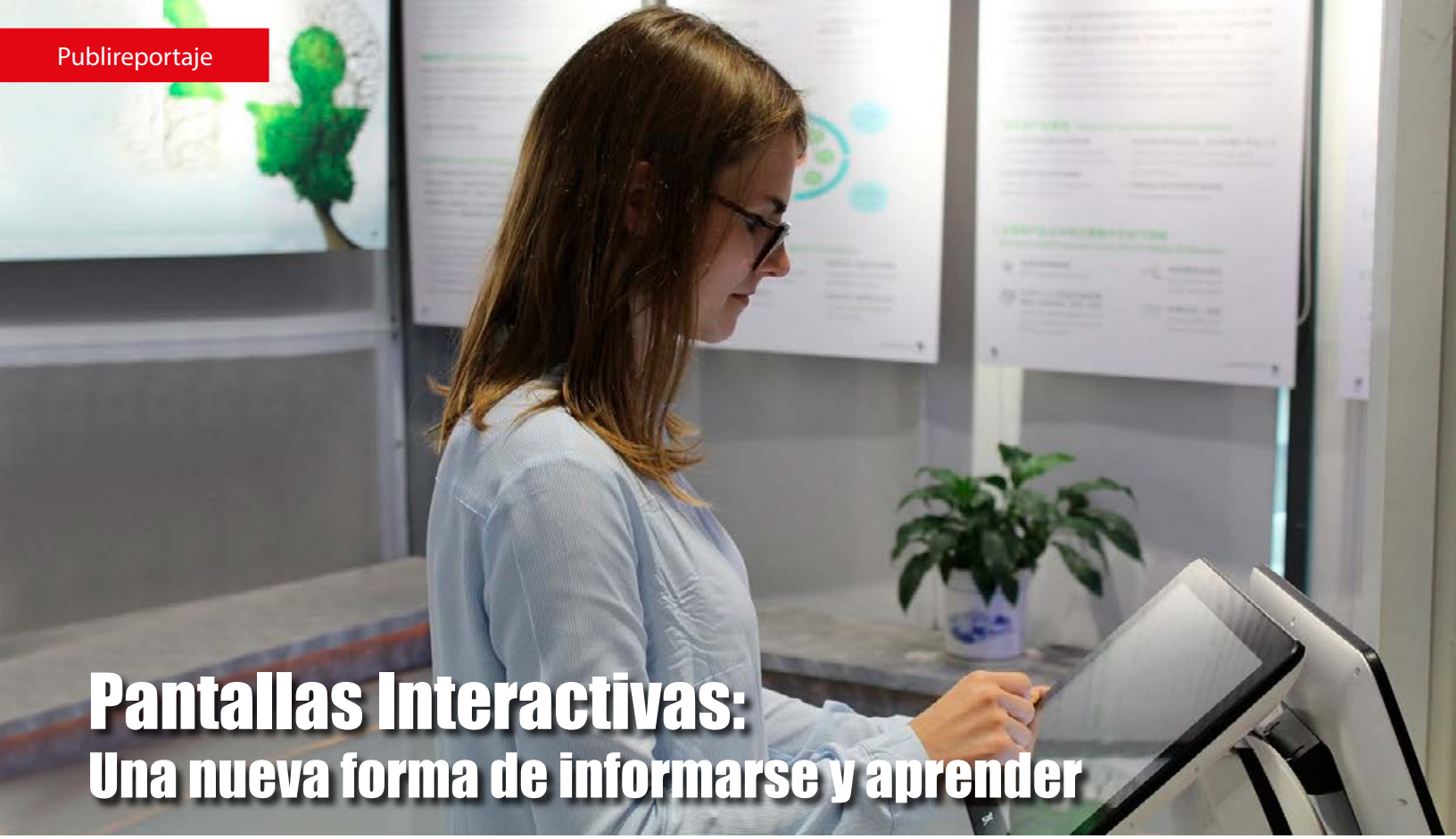
Con la opción de la virtualización de aplicaciones usted como usuario, es capaz de ejecutar en su computadora una aplicación que no está instalada en el equipo.
La aplicación es ejecutada gracias a un paquete que contiene las configuraciones necesarias. Con esta opción, tiene las herramientas disponibles en cualquier momento y el sistema operativo no será modificado.

Respalde sus documentos en la nube

Algunas empresas prefieren que los documentos y archivos de trabajo sean almacenados en una nube y no en un dispositivo. De igual forma deben tomarse medidas de seguridad informática para que la información ahí almacenada permanezca segura.

Podemos empezar por utilizar contraseñas seguras intercalando letras mayúsculas, minúsculas y números. También, puede activar una verificación, para que cada vez que quiera acceder a la nube, sea enviado a su celular un mensaje de texto que contendrá un código que deberá ingresar en el acceso a la nube.

Foto de Tobias Tullius en Unsplash



Pantallas Interactivas:
Una nueva forma de informarse y aprender

El nuevo nicho en el que se ha posicionado la empresa ZKTeco tiene como objetivo entregar información al usuario con alta calidad y altos estándares de seguridad con el mínimo contacto. Esto ya está siendo implementado en algunos recintos como establecimientos educativos, por lo que la tecnología debe ser de primer nivel para garantizar el proceso de aprendizaje, algo que la oferta de esta empresa cumple y con creces.

Pantallas interactivas táctiles con diversas funcionalidades para el despliegue de información, tótems inteligentes y otros dispositivos es una de las capacidades que busca posicionar en el mercado la empresa ZKTeco.

La nueva serie IWB de pantallas de ZKTeco cuenta con una serie de ventajas comparativas respecto a lo que hoy se dispone en el mercado como, por ejemplo, su alta calidad de imagen en 4K UHD con tamaños disponibles en 65", 75" y 86"; su arreglo de micrófonos para capturar fielmente el audio, su cámara frontal embebida de 13MP y además una capacidad de respuesta en fracciones de segundo para que quien observa pueda visualizar de manera instantánea lo escrito por el presentador o guía de un encuentro.

Así lo destaca Johebeth Pirela, product manager de ZKTeco, quien puntualiza que, "con funciones de dibujo a mano alzada, grabación de reuniones o clases con posibilidad de compartir automáticamente el contenido presentado, transmisión colaborativa inalámbrica de contenido y compatibilidad con la mayoría de las plataformas de reuniones digitales; este producto llega al mercado a servir como herramienta importante para la transformación digital de reuniones, capacitaciones, y otros diversos escenarios".

La experiencia de B2B Tech

La empresa de seguridad B2B Tech se constituyó el año 2015 buscando dar soluciones a empresas en esta materia, entregando además servicio de post venta que permitiera diferenciar su marca de las otras que hoy están disponibles en el mercado. A eso se agrega otra línea de trabajo que comenzó a ser explotada antes de la pandemia que es la Integración Audiovisual.

Jorge Mena, gerente de operaciones de B2B Tech, comenta que antes de la llegada del Covid 19 a Chile realizaron un showroom con una destacada empresa del retail en Chile "con proyectores, tres pantallas con proyección que se podían juntar o separar según necesitara el cliente".

Luego de la baja que significó en esta área la emergencia sanitaria en nuestro país y en el mundo, Mena explica que se está retomando con importantes resultados incluyendo establecimientos educacionales.

"Tenemos un cliente con contrato de mantenimiento donde tenemos un técnico de planta. Ahí revisamos toda la parte audiovisual, de redes y de seguridad. Todas las salas de clases tienen pantalla táctil que utilizan como pizarrón", puntualiza el ejecutivo.

A eso agrega que programaron una "cartelera digital que hoy se ve mucho. En puntos estratégicos del establecimiento se pasa información importante para los alumnos, los apoderados, lo que sea necesario".

Respecto al funcionamiento, Mena explica que se hace una programación, la misma que "hicimos con otra compañía con presencia en Chile y en otros países".

La tecnología busca ser un aporte no solamente en este tipo de compañías o recintos, sino también en restaurantes para dar a conocer su carta con el menor contacto posible, así como otros servicios que luego de la pandemia buscan mayores estándares de seguridad para ofrecer también a sus clientes.

Jorge Mena,
Gerente de Operaciones de B2B Tech

DATALAND: El resultado entre buenas alianzas tecnológicas

Dataland S.A nace en 1987 con el objetivo de entregar soluciones integrales al manejo y captura de información de manera personalizada, es decir, acorde a las reales necesidades de cada cliente. En simple, se adecúan a la realidad de las empresas y sus requerimientos.

Para posicionarse en el mercado y cumplir con las expectativas de los clientes su compromiso parte por invertir en desarrollos propios como los circuitos integrados DAT que permiten el destrabe de las puertas o los lectores portátiles de proximidad, así como también estar en permanente búsqueda de nuevas tecnologías que les permitan otorgar un servicio integral.

Para esta edición de Revista Seguridad conversamos con Delia Queirolo, gerente general de la empresa Dataland, quien lidera la mayoría de los proyectos enfocados en el control de acceso, uno de los servicios más requeridos en los tiempos actuales, como el solicitado para el proyecto El Soldado, una mina de cobre ubicada en la Cordillera de El Melón, comuna de Nogales, región de Valparaíso, a 125 kilómetros al norte de Santiago. Sobre esto nos cuenta: "nosotros hace varios años empezamos a instalar los torniquetes, las barreras y a hacer el link con su sistema de acreditación, existente, basado en tecnologia ZKTeco, para poder acceder a los datos y hacer las validaciones que corresponden para hacer un control de acceso. Con el tiempo esto ha ido evolucionando y es lo que estamos haciendo para personas, vehículos y conductores".

Además precisa: "ellos además de tener un control de acceso necesitan validar las acreditaciones y la forma es a través de torniquetes con lectores de cédula, y los vehículos en estos momentos con los LPR. En el Soldado ya tenemos instalado todo el equipamiento".

Por su parte, Jesús Sulbarán, ingeniero de preventa de de ZKTeco explica: "La empresa Dataland se decantó para este proyecto al implementar equipos de control de acceso peatonal de libre contacto como los son la línea SBTL6000 (puerta oscilante), quien aparte de contar con un diseño elegante y de funcionamiento estable, permiten una rápida gestión en su funcionamiento agilizando así el ingreso a la faena". Y agregó: "Adicionalmente para lo que es el control de ingreso vehicular implementaron los LPRS1000, nuestro tótem de reconocimiento de patente, el cual es de alta efectividad de lectura tanto de día como de noche y que funciona perfectamente bajos las inclementes condiciones ambientales a las cuales en dicho rubro son expuesto constantemente".

Para complementar Delia Queirolo enfatiza en las soluciones que entregan los productos de ZKTeco, "Para uno que lleva años en esto y ha visto tanto equipamiento puedo decir que los equipos son muy fáciles de trabajar, económicos y el soporte técnico que entregan es súper bueno y es muy importante. Me dan un respaldo muy importante, desde la compra al soporte posterior".

Delia Queirolo
Gerente General Dataland

"Dataland así como toda nuestra clientela contó con soporte y apoyo directo de nuestra parte al momento de la elaboración del BOM de este proyecto así como también se siente respaldado por el hecho de contar con un soporte de postventa y contacto directo con nuestra oficina para cualquier apoyo que lo amerite", puntualiza el representante de ZKTeco.

Integración de tecnologías para resolver desafíos:
La experiencia de Servitech y ZKTeco en Codelco

El servicio de hotelería en la minera estatal busca ser de primer nivel para otorgar la mejor experiencia a sus trabajadores. En ese marco, la compañía de seguridad Servitech, generó soluciones específicas que hoy la estatal busca replicar en otros campamentos en el país.

En la comuna de Diego de Almagro, en la región de Atacama, a unos 2.600 msnm. se ubica el yacimiento Rajo Inca, proyecto minero de Codelco, la principal empresa estatal de Chile y una de las mineras de cobre más importantes del mundo.

El proyecto que surgió como alternativa para potenciar y extender la vida de la última ciudad-campamento del país, El Salvador, requirió de la instalación de toda la infraestructura que permitió dotarla de los altos estándares que una compañía de carácter de clase mundial requiere.

Entre ellos está el servicio de hotelería para sus colaboradores, los que están sujetos a importantes desafíos diarios y por lo que la empresa busca entregar las mejores condiciones de confort para su descanso diario y espacio personal.

En ese contexto, la empresa Servitech Spa comenzó a entregar el servicio de acceso a las habitaciones para los trabajadores a través de varias soluciones, entre ellas, huelleros, lectura de Código QR de los carnet de identidad chileno, mediante la gestión en torniquetes de acceso.

Yeil Cedeño, gerente de Proyectos de Servitech Spa, explica que el trabajo tuvo varios desafíos: la distancia y el lugar para instalar sus sistemas, la elección idónea para el reconocimiento de las huellas dactilares de los trabajadores que están gastadas y/o secas por sus propias labores y la necesidad de la instalación de tecleras que digitan los números de identidad de cada uno de los funcionarios.

Cedeño plantea que "uno piensa que una teclera es algo relativamente sencillo. Pero para ese escenario en particular era necesario y no existía de la forma que se requería. Entonces, no sólo estaba el tema de la teclera como tal, sino que la integración con BioSecurity".

El diseño del sistema estuvo a cargo de Servitech que hizo coincidir las APP de ZKTeco en esta área, provocando un match tecnológico que significó generar una respuesta específica a un desafío planteado por la contratista a cargo del servicio de hotelería en el campamento de Codelco.

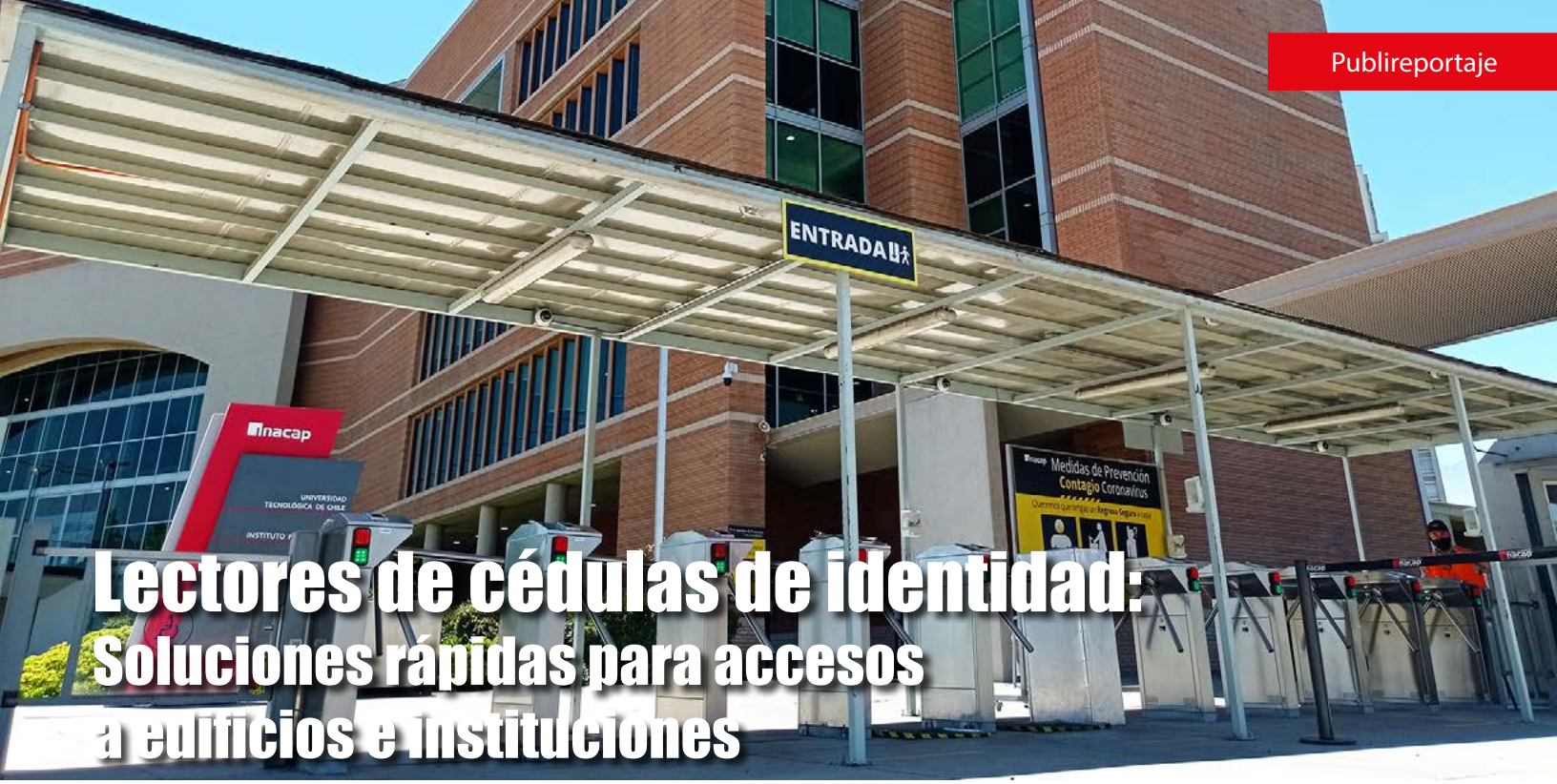
"El impacto para nuestro cliente que es el que administra estos hospedajes, fue un valor agregado importante. Porque si bien es cierto nosotros no desarrollamos, lo que hicimos fue facilitar las APP de ZKTeco para el caso de la integración con su software", explica el ejecutivo que destaca además la labor estética que se implementó con el servicio planificado y puesto en práctica junto a Ervin Balazs, socio de la empresa, a la hora de disponer del armazón, la estructura el conexionado y cableado que permiten el funcionamiento del sistema y la continuidad del mismo, además de facilitar su mantenimiento e inspecciones preventivas.

"La minería es un área muy importante en materia económica para Chile. Trabajar dentro de las faenas mineras es un privilegio y esto nos hizo ganar la confianza de este cliente. Esperamos que este tipo de implementaciones puedan extenderse y replicarse en distintos campamentos", concluye Cedeño.

Para este proyecto la empresa Servitech se decidió por los torniquetes automatizados de la línea Flap Barrier FBL4000 Pro, más conocidos en el mercado como Ala de Ángel, ya que necesitaban un equipo que posterior se realizara la autorización de acceso del usuario, fuera de rápido accionar, con excelente estabilidad de trabajo, rápido flujo de paso, y una correcta gestión. Esto de la forma más automatizada y con un diseño estético innovador

Yeil Cedeño,
Gerente de Proyectos de Servitech

Torniquetes automatizados
línea Flap Barrier FBL4000 Pro



Lectores de cédulas de identidad: Soluciones rápidas para accesos a edificios e instituciones

Juan Carlos Ríos, gerente general de Ingeniería y Soporte de una empresa de seguridad electrónica, destaca el nivel de las tecnologías que dispone ZKTeco que le han permitido dar respuesta a una demanda que va en aumento y ya está operativa en varios edificios y entidades públicas y privadas en Santiago.

Aumentar los protocolos de seguridad de manera confiable y con el menor contacto es parte de las exigencias que enfrentan las compañías que proveen este tipo de soluciones de seguridad electrónica en diferentes espacios como condominios, edificios e instituciones públicas y privadas.

Así lo reconoce Juan Carlos Ríos, gerente general de Ingeniería y Soporte Técnico Juan Carlos Ríos EIRL, empresa que recibe como requerimiento permanente el que dispositivos que de forma rápida, pero a la vez efectiva, sean capaces de lograr la lectura de cédulas de identidad para el acceso de personas. Tanto las nuevas con QR como las antiguas con código de barra, debido a que la vigencia de estas últimas se extendió debido a la pandemia.

"Cada día más nos están pidiendo la lectura de carnet para agilizar los accesos de visitas en los edificios", comenta el ejecutivo quien agrega que "es una mezcla de poder hacer un mayor control por el tema del COVID 19 para el ingreso a los edificios y por un tema de seguridad. El tema de seguridad en algunas instituciones empieza a ser mucho más importante para tener una validación para saber quién está en el edificio, quién visitó el lugar en ciertos periodos".

Ríos precisa que "si bien el código QR de la cédula tiene sus bemoles, pero es una forma rápida de poder validarlo. Porque la otra forma que la gente la encuentra que empieza a ser poco rentable, es pasarle tarjetas. El problema de la tarjeta es que el usuario muchas veces no la devuelve o pierden la tarjeta".

En este proceso de implementación de dispositivos que entreguen una solución integral a esta demanda, Juan Carlos Ríos destaca la oferta que entrega ZKTeco desde el diseño hasta el soporte final para el desempeño del producto.

"Lo que siempre he valorado de ZK es que tienen un muy buen soporte frente a algunos problemas.

Ha sido un muy buen match en cuanto a la rápida implementación de la interfaz que ellos tienen. No hay que hacer grandes configuraciones como con otros sistemas que leen cédulas, y el soporte que han brindado frente a dificultades que hubo al inicio", precisa Ríos.

Otro elemento que destaca es la facilidad para el proceso de instalación y su rápida operatividad. "El match es que tú simplemente lo conectas a laentrada Wiegand (o de datos) de cualquier controlador y estás leyendo en forma inmediata la cédula de los usuarios.
No es necesario hacer grandes cambios ni de hardware ni de software", sostiene.

Ríos puntualiza que "la flexibilidad que nos está dando ZK para el producto que tienen de lector de cédulas, es bastante bueno. Incluso, si necesitas una configuración especial, está el soporte local para hacerlo y no como con otros equipos que se deben integrar partes de distintos fabricantes para llegar a hacer la conexión. Es muy rápido".

A esto agrega que "el nivel de los equipos es bastante bueno. Hoy tenemos dos cosas importantes, una la disponibilidad a través de distintos canales de los equipos y la calidad de los equipos son buenos".

El ejecutivo señala que hay ya varios edificios de Santiago donde se está ocupando esta tecnología, entre ellos en los ingresos de INACAP de Santiago Sur y Apoquindo.

"En los accesos de visitas también nos están pidiendo ese tipo de verificación, personas que no tienen registrada, que no tienen validada, que se registren como visita con su cédula", concluye.

Johebeth Pirela, Product Manager de ZKTeco, "la biometría forma parte de la esencia de ZKTeco como desarrollador de soluciones de control de acceso; sin embargo, nuestros dispositivos permiten diferentes tipos de verificación, dándole al integrador y al usuario final la posibilidad de utilizar la tecnología que más le convenga. Por lo mismo, la lectura de carnet de identidad, ha sido unos de los requerimientos post pandemia que se estableció, por su fácil implementación y por otros beneficios indirectos asociados, como exigir a que los usuarios porten consigo en todo momento su identificación. Y estos se puede complementar al mismo tiempo con otros como es el reconocimiento facial cual de igual manera no requiere contacto y su enrolamiento se puede realizar mediante una selfi", precisa.

ZKTeco, como empresa con sede en Chile, y enfocada en solucionar las necesidades del mercado local se encarga de personalizar el lector QR-500 para poder entregar una solución fácil y accesible,

con soporte a los distintos formatos de identificación aún utilizados en el país: PDF417 y Micro-QR. Y lo mejor es que no requiere adaptadores ni conversores ya que la información es entregada de forma directa en un protocolo estandarizado por el mercado llamado Wiegand, en formato de 34 bits, el cual es un estándar en paneles de control de accesos y equipos de automatización.

Tecnologías Biométricas de ZKTeco

Permiten reconocimientos seguros, efectivos y rápidos

Los avances implementados en dispositivos con tecnologías Visible Light y Computer Vision, ayudan a mejorar los tiempos de reconocimiento de las personas que ingresan o transitan en un recinto, generando un mayor control y seguridad para las comunidades, instituciones y empresas que los utilizan.

Disminuir los tiempos de acceso a los recintos, especialmente en las empresas, es uno de los desafíos de seguridad que busca resolver la tecnología desarrollada por la compañía ZKTeco a través de dispositivos que cuentan con importantes herramientas biométricas y múltiples métodos de verificación.

Pablo Domínguez, Product Manager de la compañía, explica que hay dispositivos que incluso permiten tres tipos de identificaciones simultáneas que evitan el contacto (Rostro, Palma o QR), en el menor tiempo posible y que otorga altos estándares de seguridad y control.

"La tecnología de Visible Light que nosotros estamos desarrollado desde hace bastante tiempo, más de tres años, justamente fue una de las tecnologías que permitió producir los dispositivos con medición de temperatura y detección de cubre boca, ya que la tecnología de reconocimiento facial es mucho más precisa, proactiva, con tecnologías de aprendizaje reconocimiento profundo para el reconocimiento de rostros, como se llama", precisa.

Por ejemplo, señala que "esta tecnología permite diferenciar rostros falsos como una fotografía o un video de la misma persona. Aunque la persona esté enrolada, esta tecnología es capaz de diferenciar de estas imágenes 2D, diferenciarla de un rostro 3D o rostro vivo".

Domínguez subraya que la tecnología ha ido evolucionando en los últimos años. "Ya hemos mejorado esta tecnología en cuanto al reconocimiento facial. Hoy existe Visible Light 3D estructurada que es una tecnología que aumenta la capacidad de identificación de rostro vivo en el sentido que aumentamos las matrices de puntos de laser. El rostro tiene aproximadamente 80 puntos nodales; distancia entre los ojos, profundidad de cavidad ocular, ancho de la nariz, forma de los pómulos, longitud de la mandíbula. Éstos los medimos en base a miles para poder detectar de forma mucho más precisa un rostro vivo 3D".

Por otra parte, el ejecutivo comenta que "también hay una mejora en desempeño bajo ambientes poco luminosos. La última tecnología que ha aplicado ZK en esta tecnología tiene que ver con la tecnología Dual Spectrum (DS) que permite trabajar en ambientes con poca luminosidad tan baja como 0 lux que es prácticamente casi oscuridad total, permitiendo trabajar en ese ambiente extremo y hacer la identificación correcta de las personas".

Incluso, señala que hay productos que reconocen dos y hasta cinco personas simultáneas como la línea FaceKiosk, tecnología que podemos encontrar tanto en equipos de control de acceso como en otros de tiempo de asistencia.

"Esta tecnología ha ido reemplazando a la anterior que se denominaba reconocimiento facial de infrarrojo cercano, la cual es nuestra tecnología base que tienen nuestros productos de reconocimiento facial de las primeas generaciones y que todavía se encuentran en producción en clientes finales. Toda la tecnología Visible Light ha ido reemplazando estos modelos antiguos que han ido reemplazándose paulatinamente", puntualiza.

Esta tecnología "es la más utilizada al día de hoy, sobre todo, después de la pandemia, puesto que es una solución rápida, precisa, más segura en cuanto a controles de acceso. Y en eso, el reconocimiento facial ha sido uno de los que ha prestado la mayor seguridad y rapidez en cuanto a permitir o denegar ingresos".

Por otro lado, esta tecnología contempla un enrolamiento de las personas incluso de manera remota. "Esta tecnología de Visible Light permite el enrolamiento con un dispositivo; un enrolador externo USB que existe para hacer enrolamiento remoto y también el enrolamiento a través de una fotografía cumpliendo con ciertas características,

ésta última permite enviar esta información a través del software de gestión hacia el dispositivo el cual genera la plantilla 3D o una plantilla biométrica facial para hacer un reconocimiento correcto de la persona".

Palma 3 en 1

A la tecnología anterior, ZKTeco suma la de reconocimiento de la palma de la mano que tiene como características que no requiere el contacto de la persona con el dispositivo y hace una identificación de tres elementos de la mano: su forma, su huella y de las venas que están debajo de la piel.

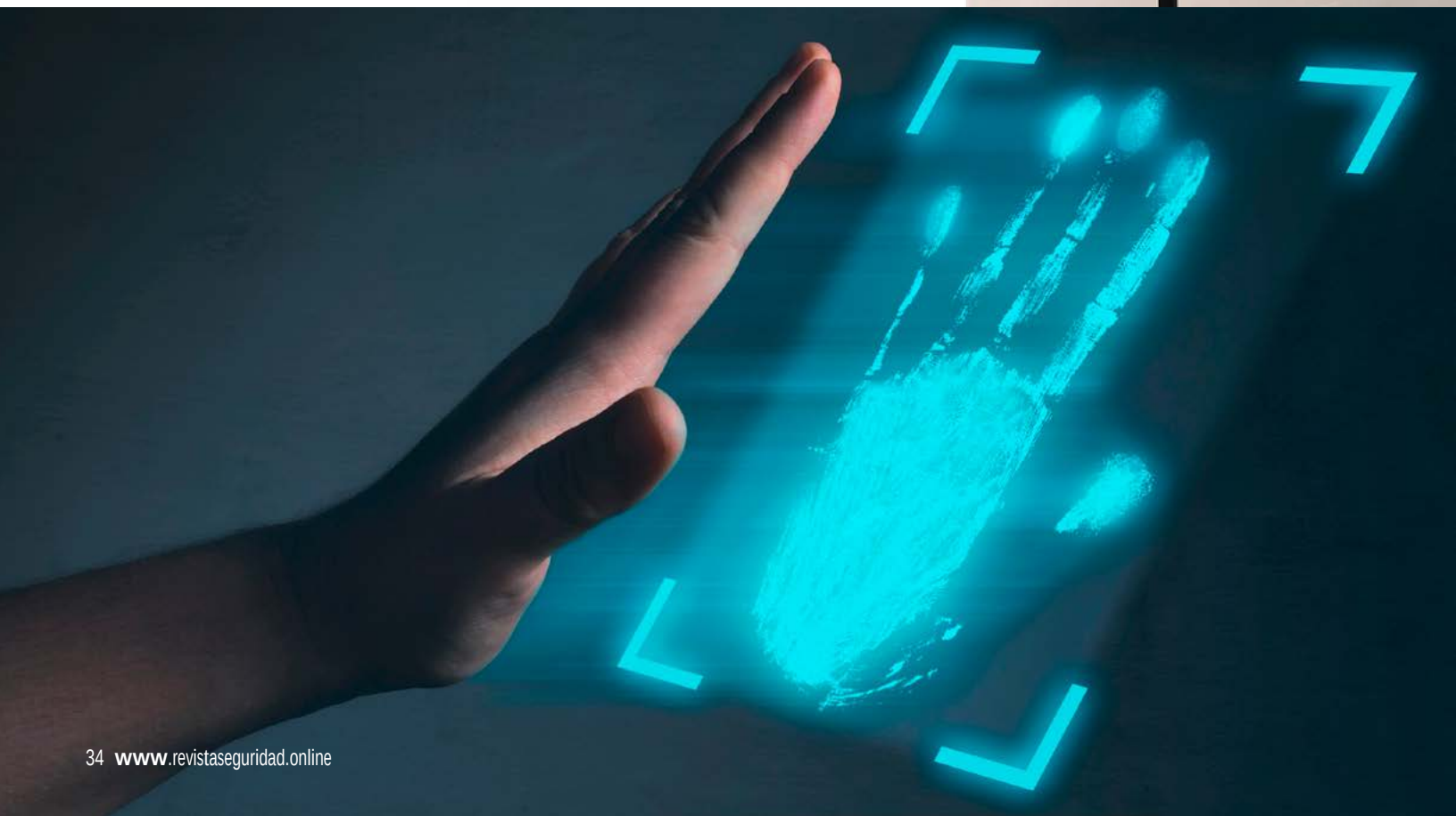
"Es una tecnología de Computer Vision . Esta es una de las tecnologías que está siendo más utilizada junto con la de reconocimiento facial. Es una tecnología que logra tener una seguridad mucho mayor ya que valida tres elementos de la mano para hacer una validación correcta: la forma, la imagen de la mano; la segunda es la huella o impresión de la palma de la mano; y luego con los infrarrojos activos que tiene esta tecnología es capaz de hacer un reconocimiento de las venas que están bajo la piel. Con estos tres indicadores hace un match".

El sistema permite el reconocimiento biométrico en un tiempo de menos 0,35 segundos y además tiene una distancia de visión entre los 30 y 40 centímetros junto con una tolerancia al ángulo del eje de la mano más o menos de 60° .

"Esta tecnología está presente en todos los equipos que tienen Computer Vision y permite contar con estas dos soluciones juntas. Incluso en algunos dispositivos, con la misma tecnología permite tener la lectura de QR estándar en el mismo dispositivo, con lo cual los dispositivos al día de hoy permiten tener estas tres tecnologías con las mismas cámaras o los mismos sensores", afirma Domínguez.

El Product Manager de ZKTeco explica que "los equipos que tienen Computer Vision y Visible Light cuentan con reconocimiento facial, tienen la tecnología de palma 3 en 1 y pueden contar con la lectura de QR tanto fijo como dinámico como estándar en el mismo dispositivo. Eso permite tener soluciones mucho más seguras ya que podemos ocupar las tres tecnologías para hacer una identificación, a distancia, sin contacto y permite una verificación mucho más rápida, precisa y segura".

En la actualidad, este tipo de tecnologías se están utilizando en edificios corporativos, casinos e instituciones de salud, generando mayores condiciones de control y seguridad para las empresas.



ZKTeco cierra exitosa participación en Expo Vivienda 2022

La empresa especialista en seguridad dio a conocer una amplia gama de soluciones para viviendas particulares y condominios, entre ellas circuitos cerrados de televisión auto instalables, cerraduras inteligentes y controles de acceso a comunidades.

Más de 6 mil visitantes tuvo la Expo Vivienda 2022 que se llevó a cabo entre el 26 al 28 de agosto en el Centro Cultural Estación Mapocho donde además se dieron a conocer diferentes proyectos que van desde las mil a las 10 mil UF, con o sin subsidio habitacional.

En el encuentro participó la empresa ZKTeco que dio a conocer una serie de alternativas de seguridad y productos IoT auto instalables, ocupando para ello la más amplia gama de dispositivos y soluciones tanto para proyectos en su etapa inicial como también para edificios, condominios e incluso para viviendas unitarias.

Johebeth Pirela, product manager de ZKTeco, señaló que el evento desarrollado entre el viernes 26 y el domingo 28 de agosto, "fue muy buen espacio para mostrar soluciones a clientes finales dentro del mismo rubro, inversionistas o aquél que está buscando su primera vivienda, y encuentra algunas soluciones adicionales. Tuvieron contacto con nuestra tecnología y en ella encontraron una solución algunos problemas básicos, como la seguridad basada en la autogestión".

Entre los productos más consultados estuvieron los kits de cámaras, sistemas de control a través de alarmas, cerraduras inteligentes, control de acceso a condominios y dispositivos de lectura de patentes en el caso de edificios.

Además, explicó "se acercó mucha gente relacionada al rubro de arriendos por períodos cortos, a través de plataformas web; en su mayoría propietarios de varias viviendas, quienes se interesaron por las cerraduras inteligentes y los beneficios que estas les podrían entregar, como la facilidad de controlar y limitar de forma remota el acceso a las mismas".
Entre otros, hubo "varios administradores de condominios que mostraron interés por el control de acceso, los torniquetes, las cámaras de lectura de patentes, etcétera; soluciones que facilitarían las labores de control en varios de los condominios con los cuales trabajan".

Para el representante de ZKTeco, esto demuestra que los productos y soluciones que ofrece la empresa apuntan a diferentes requerimientos del mercado lo que permite a la compañía seguir gestionando alianzas con emprendimientos y participar de los más variados encuentros para dar a conocer su propuesta con la mayor gestión tecnológica como de post venta.

Total Pack:, Soluciones que extienden la vida útil de la tecnología

La compañía cuenta con el conocimiento y el desarrollo de propuestas para diferentes tipos de necesidades las que junto a la tecnología de ZKTeco apunta a entregar los más altos estándares que se han traducido en confianza e incluso reducción de costos en esta área en servicios públicos y privados.

Soluciones para diferentes necesitades son las que entrega la empresa Total Pack, compañía con 30 años de presencia en el mercado y que desde hace 15 trabaja con productos de seguridad de la empresa asiática.

Manuel Pavez, gerente de Ventas de Total Pack, destaca que el elemento diferenciador de la empresa con el resto de quienes ofrecen de este tipo de servicios está en el seguimiento para otorgar una extensión eficiente de las tecnologías en las que invierte un cliente. Y en eso tienen experiencias donde lectores biométricos, por ejemplo, cuentan con cerca de diez años de funcionamiento y mantienen el mismo nivel de seguridad que al comienzo de sus operaciones.

"La diferencia está en el servicio, en el conocimiento de la marca y cómo mejor utilizar el producto para que sea de más provecho para el cliente. Nosotros nos hemos capacitado en los productos al nivel que somos capaces de recomendar una solución en particular en vez de otra", explica Pavez.

Al respecto, comenta que la tecnología que utilizan puede ser implementada tanto para la identificación de un TAG en el caso de camiones que acceden a un centro de distribución y que tiene su placa patente en cualquier lugar, mientras que en el caso de los vehículos de un edificio residencial puede ser instalado para que permita el acceso reconociendo su patente.

"Nosotros hemos sido capaces de especializarnos en el producto de la marca para poder prestar una asesoría integral a los clientes que les permita tomar una solución con más confianza", precisa el representante de Total Pack.

Entre las experiencias, Pavez comenta que fueron convocados para entregar solución a la seguridad de acceso al edificio del Ministerio de Desarrollo Social, en el cual instalaron torniquetes de ingreso para los funcionarios de esa repartición de gobierno, control de acceso a oficinas interiores, control de visitantes y también para el ingreso de vehículos al recinto.

A eso suman la implementación de tecnología de acceso a bibliotecas en recintos del barrio universitario en la comuna de Santiago, lo que se tradujo incluso en una mejor utilización de recursos humanos como de mantención y de guardias.

"Tenemos solución de acceso en el barrio universitario donde las personas que ingresan a las bibliotecas son solo estudiantes. Ya no entran vendedores ambulantes, los tipos que andan en la calle a los baños, ya no entra gente que va a vender drogas", subraya el ejecutivo.

El gerente indica que "según datos de las mismas universidades, el nivel de robos declarados bajó en un 80% y los contratos de servicios lograron ser más eficientes producto de que ya no entra gente externa, por lo tanto, los espacios comunes se logran mantener aseados y las posiciones de los guardias no son requeridas en espacios donde se sabe que hay solo estudiantes".

Para el representante de Total Pack, lo importante es "convertirme en un partner del cliente porque, por ejemplo, una solución para un estacionamiento no necesitas que te la instale y desaparezca: necesitas que la instale, haga que opere y que esa operación se mantenga sin problema en el tiempo", para lo cual además establecen un servicio de mantención periódica que permite asegurar la extensión de la vida útil de la tecnología".

Por su parte, Pablo Domínguez, product manager de ZKTeco, indica que "la flexibilidad y las herramientas existentes, para desarrollos e integraciones, que brindan los productos y soluciones de ZKTeco, entregan diversidad de oportunidades a los integradores, como es el caso de Total Pack

Manuel Pavez
Gerente de Ventas de Total Pack

de poder entregar soluciones a medida a sus clientes".

Junto con las más modernas y seguras tecnologías biométricas, existen herramientas para desarrolladores, como utilización de SDK para desarrollos de softwares personalizados con todo lo necesario para que los programadores se dispongan a trabajar y a crear, dando rienda suelta a la imaginación, y pudiendo cubrir a cabalidad lo que los clientes requieran.

Otra herramienta, son las Web APi que proporcionan algunos softwares, tanto en control de acceso, como en control de asistencia, las cuales permiten realizar de forma un poco más limitada, integraciones desde o hacia plataformas existentes.

El representante de ZKTeco enfatiza: "Total Pack, junto con realizar implementaciones con soluciones estándar nuestras, ha logrado implementar soluciones a medida, con algunos requerimiento particulares o especiales, que en ocasiones las soluciones estándar no logran entregar a cabalidad".

Así es como cobra gran importancia, lograr estas alianzas de apoyo, para lograr las sinergias suficientes antes problemáticas y requerimiento de muchos clientes en particular.

Pablo Domínguez, product manager de ZKTeco, indica que "la flexibilidad y las herramientas existentes, para desarrollos e integraciones, que brindan los productos y soluciones de ZKTeco, entregan diversidad de oportunidades a los integradores, como es el caso de Total Pack de poder entregar soluciones a medida a sus clientes".

Comunicado Oficial Seguridad Expo 2022

SEGURIDADEXPO by Fisa | CHILE

Estimados socios, colaboradores, patrocinadores y clientes,

Seguridad Expo ha sido el principal evento internacional del sector en Chile, superando los 15.000 M2 de exhibición, ha convocado a más de 30 mil visitantes en sus 6 versiones, y sobre los 300 expositores y 2.000 marcas representadas. Han estado presente todos los líderes en los rubros de Seguridad pública y privada, Seguridad industrial, laboral y bioseguridad, fuego y desastres naturales; lo que ha permitido que se posicione como la gran feria de la industria en nuestro país.

Fisa del Grupo GL events – Organizador de SeguridadExpo, agradece su participación y apoyo incondicional y les informamos que hemos decidido realizar ciertas modificaciones en el formato de Seguridad Expo 2022.

Estos cambios que obedecen a una profunda reflexión con los principales actores del sector, nos permiten definir lo siguiente:

Seguridad Expo se realizará del 3 al 5 de octubre 2023 en Parque Fisa, convocando a más de 200 empresas nacionales e internaciones de los principales sectores de seguridad, emplazadas en 20.000M2 de exhibición, con un amplio programa de actividades, como: ejercicios combinados y demostraciones, jornadas de ruedas de negocios, workshops y un Congreso Internacional con los principales referentes del sector, quienes abordarán las problemáticas locales y mundiales en esta materia; sumado a un robusto plan de visitantes.

No obstante, el día 13 de diciembre del presente año, realizaremos "Summit SeguridadExpo" en el Centro de Convención Metropolitan (Ex CasaPiedra), el cual será la antesala de la Feria de Octubre 2023. En un solo día se realizará un Congreso Internacional acompañado de un almuerzo Oficial, espacio de camaradería, networking y una exhibición para las empresas participantes ya comprometidas a la fecha (2022).

Esperamos seguir contando con su importante participación, para entre todos fortalecer las oportunidades comerciales, instancias de encuentro y debate de la seguridad en Chile.

DEEPFAKE
Una amenaza creciente

Foto de John Noonan en Unsplash

Los expertos en seguridad cibernética comparten su visión sobre cómo las empresas pueden protegerse contra un riesgo creciente. El Deepfakes está exponiendo las brechas de habilidades de seguridad cibernética de las empresas. El crimen deepfake es un peligro real y presente para las empresas.

El año pasado, solo a un banco le costó $35 millones en una sola estafa, sin embargo, muchas empresas aún ignoran los riesgos, en parte gracias a la falta de habilidades de seguridad cibernética a nivel de liderazgo.

Con la tecnología Deepfake cada vez más sofisticada, y fácilmente disponible para los delincuentes, las empresas deben ver la tecnología como una amenaza actual y no como una preocupación futura.

Comprensión de la amenaza Deepfake

A diferencia de las amenazas de seguridad cibernética establecidas, por ejemplo, malware, y piratería de bases de datos, los deepfakes aún son fáciles de descartar de las estrategias de seguridad cibernética.

Se trata de una tecnología relativamente nueva, su introducción como un divertido fenómeno de vídeo viral no ha dificultado que las empresas se percaten de la gravedad de la amenaza que ahora representa esta nueva modalidad para la seguridad. Sin embargo, han surgido varios casos de alto perfil en los últimos años, que ilustran cuán peligroso puede ser Deepfake.

En 2019, un director ejecutivo con sede en el Reino Unido, fue estafado para que transfiriera 243 000 dólares a un actor malicioso, gracias a la avanzada tecnología de voz Deepfake que lo convenció de que estaba hablando con el director ejecutivo de su empresa matriz.

Los diferentes tipos de Deepfake que se sabe que se utilizan actualmente contra las empresas incluyen fraude fantasma (donde el delincuente roba la identidad de una persona fallecida), imitación de identidad (como los ejemplos anteriores), fraude de cuenta nueva y fraude de identidad virtual (donde los delincuentes 'crean' una nueva identidad mediante la combinación de información e imágenes de varias personas).

Destacando las crecientes preocupaciones a nivel gubernamental, el FBI emitió el año pasado una severa advertencia sobre los peligros de Deepfake en un informe de seis páginas, mientras que el Programa Nacional de Inteligencia Artificial de los EAU y el Consejo para el Bienestar Digital emitieron una guía, para aumentar la conciencia pública sobre la seguridad. amenaza.

Cómo los equipos de seguridad cibernética deben responder a Deepfake

Si bien la tecnología está a la vanguardia de la lucha de la mayoría de las empresas contra el delito cibernético, no existe ningún software o sistema que las empresas puedan "comprar" para proteger su negocio contra las amenazas de Deepfake.

Si bien son una preocupación de seguridad cibernética, su preocupante incremento se debe a lo que podemos definir como un "error humano" por falta de verificación.

En la actualidad, la mayoría de los Deepfakes incorporan señales reveladoras de que algo no está del todo bien, con una llamada o un vídeo si sabes qué buscar, pero estas tecnologías se están volviendo más sofisticadas.

Resulta fundamental de seguir avanzando en su prevención. Tener las habilidades adecuadas de seguridad cibernéticas en su negocio, tanto a nivel de soporte como de liderazgo, es la mejor manera de asegurarse de mantenerse por delante de los estafadores". Sin embargo, gracias a los avances continuos en la tecnología, Deepfakes pronto también podría representar un riesgo para la actividad automatizada, con el potencial de ayudar a los ciberdelincuentes a pasar los protocolos de seguridad de vídeo y audio.

La recomendación principal se orienta a que cada vez que alguien le pida que haga algo como transferir dinero o compartir datos en un teléfono o una vídeo llamada, verifíquelo en otro lugar. Envíelos por correo electrónico directamente, envíe una nota y obtenga esa verificación adicional.

No existe un método garantizado para detectar un Deepfake, ya que la tecnología cambia todo el tiempo, por lo que la clave es cambiar su cultura para educar a todos sobre los riesgos".

Debemos entender que la seguridad cibernética no solo se refiere a tecnología, no pudiendo dejar de lado la importante contribución del factor e intuición humanas.

Con las amenazas de seguridad cibernética en constante evolución, las empresas necesitan contar con las personas adecuadas para rastrear las amenazas y desarrollar defensas contra ellas.

Las políticas de confianza cero son un gran paso para educar a cada individuo sobre los riesgos que plantean las estafas cibernéticas (Deepfake o de otro tipo), pero deben ser dirigidas por personas con el conocimiento tecnológico adecuado y las habilidades blandas para involucrar a los empleados en toda la empresa y, especialmente a nivel directivo.

El fraude deepfake quizás esté dirigido de manera desproporcionada a los profesionales senior en comparación con otros métodos de delitos cibernéticos, ya que estos objetivos de alto riesgo y alto valor pueden proporcionar un retorno más significativo a los delincuentes que han invertido en la tecnología.

Educar a su equipo de seguridad cibernética, así como a los usuarios comerciales, sobre las tecnología y los riesgos potenciales de Deepfake es crucial para proteger su organización. También es esencial contar con un sólido equipo de talentos en seguridad cibernética que estén capacitados y listos para combatir las amenazas de seguridad de hoy en día".

Con el talento de liderazgo en seguridad cibernética en alta demanda y escasez en todos los sectores, las empresas deben actuar ahora para educar a sus empleados y asegurar las habilidades que necesitan para enfrentar las amenazas de seguridad de Deepfake, o correr el riesgo de sufrir ataques de contenido sintético, en el futuro cercano.

Métodos para combatir Deepfakes

Actualmente, las técnicas para identificar deepfakes han conseguido llegar a un nivel de precisión del 86, 6%, lo cual está muy bien, pero en un futuro se tendría que poder asegurar llegar al 99% de seguridad y consistencia. Los métodos que hoy en día se están utilizando para identificar los deepfakes y por el momento han funcionado correctamente son varios.

Uno de ellos es el de análisis de metadatos, información textual sobre la producción del archivo multimedia (cámara, ISO, data de creación...), para ver si la imagen ha estado manipulada previamente. Es posible modificar los metadatos pero la gran mayoría de archivos contienen la información de los programas de edición utilizados, facilitando así, la identificación de las intervenciones en los archivos. No es totalmente eficaz pero puede ser un buen método de detección preliminar de deepfakes.

Otro sistema as analizando el nivel de error (ELA, Error Level Analysis) de los métodos de compresión de imágenes de archivos como JPG, que al comprimirse pierden información. Así pues, hace falta saber que las imágenes editadas acostumbran a tener áreas con diferentes niveles de artefactos de compresión, ya que han estado sometidas a varios sistemas de compresión.

También se podriá intentar identificar los artefactos visuales, residuos de la creación de rostros falsos con deepfakes, entre los que se pueden destacar:

1.- Que la fusión de las diferentes imágenes utilizadas para crear la falsa no sea totalmente coherente y falle en consistencia global. Como por ejemplo, que el iris del ojo derecho tuviera un color diferente al izquierdo, con excepción de los pocos casos de heterocromía.

2.- Que se produzca un error de iluminación imprecisa y distorsionada en las figuras debido al intento de fusionar varias imágenes con diferente luz. Eso terminaría provocando que la imagen final no tuviera total coherencia lumínica.

3.- Que se produzca un error geométrico en los ajustes morfológicos de los rostros y figuras humanas, especialmente expresado en bordes fuertes o tacas muy contrastadas alrededor de los límites faciales de la máscara que afectarían zonas como la de la nariz, la cara o las cejas.

Por último, se ha descubierto que a menudo los deepfakes tienen errores en la estructura de los rostros. Eso se debe al hecho que se crean a partir del reemplazo de partes del rostro original con imágenes faciales sintetizadas, y como las personas tienen estructuras de la cara diferentes, la tecnología de los deepfakes no acaba de conseguir garantizar que todos los puntos de referencia identificados por la computadora se alineen correctamente.

Imagen de tigerlily713 en Pixabay

Policiamiento predictivo en la era de los algoritmos y la justicia criminal inteligente

En la era digital actual, vivimos en la denominada "sociedad de vigilancia", atestados de videocámaras en las metrópolis o grandes conglomerados urbanos, que sirven para identificar demostrantes en protestas y reconocer a la distancia dentro de las masas a opositores políticos o personas que viven al margen de la ley, a través de sistemas de datos biométricos instalados en aeropuertos, zonas fronterizas, estaciones de tren, estadios de fútbol, etc., que identifican microgestos faciales o voces.

Esta aplicación de técnicas modernas basado en el uso de algoritmos y sistemas de datos biométricos en el trabajo policial, en la administración de justicia y en el sistema penitenciario, son medios de ayuda técnica apenas prescindibles, que ha alcanzado gran relieve en el debate de la política criminal contemporánea, especialmente en el policiamiento predictivo, tanto en el ámbito de la gerencia de amenazas, el análisis criminal, como en la ejecución de la pena orientada al riesgo.

Su aplicación se torna técnicamente más inteligente y nos plantea cada vez más cuestionamientos de orden legal, criminológico, criminalístico, científico, administrativo como social.

Delitos medidos o calculados y criminales computados

La politóloga suiza Monika Simmler refiere en su reciente libro "Smart Criminal Justice", que nos encontramos en la "Segunda era de las máquinas", que ha tomado el control del mundo y que la "Era de los algoritmos" ha sido interrumpida, citando en dicha obra un artículo publicado en el New York Times de junio del 2020, titulado "Erróneamente acusado por un algoritmo", que hacía alusión a la historia de un afroamericano R.J. Williams, que fue detenido ante los ojos de su familia en Detroit, por que un algoritmo del software de reconocimiento facial lo identificó erróneamente. Queda abierta la interrogante, si Williams fue el primero en aterrizar en una cárcel por un error técnico .

Este desarrollo marca el modo o la práctica de como se debe de hacer frente a la criminalidad hoy en día, la técnica ha cambiado el mundo, en el que la inconducta social como tal debe de ser identificada, variando también, los métodos como deben de evitarse, esclarecerse y sancionarse los hechos delictivos, vale decir, la prevención criminal, la criminalistica, el proceso penal y la ejcución de la sanción.

En efecto, los algoritmos apoyados en instrumentos técnicos prometen poder calcular la probabilidad de hechos delictivos en un "momento X" y en un un "lugar Y", sirviéndose para ello de métodos estadísticos modernos, análisis de la Big Data y modelos de aprendizaje avanzados.

El algoritmo es una instrucción de actuación: "si pasa A, sucede B", ello conlleva a una pérdida de individualidad, de medición y de decisión en un caso individual, ya que los algoritmos son muy estrictos. Ahora la interrogante planteada es, si puede ser justo un régimen estricto de circunstancias con las que la administración de justicia debe de confrontarse.

La justicia criminal inteligente

La justicia criminal inteligente implica el empleo de tecnología en la administración de justicia sobre la base de una toma de decisiones algoritmica y la recolección, análisis y evaluación de una inmensa cantidad de datos, comprendiendo el ámbito del trabajo policial, la justicia penal y el sistema correccional. Una justicia penal inteligente desea obtener las ventajas de la técnica inteligente y moderna, extrayendo todo su potencial para un trabajo policial y una administración de justicia más eficiente y efectiva.

Es necesario comprender que no todo simple algoritmo o cada digitalización puede subsumirse dentro de la justicia criminal inteligente. Los algoritmos comprenden un vasto campo de usos, como tales, los algoritmos abarcan un campo muy amplio de aplicaciones, ya que básicamente toda determinación de "si A, entonces B" ya es algorítmica. Asimismo, toda aplicación técnica se basa en algoritmos, por lo que toda digitalización per sé con el uso de algoritmos en general, debe distinguirse de una aplicación avanzada en el sentido de la justicia inteligente.

Sin embargo, los límites entre la llamada "justicia electrónica", es decir, una simple digitalización de los procedimientos, y la "justicia inteligente" son

fluidos, por lo que siempre hay que considerar y debatir un amplio espectro de aplicaciones en un primer momento.

En el ámbito del trabajo policial cabe destacar el policiamiento predictivo, que desde hace algún tiempo ha impregnado el discurso de la política criminal y criminalistica, abarcando el aprovechamiento de instrumentos técnicos en el ámbito de la gerencia de riesgos o en el trabajo de investigación policial.

En relación con la justicia penal y los servicios penitenciarios, yace en el centro del debate las evaluaciones psiquiátricas forenses en general, y los pronósticos de reincidencia en particular.

El policiamiento predictivo

El policiamiento predictivo es una modalidad de operativo policial ejecutada por los agentes de la policía, que contemplan una intervención en una zona puntual en días y horarios específicos y contra determinadas personas en virtud de pronósticos derivados de mediciones técnicas en base a evaluaciones estadísticas. Jennifer Pullen de la Escuela de Leyes de la Universidad de San Gallo en Suiza, define el policiamiento predictivo como "el uso de procesos técnico-analíticos, que mediante pronósticos estadísticos identifican sucesos probables, los cuales exigen la intervención policial dando con ello la posibilidad a la policía de adoptar medidas preventivas". Sin embargo, estos resultados de las previsiones también pueden utilizarse para resolver delitos pasados.

Las predicciones, así como la probabilidad de que se produzca un delito, se calculan mediante programas informáticos, que utilizan el análisis de datos y algoritmos didácticos. En el proceso, los resultados pueden incluir predicciones tanto basadas en la ubicación como en la persona.

Por otro lado, se calcula la presunta delincuencia de un individuo en función de diversos factores de riesgo, por lo que estas personas se introducen posteriormente en una base de datos de peligrosidad, por ejemplo, en el marco de la gestión de riesgos o amenazas. Es evidente que el objetivo es prevenir la delincuencia o, al menos, reducirla siempre que sea posible.

Patricia Schefer, gerente digital y de comercio electrónico de Zúrich, agrega que el policiamiento predictivo, es un proceso que dentifica patrones a partir de un conjunto de datos pasados mediante el análisis de correlaciones estadísticas. En consecuencia, la aplicación del policiamiento predictivo no se basa en previsiones definitivas, sino siempre en probabilidades.

Teorías criminológicas y policiamiento predictivo

Los software de policiamiento predictivo actuales trabajan con datos criminales históricos y en virtud de estos datos elaboran pronósticos sobre áreas del crimen y perfíles de personas criminales futuras. La aplicación del policiamiento predictivo no solo se basa en el desarollo de algoritmos previsualizados e instrumentos de análisis técnicos modernos, sino también esencialmente en base a teorías criminológcas, de cuyos resultados se basan los programas informáticos. Por lo tanto, para aplicar el policiamiento predictivo de forma exhaustiva, hay que tratar también los conceptos criminológicos en los que se basa.

Estas teorías presuponen en su mayoría, que la delincuencia es un proceso predecible, según el cual, tanto los delincuentes como las víctimas siguen ciertas pautas de comportamiento universales y estadísticamente determinables.

Dentro de las teorías criminológicas que avalan el empleo del policia-

Foto de Tingey Injury Law Firm en

miento predictivo, tenemos el enfoque de elección racional (que contempla a las personas delincuentes como seres que actúan racionalmente, los cuales consideran los riesgos tanto en el planeamiento de sus actos como en la ejecución del mismo, en función a la ponderación (costo-beneficio), el pronóstico de repetición próxima (que complementa a la teoría de victimización repetitiva, en la cual una victimización sucitada en un lugar o una persona indexa más victimización), la teoría de la actividad rutinaria (que condiciona la criminalidad a determinadas constelaciones espaciales y temporales, elevando la probabilidad de victimización), la teoría de las ventanas totas (denominado modelo del desorden) y la teoría del estilo de vida (otro de los llamados enfoques situacionales, la mayor susceptibilidad de ciertas personas a la victimización se justifica con el estilo de vida). Estas teorías brindan una fundamento científico al proceso de policiamiento predictivo.

El policiamiento predictivo como proceso general

El policiamiento predictivo es un proceso policial holístico e integral, que no solo se basa en el pronóstico, sino en el cierre de un círculo de análisis de datos, implementación de medidas, reflexión de los efectos y una nueva recolección de datos.

Este proceso consiste en un primer paso, en una recolección de datos y en un segundo paso, en el análisis de estos datos para generar un pronóstico. Un tercer paso después del pronóstico, consiste en una reacción de la policía frente al mismo, aquí la policía tiene a su disposición distintas posibilidades de intervención en el marco preventivo como recurrir al seguimiento y observación para atraparlo in flagranti y proceder a detenerlo, o fortalecer el patrullaje visible con el fin de marcar presencia policial, constituyendo un elemento disuatorio para que no se llegue a perpetrar un hecho delictivo.

Sin embargo en el marco de una estrategia mixta, la policía puede realizar operativos preventivos y represivos, basados en un incremento de controles policiales que tengan ambos efectos. El cuarto y último paso, como resultado de la acción policial producto del pronóstico emitido, el entorno delictivo variará, siendo necesario recoger nuevos datos para determinar la situación actual.

Categorías del proceso del policiamiento predictivo

Olivia Zingg, del Centro de Competencia de Derecho Penal y Criminología de la Universidad de Lucerna en Suiza, identifica 4 categorías en un proceso de policiamiento predictivo: 1. categoría: Localización de la criminalidad, 2. categoría: Evaluación de la peligrosidad, 3. Evaluación de riesgos de reincidencia y 4. Categoría: Identificación de la víctima

1 **Localización de la criminalidad**: En esta categoría el policiamiento predictivo se centra en fijar las regiones o zonas de riesgo y los momentos de riesgo con la ayuda de datos espaciales sociales y de delincuencia. Aqui se determina que áreas y momentos son vulnerables para potenciales hechos delictivos, en otras palabras localizar la criminalidad para minimizarla en todo el país. Los métodos que se emplean en esta categoría son el Analisis Hot Spot, la regresión estadística, recolección de datos y el pronóstico de repetición próxima, los cuales son usados para indagar probables lugares futuros de la delincuencia y su marco temporal en base a sucesos pasados.

Estos métodos darán como resultado recomendaciones de medidas policiales en los puntos críticos para reducir la criminalidad. Aquí se identifican los factores espaciales que pueden constituir un alto riesgo de criminalidad. Con este proceso se pueden identificar además los lugares de alta victimización. En Suiza se usa el programa de software PRECOBS (Pre Crimen Observation System) en las policías cantonales de Zúrich, Argovia y Basilea-Campo.

2. **Evaluación de la peligrosidad:** En esta segunda categoría se identifica individuos que presentan una alta probabilidad de que puedan cometer hechos delictivos futuros. Los métodos de análisis preventivo utilizan modelos de regresión y clasificación que convierten la existencia de factores de riesgo específicos para delincentes en un pronóstico de probabilidad.

La persona identificada será clasificada como un alto factor de riesgo, en virtud del análisis estadístico realizado. La probabilidad de que esta persona sea delincuente, es según la evaluación del algoritmo considerablemente mayor que en las personas promedio. El trabajo preventivo de la policía intenta en esta categoría evaluar e influenciar a corto y mediano plazo, los factores de riesgo de las personas identificadas.

Los software más conocidos son hot-people system en EEUU (hots lists), Strategic Subject List de la Policía de Chicago, RADAR-iTE (Regelbasierte Analyse potentiell destruktiver Täter) utilizado por la Bundeskriminalamt (BKA) de Alemania

Foto de Campbell Jensen en Unsplash

para identificar terroristas islámicos y DyRiAS (Dynamisches Risiko Analyse System) utilizado en Suiza para identificación temprana de individuos potenciales con alto riesgo de conducta violenta y acoso en los estadios, escuelas, centros de trabajo y el DyRiAS-Intimpartner, que se circunscribe para prevenir la violencia doméstica.

3. **Evaluación de riesgos de reincidencia**: En esta categoría se identifica el riesgo de reincidencia de una persona. Ello implica medidas policiales represivas y penales a diferencia de la categoría 2, en la que se aplican medidas policiales meramente preventivas, ya que en esta última no se han adoptado medidas procesales penales. El policiamiento predictivo pretende monitorear amenazas futuras, intentando impedir que una persona ya condenada, vuelva a cometer una infracción penal.

En el sistema correccional suizo-alemán para la evaluación de reincidencia de una persona que ya está cumpliendo su pena, se emplean procesos similares a la categoría 2 para la evaluación de la peligrosidad en base al sistema ROS (Risiko-orientierten Sanktionenvollzug), vale decir una evaluación de la peligrosidad durante la ejecución de la pena orientada al riesgo. Su objetivo es promover la concienciación sobre los riesgos a lo largo del proceso y tiene como objetivo la resocialización sostenible y la prevención. La problemática de estos pronósticos está en que siempre se focalizan en el pasado del delincuente, lo cual se contrapone a los ideales de de resocialización del derecho penal.

4. **Identificación de la víctima**: Su diferenciación con los métodos aplicados en las otras categorías está en que no se ocupan de potenciales delincuentes, sino de personas, que en promedio muestran una alta probabilidad de ser víctimas de un hecho delictivo y lugares, en los cuales tales personas podrían ser víctimas de un hecho delictivo.

El objetivo es evitar estos hechos delictivos. Aqui no son identificadas personas individuales sino grupos de riesgo enteros. En los Estados Unidos existe la denominada Strategic Subject List, una lista basada en algoritmos sobre la base de datos criminales, que identifican a potenciales autores y víctimas de hechos criminales, dentro de estas categorías los algoritmos no hacen distinción alguna que impliquen distorsiones, como el color de piel, género y etnia. Personas con gran vehemencia serán informados y prevenidos por las autoridades policiales competentes.

Gerencia de amenazas como nuevo paradigma de la policía

Monika Simmler y Simone Bruner del Centro de Competencia de Derecho Penal y Criminología de la Universidad de San Gallo, afrman que el objetivo de la gerencia de amenazas por parte de la policía es percibir los desarrollos peligrosos de una persona para cometer actos violentos, para así poder impedirlos.

Esta afirmación se basa en la convicción generalizada de que la violencia selectiva grave suele ser la última fase de la escalada de una tensión, que se ha ido desarrollando durante mucho tiempo, por lo que el autor de la violencia suele mostrar un comportamiento llamativo incluso antes del acto. Por lo general esta situación se hace evidente en determinados ámbitos como la violencia familiar, el acoso sexual, la violencia escolar, las amenazas contra autoridades, el hooliganismo (violencia en los estadios), el extremismo violento y la radicalización. Su monitoreo requiere de un trabajo sistemático e interinstitucional.

La gerencia de amenazas se focalizan en las personas, que presentan un cierto grado de peligrosidad, siendo definidas como "personas peligrosas", en este contexto se carece de una definición legal uniforme de "persona peligrosa", aquí existe un vacio legal en la protección de los derechos fundamentales de las personas que se derivan del principio fundamental de la presunción de inocencia, en este contexto Jasmin Bueler de la Escuela de Leyes y Economía de la Universidad de San Gallo, postula la "presunción de no peligrosidad", que debe ser garantizada a toda persona en un estado democrático, subrayando que estos pronósticos pueden constituir un serio peligro para la seguridad y el orden público, en un estado de derecho moderno.

Reflexión final

Las crecientes expectativas de seguridad en la sociedad posmoderna implican hoy en día una demanda de intervención, incluso antes de que se produzcan infracciones de las normas y actos penalmente relevantes.

Hoy los medios de comunicación y los políticos, hipersensibilizados con el tema de seguridad, acusan regularmente a las fuerzas del orden de intervenir tarde en los sucesos peligrosos, diciendo a menudo de forma acusadora, que el autor ya era conocido por la policía.

Esta evolución actual hacia una mayor necesidad de prevención, que se pone de manifiesto en el plano legal, procesal y policial, exige un cambio de orientación de los actores del sistema de justicia penal vigente.

En este contexto, tenemos el denominado proceso de policiamiento predictivo, que comprende el desarrollo de los llamados métodos policiales predictivos, que son una herramienta de previsión estadística para determinar la probabilidad de un acontecimiento futuro y contribuir así a la prevención de la delincuencia.

El paradigma del policiamiento predictivo implica para los cuerpos de seguridad y policía el aprovechamiento de las nuevas tecnologías, para ello, es necesario definir claramente las condiciones marco para dicha actuación policial.

En un estado de derecho liberal el punto de orientación es claro, son los derechos fundamentales constitucionales los que nos muestran la línea divisoria entre los medios que puede emplear un estado y que medios no puede emplear, ya que estos últimos no estarían en concordancia con nuestra libertad, autonomía y dignidad.

Los derechos fundamentales contituyen la única garantía jurídica para que no se cruce la línea roja, donde la tecnología no nos sirva más, sino

Autor: Javier Gamero Kinosita

SeguridadExpo: 25 - 27 Octubre, Santiago, Chile

SeguridadExpo es el principal evento internacional del sector en Chile, y atrae a más de 5.000 mil visitantes por su amplia oferta de soluciones tecnológicas del sector y su interesante programa de actividades. La exhibición está sectorizada en 3 salones: Seguridad pública y privada; Seguridad industrial, laboral y bioseguridad y Fuego y desastres naturales.

El evento tiene por objetivos:

- Reafirmar el importante rol de la Seguridad en Chile
- Mostrar los desarrollos locales de bienes, productos y servicios orientados a la industria.
- Introducir al mercado nuevas tecnologías no disponibles en Chile
- Intercambiar experiencias, tecnologías y desarrollos internacionales con la industria chilena.
- Entregar soluciones efectivas a las policías , FFAA y civiles

Cyber Security Summit: 24 - 26 de Octubre 2022 Minneapolis

La seguridad cibernética deficiente está afectando cada vez más a todos los niveles de la sociedad, ya sea a nivel nacional, local o personal.
Con unas pocas pulsaciones de teclado, los estados nacionales, los grupos terroristas, las organizaciones sin estado y los individuos deshonestos pueden lanzar un ataque cibernético desde cualquier lugar y en cualquier momento, perturbando y dañando nuestra democracia y forma de vida.
Para afrontar el problema, necesitamos la ayuda de todos.
En la Cumbre de Seguridad Cibernética, nuestra misión es producir un consorcio de múltiples partes interesadas que reúna los intereses de la industria, el gobierno y la academia en un esfuerzo por mejorar el estado de la seguridad cibernética tanto a nivel nacional como internacional.

TECHSPO DUBAI 18 - 19 Octubre 2022, Dubai

TECHSPO Dubai es una exposición tecnológica de dos días que reúne a desarrolladores, marcas, comercializadores, proveedores de tecnología, diseñadores, innovadores y evangelistas que buscan marcar el ritmo en nuestro avanzado mundo tecnológico.

Exhibiendo la próxima generación de tecnología e innovación; Internet , dispositivos móviles , AdTech , MarTech y tecnología SaaS , los expositores tienen la oportunidad de mostrar sus empresas a los consumidores, los inversores de mayor calibre, hordas de prensa, el talento más buscado y el grupo más grande de entusiastas de la tecnología que buscan celebrar los productos emergentes. . Prepárese para inspirarse, sorprenderse y educarse sobre cómo estas tecnologías en evolución impactarán en su negocio para lograr un mayor crecimiento.

CBRNe 5 - 7 Octubre 2022, Denver Colorado USA

La cumbre CBRNe anual de EE. UU. llegará a Denver, CO, del 5 al 7 de octubre de 2022. Este evento reúne a destacados funcionarios de las agencias militares, civiles y científicas para brindarle una perspectiva completa sobre todas las amenazas y amenazas CBRNe . retos

Durante la conferencia y exposición de 2 días, escuchará diferentes perspectivas sobre la preparación, la resiliencia y la respuesta CBRNe. Con el mundo entrando en un nuevo capítulo con la pandemia global de COVID detrás de nosotros, muchos gobiernos ahora están viendo la importancia de mejorar las capacidades CBRNe para hacer frente a una futura pandemia.

MÁXIMOS REFERENTES EN ARMAMENTO NO LETAL

BULL SERVICE

* Disuasión efectiva dentro del marco legal
* No afecto a ley de Armas

DEFENSA DEL HOGAR

POLICIAS

INDUSTRIA DE LA SEGURIDAD

BLINDAJE AUTOMOTRIZ CUSTOMIZADO

SATISFACCIÓN 100% GARANTIZADA

www.bullservice.cl
+56 9 4623 8380 / +56 9 9909 1958

@bullservicechile @bull.service

Save the Date!

3 - 5 OCT. 2023

PARQUE FISA
SANTIAGO - CHILE

PRESENCIAL

¡Hablemos! WhatsApp: +56 9 4481 6922 | Email: info@seguridadexpo.cl

SEGURIDADEXPO

by Fisa | CHILE

PARTICIPA EN EL PRINCIPAL ENCUENTRO DE LA INDUSTRIA DE LA SEGURIDAD NACIONAL E INTERNACIONAL:

CONECTA
CON EMPRESAS, PROFESIONALES Y TOMADORES DE DECISIÓN

MARKETPLACE
EXHIBE TUS PRODUCTOS Y SERVICIOS DE FORMA 100% DIGITAL

NETWORKING
ESPACIO DE ENCUENTRO EN EL SECTOR

CHARLAS Y CONFERENCIAS
NUTRIDO PROGRAMA DE ACTIVIDADES

[7ª Exhibición y Congreso Internacional de Seguridad Integral]

GL events

@seguridadexpo

www.seguridadexpo.cl

ORGANIZA Y PRODUCE

Fisa