Mayo - Junio 2025 / edición 1°

CON SEGURIDAD

Magazine Latam

INFORMACIÓN SIN FRONTERAS

www.conseguridad.com

GRUPO EDITORIAL • GRUPO EDITORIAL • GRUPO EDITORIAL • GRUPO EDITORIAL •

MS GLOBAL

Mayo - Junio 2025 / No. 1° / Año 1
México y Latam / precio $60.00 MXN / $3.00 USD

CIBERSEGURIDAD
SEGURIDAD
SAFETY
REDES
FIRE

SEGURI EXPO ECUADOR

XI Feria internacional de seguridad

QUITO

CENTRO DE CONVENCIONES METROPOLITANO DE QUITO

5 - 6 JUNIO 2025

11ava edición

seguriexpoecuador

www.exposeguridadecuador.com
info@myestrategia.com

MEMBER SEGU EXPO NEXUS

RED DE CONEXIONES & NEGOCIOS PARA PROFESIONALES Y EMPRESAS DE LA INDUSTRIA DE LA SEGURIDAD EN LATINOAMERICA

Seguridad como tema de cultura general

Estimados lectores de América Latina:

Es un honor presentarles el primer número de **Con Seguridad Magazine**, publicación que nace con la firme misión de convertirse en el nuevo punto de referencia para quienes entienden que la seguridad, en todos sus niveles, es hoy más que nunca un tema de cultura general.

Este lanzamiento es fruto de la alianza estratégica entre **Con Seguridad (Venezuela)**, liderada por el profesional de la industria, **Alfredo Yuncoza**, y **Grupo Editorial MS Global**, responsable de las reconocidas magazines **Más Seguridad** y **Global Defense (México)**, bajo la dirección de **Humberto Mejía**.

Con Seguridad Magazine apunta directamente a los mercados de México, Venezuela y toda América Latina, con la mirada puesta en ofrecer información de valor sobre las últimas tendencias tecnológicas de los fabricantes más destacados a nivel mundial. Además, reúne en estas páginas una diversidad de opiniones y análisis de expertos de diferentes países, con la finalidad de brindar un panorama amplio, crítico y actualizado del sector.

Entre los temas que nutrirán cada edición destacan los avances legislativos, los procesos de capacitación y certificación profesional, así como las iniciativas de las asociaciones que integran a los líderes de la industria en la región, entre otros.

Más que un "nuevo competidor", **Con Seguridad Magazine** se posiciona como un aliado en la construcción de una cultura sólida de prevención, en el impulso al desarrollo profesional, y en la generación de herramientas para una mejor toma de decisiones en empresas y organizaciones.

Esta revista será, además, un espacio privilegiado para que los patrocinadores den visibilidad a sus marcas, productos y soluciones ante una audiencia altamente especializada. Aquí, tanto profesionales como usuarios finales encontrarán un escaparate de información objetiva, oportuna y confiable, construida por una red de expertos comprometidos con el crecimiento de la industria.

Con entusiasmo y convicción, les damos la bienvenida a este nuevo concepto editorial, concebido para apoyar su labor diaria y fortalecer sus estrategias. **Con Seguridad Magazine** marcará, sin duda, un antes y un después en el sector de la seguridad en América Latina. Nos proponemos ser su fuente de análisis, tendencias y perspectivas para enfrentar los retos de hoy y de mañana.

CON SEGURIDAD
Magazine Latam

DIRECCIÓN GENERAL

HUMBERTO MEJÍA, DSE, CPSI, CIEIE
NORTEAMÉRICA / ESPAÑA
hmejia@conseguridad.com

ALFREDO YUNCOZA, CSSM, CPOI, CPO
CENTRO / SUDAMÉRICA
ayuncoza@conseguridad.com

DIRECCIÓN COMERCIAL

MARÍA ANTONIETA JUÁREZ CARREÑO
DIRECCIÓN COMERCIAL Y RELACIONES PÚBLICAS
marieclaire@conseguridad.com

COORDINACIÓN EDITORIAL

BEATRIZ CANALES HERNÁNDEZ
COORDINACIÓN EDITORIAL
edicion@conseguridad.com

COORDINACIÓN DISEÑO

SERGIO GIOVANI REYES POZO
COORDINACIÓN DISEÑO
diseno@conseguridad.com

MARKETING LATAM

SARA MEJÍA CASTRO
DESARROLLO DE NEGOCIOS LATAM
negocios@conseguridad.com

CORRESPONSAL

CARMEN CHAMORRO
CORRESPONSAL ESPAÑA
corresponsal@conseguridad.com

ADMINISTRACIÓN Y CONTABILIDAD

OSCAR TENORIO COLÓN
ADMINISTRACIÓN Y CONTABILIDAD
contabilidad@conseguridad.com

CONTACTO

Tel: +52 55 1607 1398 (México)
WhatsApp: +58 424 1390 359 (Venezuela)
WhatsApp: +52 55 1894 7067 (México)
asistencia@conseguridad.com

Con Seguridad Año 1, No 1, Mayo/Junio 2025, Publicación Bimestral de **Grupo Editorial MS Global S. de R.L. de C.V.**, con domicilio en Av. Primero de Mayo No 15, Piso 11, Ofic. 1108, Col. San Andrés Atoto, Naucalpan, Estado de México, C.P. 53500, Tel: +52 5518447067 . **Editor responsable: Humberto Mejía Hernández.** Certificado de Reserva 04-2022-050614181900-102 otorgado por el Instituto Nacional del Derecho de Autor. Certificado de Licitud de contenido No. 11483 y Certificado de Licitud de Título No. 13910, otorgados por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación. Autorización del Registro Postal: PP15-5134 otorgado por Sepomex. Se autoriza la reproducción citando al medio y autor del texto, previo acuerdo por escrito con el editor. Impresa en: **Grupo Mejía Impresores**, calle La Poza No. 72, Col. San Lorenzo Totolinga, Naucalpan de Juárez, Estado de México, Tel: +52 5518947067.

CONTENIDO

CALENDARIO
CURSOS ALAS 2025

MAR	ABR	MAY	JUN	JUL
11 - 14	22 - 25	27 - 30	17 - 20	22 - 25
Video Vigilancia	Control de Acceso	Inteligencia Artificial en Seguridad	Alarmas y Detección de Intrusión	Operadores de Cuartos de Control

AGO	SEP	OCT	NOV	DIC
19 - 22	23 - 26	28 - 31	25 - 28	9 - 12
Evaluación de Riesgos de Seguridad	Ventas para la Industria de la Seguridad	Gerencia de Proyectos	Video Vigilancia	Operadores de Cuartos de Control

Este curso y muchos más los puedes disfrutar en la modalidad InCompany

Alarmas y Detección de Incendios • Alarmas y Detección de Intrusión • Ciberseguridad para Alta Gerencia • Ciberseguridad y Protección de Activos Digitales • Control de Acceso • Drones en Seguridad • Evaluación de Riesgos de Seguridad • Evaluación del Retorno de la Inversión • Fundamentos de Seguridad Electrónica • Gerencia de Proyectos • Integración de Sistemas de Seguridad • Inteligencia Artificial en Seguridad • Management 3.0 • Operadores de Cuartos de Control • Redes IP e Inalámbricas • Seguridad Perimetral • Ventas para la Industria de la Seguridad • Video Vigilancia •

www.alas-la.org

CURSOS ALAS

ASOCIACIÓN LATINOAMERICANA DE SEGURIDAD

Si eres **Socio ASIS,** obtendrás **puntos CPEs** en esta actividad

CRISTIAN MOLINA
Coordinador de Cursos
Whatsapp:
+57 321 6153367

Los profesionales de LATAM

Master en Políticas de Seguridad y Defensa, 1999-2001, FLACSO.
Máster en Políticas Públicas, Universidad Complutense, 1993-96, Madrid, España.
Lic. Ciencias Políticas, Mención Estudios Socioeconómicos. Universidad Autónoma de Santo Domingo, 1982.
Diplomado en Planificación de Proyectos, Universidad Nacional Pedro Henríquez Ureña y Universidad del Estado de Israel, 1982.
Diplomado en Política Exterior de los Estados Unidos, USIS, Rep. Dominicana, 1983.
Diplomado en Métodos y Técnicas de Investigación Empírica, CERESD-UASD. 1983.
Profesor e Investigador Asociado de la Facultad Latinoamericana de Ciencias Sociales (FLACSO) 2000-).
Profesor y Fundador del Instituto de Altos Estudios Para la Seguridad y La Defensa (IADESEN) hoy Escuela de Graduados (EGAE). Ministerio de las Fuerzas Armadas, Rep. Dominicana, 2001-09.
Miembro del Comité Científico del EGAE. Ministerio de las FFAA, Rep. Dominicana. (2016-)
Profesor Invitado del Instituto Militar de Estudios Superiores (IMES), Rep. Dominicana, 2001-2004.

Daniel Enrique Pou Suazo
República Dominicana

¿Seguridad privada para 100 mil deportados?

Y empezó a cumplirse la amenaza del Presidente estadounidense Donald Trump: sacar de su país a indocumentados, medida que afecta de inmediato a poco más de 2 millones de mexicanos y otro importante número de latinos. Ante este éxodo, la seguridad privada se dice lista para dar empleo a 100 mil connacionales repatriados.

El sector de la protección, representado por Agrupaciones de Seguridad Unidas por México (ASUME) y presidido por Armando Zúñiga Salinas, "levantó la mano para ofrecer estas plazas laborales".

Sin duda la intención es buena, considerando que tal vez haya varios miles de exguardias intramuros, técnicos instaladores, monitoristas o blindadores, etc., que hayan sido deportados, pero conociendo un poco el mercado estadounidense de la seguridad es difícil que estos hubiesen sido contratados en la Unión Americana sin los documentos pertinentes para demostrar su estancia legal.

Por otra parte, ¿en el supuesto que los repatriados se interesen en el servicio de seguridad privada mexicana por cuestiones de remuneración salarial le convendrá contratarse?

Según ASUME, órgano conformado por 32 de las asociaciones más importantes de seguridad privada de México y con más de 8 mil empresas afiliadas, trabajará en estrecha colaboración con el gobierno mexicano, organismos empresariales como el Consejo Coordinador Empresarial (CCE), autoridades locales y federales, para garantizar que esta integración laboral sea efectiva. Hasta el cierre de edición de este ejemplar, no he tenido conocimiento de cuantos repatriados ya hayan sido contratados en el gremio aseveró Zúñiga Salinas

"Como sector estratégico que genera más del 2% del Producto Interno Bruto (PIB) nacional y da empleo formal a cerca de un millón de personas, la industria de la seguridad privada tiene la capacidad y el compromiso de apoyar a quienes regresan a México en busca de una nueva oportunidad para construir un futuro digno.

Importante mencionar que la iniciativa de ASUME incluye:
Capacitación Certificada: A través de programas especializados, los migrantes recibirán formación profesional certificada por organismos como el CONOCER, que les permitirá desempeñarse con estándares de calidad y seguridad.

Condiciones Laborales Dignas: Se asegurará que los empleos ofrezcan prestaciones sociales, salarios competitivos y oportunidades de crecimiento.

Inclusión Regional: El esfuerzo estará enfocado en las zonas con mayor concentración de repatriados, contribuyendo al desarrollo local y la cohesión social.

No soy "aguafiestas" pero... ASUME ofreció 100 mil empleos, Oxxo 50 mil, el CCE 35 mil y otro grupo de empresas 70 mil, pero en diciembre de 2024 se perdieron 450 mil empleos, según el INEGI. Hoy muchas Pymes, desempleados y hasta desempleados se preguntan y postean en redes sociales: "¿para los nativos pan y agua, o solo demagogia y oportunismo?

Por cierto, el nicho de los guardias privados en el que más elementos requiere y contrata anualmente, pero para nadie es un secreto la altísima rotación que registra, en buena parte por empresas de mala calidad y dudosa reputación, "castigados" salarios, jornadas extenuantes, condiciones laborales cuestionables y hasta discriminación de "directivos" y clientes hacia los empleados...

¡Gracias y nos leemos pronto, pero Fuera de Grabación!

Lanza HIKVISION Calendario de capacitaciones 2025

▪ Cursos para distribuidores e integradores. Conocimientos actualizados que les permitan destacar en un mercado cada vez más competitivo y tecnológicamente avanzado.

Hikvision México presenta su Calendario 2025 de cursos, capacitaciones y talleres para potenciar y validar los conocimientos teóricos y prácticos de sus distribuidores, instaladores e integradores en áreas específicas de la seguridad electrónica, asegurando que posean las habilidades necesarias para desempeñarse de manera efectiva en sus roles.

"El arranque de las capacitaciones en 2025 representa una oportunidad estratégica para fortalecer las destrezas técnicas, comerciales y de servicio al cliente de integradores, canales e instaladores y, de esta manera, empoderarlos con conocimientos actualizados que les permitan destacar en un mercado cada vez más competitivo y tecnológicamente avanzado", comenta Fran Sánchez, Marcom Director en Hikvision México.

Resalta que se ha diseñado un calendario integral de capacitaciones que mes con mes se anunciará vía redes sociales, encauzado en el diseño de sistemas avanzados de seguridad con dispositivos Hikvision para que así los participantes desarrollen soluciones completas y verticales: "Nuestro compromiso es fortalecer su desempeño para ofrecer soluciones innovadoras y confiables al mercado mexicano".

Para consultar las fechas de 2025 y para registro, visitar **https://bit.ly/427AxeF**. Cada mes se anunciarán vía redes sociales (**@HikvisionMexico**) las nuevas fechas. Asimismo, a través de la aplicación HPP (Hik-Partner Pro), los participantes podrán expandir su conocimiento y la influencia de su negocio, obteniendo más oportunidades comerciales: Busca en Google play store como Hik-Partner Pro (Formerly HPC).

Fran Sánchez
Marcom Director en Hikvision México.

HIKVISION

DESCARGA Y ÚNETE A LA COMUNIDAD DE

Hik-Partner Pro

Asistente comercial de seguridad en la punta de sus dedos.

- Accede a información y beneficios exclusivos.
- Utiliza herramientas y funciones para potenciar tu negocio.
- Brinda servicios de valor agregado.

Escanea el **código QR** para descargar la aplicación **Hik-Partner Pro.**

Consulta el portal en **www.hik-partner.com**

@HikvisionMx
www.hikvision.com/mx

Hikvision México
sales.mexico@hikvision.com

Gana AJAX premios Security & Fire Excellence Awards 2024

- *Mejor fabricante de sistemas de seguridad y de protección contra incendios.*
- *Ganador en la categoría de Alarma anti intrusión o producto de disuasión exterior del año.*

La empresa internacional de tecnología y el mayor fabricante europeo de sistemas de seguridad, Ajax Systems, sigue alcanzando nuevas cotas. Anunció que ha sido reconocido como el mejor fabricante de sistemas de seguridad y de protección contra incendios en los prestigiosos premios Security & Fire Excellence Awards 2024 en el Reino Unido. La empresa recibió el reconocimiento en esta categoría a través de una votación abierta de profesionales de la industria.

Los premios anuales Security & Fire Excellence Awards, apoyados por IFSEC & FIREX, sirven de referencia para reconocer los logros más destacados en los sectores de la seguridad y de la protección contra incendios. Los premios reconocen a las empresas y personas que han demostrado un rendimiento excepcional, soluciones de vanguardia y dedicación a la mejora de la seguridad a escala mundial.

"Estamos felices de haber sido reconocidos en los premios Security & Fire Excellence Awards 2024. Este reconocimiento refleja la dedicación de nuestro equipo a la creación de soluciones de vanguardia que establecen nuevos estándares en el sector", señaló Valentine Hrytsenko, director de Marketing.

"Estamos muy orgullosos de que Ajax Systems haya sido reconocido como el mejor fabricante de sistemas de seguridad y de protección contra incendios del sector. La protección contra incendios siempre ha sido fundamental en nuestra estrategia de innovación, y ganar esta prestigiosa categoría confirma la eficacia, la fiabilidad y la avanzada tecnología de nuestras soluciones", agregó Paul Pope, director Global de Protección contra Incendios.

Constantemente Ajax Systems recibe el reconocimiento de la comunidad profesional británica de la seguridad, en particular de IFSEC & FIREX, que regularmente preselecciona a la empresa como finalista en muchas categorías. En 2017, Ajax Systems fue nombrado ganador en la categoría de Alarma anti intrusión o producto de disuasión exterior del año. La empresa fue reconocida como finalista de cuatro premios y ganó en la categoría de Iniciativa ESG de seguridad o protección contra incendios del año en los premios Security & Fire Excellence Awards 2023.

Tras estos logros, el KeyPad TouchScreen Jeweller ganó el premio PSI Premier Awards 2024 como Producto de control de acceso del año. La empresa fue reconocida como el mejor fabricante de equipamiento de seguridad para casas inteligentes en los premio Security Awards 2024 en el Reino Unido, organizados por Corporate Vision.

ASIS INTERNATIONAL | CAPÍTULO MÉXICO 217

ACOMPÁÑANOS A NUESTRAS REUNIONES MENSUALES

- 14 ENERO — IPS
- 11 FEBRERO — PROTEGE
- 4 MARZO — TimeWeb
- 1 ABRIL — TU MARCA AQUI
- 6 MAYO — SIS PROTEC
- 24 JUNIO — EXPO SEGURIDAD SEPSISA SEGURIDAD PRIVADA
- 8 JULIO — COSEPROS SERVISEG
- 5 AGOSTO — ASIS LATAM&CA 2025 TU MARCA AQUI
- 2 SEPTIEMBRE — GSX detecta
- 7 OCTUBRE — MÉXICO IPSB SUMMIT
- 11 NOVIEMBRE — TU MARCA AQUI
- 2 DICIEMBRE — Multiproseg

REUNIONES MENSUALES 2025 RM — ASIS CAPÍTULO MÉXICO 217 — LIVE STREAMING — PAPRISA

AFÍLIATE Y SÉ PARTE DE NUESTRA COMUNIDAD

ASIS INTERNATIONAL	ASIS INTERNATIONAL | CAPÍTULO MÉXICO 217	ASIS INTERNATIONAL | CAPÍTULO MÉXICO 217
MEMBRESÍA INTERNACIONAL	**MEMBRESÍA CAPÍTULO MÉXICO**	**RENOVACIÓN CAPÍTULO MÉXICO**
125 USD	**$5,650 MXN**	**$3,750 MXN**

Contáctanos en Linktree*

#ASISxTIyPARATI

Revolucionando el control de acceso por reconocimiento facial con Salto Orion, una solución innovadora

SALTO WECOSYSTEM

INSPIRED ACCESS

▪ La mejor solución de su clase que prioriza la comodidad, la privacidad, la seguridad y una experiencia de usuario sin fisuras

Salto Orion es la primera solución de control de accesos con reconocimiento facial del mercado que sólo requiere la cara del usuario como credencial.

Al requerir únicamente la cara del usuario como credencial de acceso, Orion tiende un puente entre el control de acceso y la tecnología de reconocimiento facial. Con Orion ponemos la experiencia del usuario en primer plano para conseguir un acceso sin llave más rápido, seguro, cómodo y privado.

Cada usuario obtiene acceso sin esfuerzo a través de una credencial de acceso genuinamente única -su rostro-, eliminando la necesidad de llaves o tarjetas físicas. Esta innovadora tecnología agiliza el proceso de acceso y mejora la seguridad al eliminar por completo el riesgo de pérdida o robo de credenciales.

Además, Salto Orion proporciona un desbloqueo de puertas rápido y sin fricciones. El usuario sólo tiene que acercarse al punto de acceso, mirar el terminal Orion-C y la puerta se desbloquea.

Salto Orion es una solución completa de control de accesos. Combinando nuestra gama de algoritmos innovadores, hardware y soluciones de software, Orion ofrece tiempos de respuesta rápidos y altos niveles de seguridad, con la confianza de la marca.

Orion, la próxima evolución del control de accesos

Salto Orion representa un nuevo tipo de experiencia de acceso inteligente para organizaciones de cualquier tamaño. Seguro, conectado, sin contacto y fácil de instalar, configurar y utilizar, aprovecha la avanzada tecnología de reconocimiento facial de Salto para mejorar el control de acceso en todas las puertas.

Con esta innovación, Salto está redefiniendo la forma en que las personas acceden a los espacios. Salto Orion es la mejor solución de su clase que prioriza la comodidad, la privacidad, la seguridad y una experiencia de usuario sin fisuras.

Disponible en negro, Salto Orion se puede reservar hoy y está disponible a partir de enero.

salto
INSPIRED ACCESS

ORION

LA INNOVADORA SOLUCIÓN DE ROSTRO COMO CREDENCIAL

Garantice un acceso seguro con la tecnología de reconocimiento facial más avanzada. Permita a los usuarios acceder utilizando sólo la cara como credencial única, eliminando la necesidad de llaves físicas, tarjetas de acceso o credenciales móviles. Salto Orion agiliza y optimiza el proceso de acceso, mejorando la seguridad al eliminar el riesgo de pérdida o robo de credenciales. Con Orion, puede obtener un control total sobre instalaciones de cualquier tamaño, todo desde una única fuente.

Aplicación
Potente tecnología de reconocimiento facial que redefine la forma en que las personas acceden a los espacios.

Tecnología
Orion simplifica el reconocimiento facial, garantizando un funcionamiento rápido, preciso y sin contacto.

Capacidades
Orion ya está integrado en Salto Space, la plataforma de control de acceso inteligente todo en uno.

Prestaciones
Orion ofrece un tiempo de respuesta rápido, que permite a los usuarios acceder a cualquier punto de entrada de Salto rápidamente y sin problemas en menos de un segundo.

Tecnología de fibra óptica para protección de grandes sitios

- Útil para la protección de cercas, rejas, muros o combinaciones diversas de barrera físicas que se utilizan habitualmente en entornos de alta seguridad.
- La serie EchoPoint™ utiliza un avanzado algoritmo de clasificación de reconocimiento de patrones para ayudar a analizar los tipos de intrusiones.

Las soluciones perimetrales de fibra óptica utilizan fibras sensibles a las vibraciones que se integran en barreras físicas, como mallas o muros, o se entierran bajo tierra. La fibra óptica detecta cambios de presión, vibraciones o movimientos causados por un intruso que intenta escalar, cortar, perforar o traspasar el perímetro. Al detectar vibraciones o movimientos cuando un intruso intenta traspasar el perímetro, estos sistemas proporcionan alertas tempranas que permiten a los equipos de seguridad responder rápidamente antes de que se produzca la intrusión, mitigando la amenaza posible.

Las soluciones de fibra óptica de OPTEX son especialmente útiles para la protección de cercas, rejas, muros o combinaciones diversas de barrera físicas que se utilizan habitualmente en entornos de alta seguridad, como centrales eléctricas, prisiones, bases militares y aeropuertos. La serie EchoPoint™ DAS utiliza la tecnología de fibra óptica más avanzada en la actualidad y ofrece una opción en aplicaciones donde haya necesidad de enterrarse, montarse en mallas, muros o implementarse en modo híbrido, proporcionando un método de detección discreto y a prueba de manipulaciones para proteger lugares sensibles sin necesidad de equipos visibles, eliminando puntos de falla sobre el perímetro.

Los sistemas de fibra óptica son extremadamente resistentes a los daños ambientales, particularmente a la inducción por tormentas eléctricas, campos EM o RFI, incluso son intrínsecamente seguros, lo que los hace muy fiables en entornos difíciles y condiciones adversas.

Localización precisa de puntos hasta 100 km

La serie EchoPoint™ utiliza algoritmos de detección inteligentes para localizar con precisión la ubicación de una intrusión de +/- 6 m en un rango de hasta 100 km. La localización del punto se ve favorecida por la zonificación virtual que se configura para dividir el sistema en múltiples áreas de detección definidas por software que pueden oscilar entre 10m-100k. Esta detección altamente precisa y fiable hace que los sensores sean ideales para proteger grandes perímetros y lugares de seguridad de alto riesgo en los que es fundamental localizar e identificar el punto exacto de intrusión.

Algoritmos avanzados y clasificación

Los sistemas EchoPoint™ utilizan un avanzado algoritmo de clasificación de reconocimiento de patrones para ayudar a analizar los tipos de intrusiones. En una aplicación de vallado, puede clasificar y reconocer los intentos de intrusión, como el corte en la cerca, escalamientos, o trepar por encima apoyándose de una escalera, lo que puede ser útil para determinar cualquier punto débil o predecir el comportamiento futuro del intruso. En una aplicación enterrada, el EchoPoint puede identificar si las vibraciones son causadas por pisadas humanas, o por excavación manual, con máquinas o paso de vehículos. Del mismo modo, esta información puede utilizarse para mejorar la configuración de seguridad, fortaleciendo aún más un emplazamiento.

Facilidad de uso y fiabilidad

Los sensores Echo Point se han diseñado pensando tanto en su facilidad de uso como en su alta fiabilidad. Nos hemos asegurado de que el EchoPoint sea fácil de instalar, ajustar y gestionar con una interfaz fácil de usar y sencilla, lo que hace que todo el sistema sea muy fácil de manejar. Está altamente automatizado y la resolución de problemas puede realizarse fácilmente dentro o fuera de las instalaciones, lo que le ofrece más opciones.

Lo que lo diferencia son las funciones de tolerancia a cortes y redundancia del sistema para evitar fallos del sistema y resistir intentos de manipulación, que no siempre se encuentran en otros sensores de fibra óptica. Las medidas de redundancia de sistema garantizan que, en caso de fallo de un procesador, el segundo procesador tomaría automáticamente el relevo para asegurarse de que el sistema sigue operativo y el perímetro se mantenga activo.

Fiber SenSys

AN OPTEX GROUP COMPANY

FSI intrusion detection systems are used to protect the most important information, facilities and resources of government, military and private sector agencies world-wide.

Fiber technology will detect climbing, crawling, cutting fences and drilling through walls and ceilings.

You can now utilise the Fibre Optic technology in a buried setting.

Seguridad regional: Lo que nos dejó 2024 y lo que se viene en 2025

Fernando Vaccotti
Capitán de Navío®, Phd CPO
Uruguay
Articulista invitado

Montevideo, Uruguay.- El año 2025 comenzó de manera vertiginosa. La conflictividad a nivel global parece mantenerse en su máximo nivel histórico -*56 conflictos armados*- de acuerdo con la información. Desde la caída de Ecuador en el caos provocado por el crimen organizado en ese país, hasta cómo los gobiernos afrontan los desafíos políticos planteados por poderosos grupos criminales, este periodo parece presentarse como otro punto de inflexión en la ya casi permanente y estructural batalla entre el bien y el mal.

La reciente asunción del Presidente Trump en EE. UU., planteó una serie de nuevos enfoques en todo lo referente al manejo y la administración de esa potencia y en particular lo vinculado estrictamente a seguridad y defensa, ha generado rápidamente efectos de todo tipo a nivel diplomático, geopolítico, geoeconómico, social y hasta ha sido fundamental en un acuerdo de cese al fuego e intercambio de rehenes en el ya extenso conflicto entre Israel y Hamás, demostrando la importancia de este nuevo liderazgo internacional.

24 horas antes había comenzado el acuerdo de cese al fuego e intercambio de rehenes en el marco del conflicto Israel – Hamás para el cual la intervención de Trump fue clave. En un histórico discurso, entre otras cosas dijo: "Nuestra soberanía será restablecida. Se restablecerá nuestra seguridad. Se reequilibrará la balanza de la justicia. Se pondrá fin al armamentismo despiadado, violento e injusto del Departamento de Justicia y de nuestro gobierno".

Es decir, que, sin haber siquiera asumido, el "efecto Trump" ya daba sus primeros resultados entre otros en el mundo de la guerra. Y es que hay que pensar en el *conflicto* como concepto que siempre o casi siempre se asocia al poder y en todo lo que se mueve y se maneja alrededor de ello.

¿Qué es la FTO y sus alcances?
Una ley de 1996 le posibilitó a EE. UU. crear una lista de Organizaciones Terroristas Extranjeras (FTO, por sus siglas en inglés). La gestiona el Departamento de Estado, y hoy la integran *75 grupos y personas físicas*, que van desde las yihadistas Al Qaeda y Estado Islámico, pasando por la palestina Hamás, hasta las FARC y el ELN en Colombia y Sendero Luminoso en Perú.

Para combatir las organizaciones mexicanas que controlan el tráfico de drogas, el gobierno estadounidense ha utilizado de forma constante la Ley de Designación de Cabecillas de Narcóticos Extranjeros de 1999, más conocida como la "ley de capos" (Kingpin Act).

Impacto 2025 en la seguridad regional

En otros casos están siendo alojados en nuevos establecimientos que van a estar dedicados a este tipo de delincuentes. En un hecho sin precedentes, El Salvador ha firmado acuerdos de cooperación con EE.UU. que incluyen la utilización de la mega cárcel (CECOT) para la internación de delincuentes deportados.

La cárcel de Guantánamo en la isla de Cuba, está siendo reacondicionada y destinada a recibir criminales condenados.

La región está convulsionada y el personal profesional a cargo de las tareas de seguridad, más que nunca debe realizar una muy buena lectura de esta situación. La estrecha colaboración entre seguridad pública y privada debe concretarse en acciones preventivas y en planes de todo tipo pues el COT no va a detener sus acciones y por el contrario, las mismas van a recrudecer.

Ha quedado atrás o está quedando atrás una era de liderazgo político débil en la región.

Por estos motivos, la tarea del profesional de seguridad es cada vez más importante y se debe trabajar a todo nivel para jerarquizarla, no solo profesionalmente si no trabajar en la formación ética del profesional de seguridad.

En la medida en que la seguridad privada se haga respetar y sea vista con buenos ojos, será un eslabón clave en esta lucha que se ha entablado contra el "Universo del mal", como le llamamos comúnmente a ese sector que, desde las oscuridades, se encarga de destruir vidas y llevar el caos a la sociedad.

Latinoamérica sufre y al decir de calificados colegas, "*A fin de cuentas, el enfoque transaccional ayuda a explicar por qué la resistencia al crimen organizado en LAC ha decaído en primer lugar:* ***cuando todo está en venta, nada es sagrado***".

¡Únetenos!

CON SEGURIDAD
Magazine Latam

Síguenos en

Telegram e Instagram

@conseguridadmagazine

¿Todo es cuestión de actitud?

José Paulino González
Coach de alto desempeño y especialista en seguridad.
EE.UU.
Articulista invitado

Quizás en Tik Tok...

Hace algunos años, un joven de mi equipo me pidió una reunión para decirme que quería hacer carrera en el departamento de *IT Security*. Deseaba formar parte de ese equipo y quería saber si yo podía recomendarlo. Le apasionaba el tema, tenía experiencia en seguridad física y siempre demostraba una actitud positiva acompañada de un gran espíritu de servicio. Sin embargo, había una limitación importante: no tenía idea de lo que era un *firewall* y apenas sabía identificar el *software* adecuado para redactar un documento. Yo sabía que contaba con la actitud correcta y la pasión necesaria porque ya tenía algún tiempo formando parte de mi equipo de trabajo, pero no era necesario ser un entrevistador experto para saber que no poseía las competencias técnicas para integrarse al equipo de *IT Security*.

Recomendarlo en esas condiciones habría sido una irresponsabilidad absoluta de mi parte, ya que lo habría afectado tanto a él como al resto del equipo y quizás a toda la organización. La buena noticia es que estas habilidades y competencias pueden desarrollarse. Sabiendo que aún no estaba listo para el cargo, diseñamos un plan que le permitiera adquirir las competencias necesarias. Siguió el plan con disciplina y, después de un par de años, logró obtener la posición que tanto deseaba. (la paciencia es indispensable porque los resultados inmediatos solo existen en las redes sociales).

Un líder de seguridad entiende la importancia de la actitud, tanto la propia como la de los miembros de su equipo, especialmente si estos tienen contacto directo con clientes internos o externos. Sin embargo, también reconoce que la actitud por sí sola no es suficiente, y que basar un proceso de selección o plan de carrera de un colaborador únicamente en este criterio eleva los niveles de riesgo y genera vulnerabilidades innecesarias.

En seguridad, no basta con ser una persona optimista, empática y entusiasta; además de las caracteristicas de la personalidad que conforman la actitud, es absolutamente indispensable contar con las competencias, habilidades y destrezas necesarias para el desempeño de sus funciones. La idea de que "todo es 100% actitud" es un mito urbano lleno de romanticismo que puede servir para Tik Tok o para una campaña de marketing, pero no tiene fundamento en el complejo y cada vez más exigente mundo de la seguridad.

Una ecuación que me gusta para resumir todo este punto es la que comparte Victor Kuppers:

(Competencias + Habilidades blandas) x Actitud = Valor o potencial de la persona.

Al igual que este mito sobre la actitud, existen otros que, aunque parezca increíble, aún persisten en tiempos de Inteligencia Artificial. Algunos de ellos son:

- "El líder nace, no se hace".
- "La jerarquía o la posición me darán el liderazgo que necesito".
- "Como líder de seguridad, debo tener el control y la última palabra".

Escríbenos tu opinión y cuéntanos si conoces otros mitos y quieres compartirlos con la comunidad.

Protección ejecutiva digital

Héctor Robles Conde
President LAM, VP Global Operations.
FIRSTCALL
México
Articulista invitado

¿Qué es la protección digital ejecutiva y cómo funciona?

La protección digital ejecutiva (DEP, por sus siglas en inglés) se refiere a la salvaguardia de individuos de alto perfil, como CEOs, políticos, celebridades y otros ejecutivos, contra amenazas cibernéticas. Estas amenazas pueden incluir hackeos, filtraciones de datos, acoso en línea, Doxxing y robo de identidad. La DEP combina medidas de ciberseguridad, prácticas de higiene digital personal y monitoreo continuo para garantizar la seguridad digital y la privacidad de estos individuos.

Componentes de la Protección Ejecutiva Digital

Evaluación de riesgos y perfiles

- Evaluación de vulnerabilidades: Identificación de debilidades en la huella digital del ejecutivo, incluyendo redes sociales, cuentas de correo electrónico y otras presencias en línea.
- Inteligencia de amenazas: Recolección y análisis de información sobre amenazas potenciales de diversas fuentes, incluyendo la web oscura y redes sociales.

Higiene cibernética y capacitación

- Educación y capacitación: Enseñar a los ejecutivos y sus familias sobre las mejores prácticas en ciberseguridad, como la creación de contraseñas seguras, reconocer intentos de phishing y métodos de comunicación segura.
- Comunicación segura: Asegurar el uso de canales de comunicación encriptados para discusiones y transacciones sensibles.

Tecnologías y medidas proyectivas

- Seguridad de dispositivos: Instalación y mantenimiento de software de seguridad en todos los dispositivos, incluyendo programas antivirus, cortafuegos y VPNs.
- Redes seguras: Configuración de redes Wi-Fi seguras y uso de VPNs para proteger los datos transmitidos por internet.
- Encriptación de datos: Asegurar que los datos sensibles estén encriptados tanto en tránsito como en reposo.

Monitoreo y respuesta

- Monitoreo continuo: Uso de herramientas para monitorear la huella digital del ejecutivo en tiempo real en busca de signos de compromiso o amenazas emergentes.
- Respuesta a incidentes: Tener un plan robusto para responder rápidamente y mitigar cualquier incidente de seguridad, incluyendo la notificación a las partes relevantes, contención de la brecha e inicio de procedimientos de recuperación.

Protección de información personal

- Minimización de datos: Reducir la cantidad de información personal disponible en línea eliminando datos innecesarios y asegurando que las configuraciones de privacidad estén correctamente configuradas.
- Gestión de reputación: Monitorear y gestionar menciones en línea y contenido potencialmente dañino para proteger la reputación del ejecutivo.

Convergencia física y digital

- Seguridad integrada: Combinar medidas de protección física (como guardaespaldas personales) con seguridad digital para proporcionar una protección integral.
- Control de acceso: Asegurar que el acceso físico a dispositivos y redes esté restringido y monitoreado.

Cómo funciona la protección ejecutiva digital

1. Evaluación inicial: Realizar una evaluación exhaustiva de la presencia digital actual del ejecutivo e identificar vulnerabilidades.

2. Implementación de medidas de protección: Desplegar herramientas y protocolos de seguridad para proteger contra las amenazas identificadas, y Educar al ejecutivo y su familia sobre las mejores prácticas en ciberseguridad.

3. Monitoreo continuo:
- Utilizar herramientas avanzadas de monitoreo para observar actividades sospechosas o brechas.
- Actualizar regularmente las medidas de seguridad para adaptarse a nuevas amenazas.

4. Respuesta y recuperación de incidentes:
- Responder rápidamente a cualquier incidente, conteniendo y mitigando el daño. - -
- Investigar las brechas para comprender el vector de ataque y prevenir futuras ocurrencias.

5. Revisiones y actualizaciones regulares:
- Realizar revisiones periódicas de la postura de seguridad digital del ejecutivo.
- Actualizar la capacitación y las medidas de seguridad en línea con las amenazas emergentes y los avances tecnológicos.

La protección digital ejecutiva es un proceso continuo que requiere vigilancia, adaptabilidad y un enfoque proactivo ante las amenazas cibernéticas en evolución. Al integrar medidas de protecciónd digital integrales, los ejecutivos pueden proteger su privacidad y mantener la integridad de sus vidas personales y profesionales.

El análisis cualitativo en seguridad en tiempos de la IA

▪ Una falsa dicotomía entre dos recursos complementarios.

José María Amarilla
CPP EIE, Miembro del Consejo Consultivo Latino de IFPO
Paraguay
Articulista invitado

Asunción, Paraguay.- "La mente humana es un sistema sorprendentemente eficiente y elegante que opera con una cantidad limitada de información. No trata de lesionar correlaciones a partir de datos, sino que intenta crear explicaciones". Noam Chomsky, gran pensador contemporáneo, muy crítico de la Inteligencia Artificial.

En la contemporánea gestión integral de riesgos, los estudios cualitativos siguen siendo esenciales en la era de la Inteligencia Artificial, por un sinnúmero de razones, mientras que la IA proporciona herramientas indispensables para la pronta y eficiente respuesta a diversos niveles de amenaza.

En primer lugar, la protección de la vida y los bienes de las personas –propósito final de cualquier principio de seguridad—requiere de una comprensión profunda del comportamiento humano, tanto en sus aspectos asociativos como en los anómicos, como el de la criminalidad, las amenazas y las vulnerabilidades.

Los recursos cualitativos como los estudios de seguridad, entrevistas en profundidad y grupos focales, permiten explorar y comprender las experiencias, motivaciones y comportamientos humanos de una manera que los datos cuantitativos no pueden. La IA, por su parte, facilita el procesamiento de grandes volúmenes de datos que pueden respaldar la toma de mejores decisiones, mientras los estudios cualitativos revelan el "por qué" de esos datos.

La IA a menudo se basa en datos estructurados y grandes conjuntos de información. Los estudios cualitativos, por su lado, proporcionan un contexto analítico detallado que ayuda a interpretar y reconstruir esos datos, ofreciendo "insight" comprehensivos que justifican la etimología de la palabra "inteligencia", la cual deriva del latín "interligare": Vincular datos e ideas diversas o aparentemente inconexas.

Los métodos cualitativos aplicados a la seguridad tienen también la capacidad de identificar fenómenos emergentes que aún no están reflejados en los datos cuantitativos, como por ejemplo las vulnerabilidades particulares de una corporación, nuevas tendencias delictivas, las amenazas emergentes y otros aspectos analíticos. Esto es crucial para la generación de políticas de prevención, donde la IA puede no tener datos históricos suficientes.

Por otro lado, los estudios cualitativos aseguran que la tecnología y la IA se desarrollen con una comprensión profunda de las necesidades y experiencias humanas en materia de seguridad, promoviendo el diseño centrado en el usuario y la ética en el desarrollo tecnológico, por ejemplo, en la protección de la privacidad y los derechos individuales.

La implementación de IA tiende a tener efectos sociales significativos y crecientes que suplantan tareas ancestrales, pero los estudios cualitativos mantienen un rol clave en evaluar estos impactos, asegurando que sean tomadas en cuenta las perspectivas, derechos y preocupaciones de las comunidades de interés.

En definitivas, todo indica que, mientras la IA ofrece capacidades poderosas para el análisis de datos a gran escala, los estudios cualitativos se mantendrán cruciales para comprender el contexto humano detrás de esos datos, garantizar un enfoque ético centrado en el usuario, y explorar nuevos fenómenos sociales que afectan a la seguridad y protección del ser humano.

La combinación de ambos enfoques, y no la falsa contradicción entre ellos, permite un análisis más robusto y una mejor toma de decisiones, para el cumplimiento de la máxima de la Seguridad Humana: "vivir libres de miedo y protegidos de toda perturbación".

Amenazas cibernéticas son el mayor riesgo para el crecimiento empresarial en general

- Las infraestructuras críticas en América Latina son muy vulnerables, careciendo de estructuras básicas, como identificación de escenarios de ciberataques con el perfil de sus agresores identificados.

Dr. Antonio Celso Ribeiro Brasiliano
PhD, Doctor en Filosofía en Ciencias de la Seguridad Internacional, Cambridge International University, Inglaterra. Presidente de Brasiliano INTERISK.
Brasil
Articulista invitado

São Paulo, Brasil.- Un estudio realizado por la aseguradora Chubb, en alianza con Harris Poll, señaló que la ciberseguridad se ha convertido en la principal preocupación entre los líderes empresariales de Estados Unidos y Canadá. De las 500 empresas encuestadas, 74% consideró que las violaciones cibernéticas y fugas de datos eran las amenazas más graves para la sostenibilidad de su negocio. Estos riesgos han superado con creces otros desafíos, como los cambios regulatorios y las inestabilidades políticas, lo que pone de manifiesto el importante impacto financiero y operativo de los ciberataques.

Además de la ciberseguridad, la disrupción tecnológica fue otro factor destacado en el informe, en especial, debido al creciente uso de la Inteligencia Artificial en el sector corporativo. Casi el 80% de las empresas dijeron que estaban implementando herramientas basadas en IA, pero muchas informaron preocupaciones sobre los riesgos asociados, como la manipulación de datos y la creación de información errónea. Las medianas empresas fueron las más afectadas por los desafíos tecnológicos, con un 60% que experimentó dificultades relacionadas con la integridad de los datos y transformación digital.

El informe también reveló que las pequeñas empresas son particularmente vulnerables a los problemas financieros. Alrededor del 70% citó las dificultades de flujo de caja como uno de los mayores obstáculos para el crecimiento, mientras que la inflación y el aumento de las tasas de interés también se mencionaron como barreras significativas. A pesar de esto, los líderes reconocen la importancia de proteger sus operaciones y el 89% planea expandir sus pólizas de seguro, especialmente contra ataques cibernéticos e interrupciones del negocio.

Entre las estrategias de mitigación más utilizadas, se señaló el monitoreo constante de incidentes cibernéticos como la práctica más eficiente, siendo esencial para el 41% de los ejecutivos. Este enfoque refleja una creciente preocupación por abordar de manera proactiva las amenazas en

lugar de simplemente reaccionar a los incidentes. Sin embargo, más de un tercio de los encuestados admitió que sus empresas aún no son completamente efectivas en la gestión de riesgos emergentes, lo que demuestra la necesidad de avances en este campo.

El estudio, titulado Risk Decisions 360°: Emerging Risks That Can Impede Sustainable Company Growth, se realizó con empresas de diferentes tamaños y sectores. Señaló que desafíos como ciberseguridad, cambio climático y daño reputacional por eventos en redes sociales se han intensificado en los últimos años. Para los expertos de Chubb, el informe sirve como una advertencia para que las empresas inviertan en soluciones más robustas e integradas, que les permitan adaptarse a un entorno empresarial cada vez más complejo y digitalizado.

2 mil ataques de ransomware a infraestructuras críticas

Un proyecto mantenido por la Universidad de Temple, EE.UU., ha documentado más de 2 mil ataques de ransomware dirigidos a infraestructuras críticas desde 2013. Conocida como Critical Infrastructure Ransomware Attacks (CIRA), la base de datos ofrece una visión completa de estos incidentes, incluida información sobre víctimas, industrias afectadas, grupos de amenazas involucrados y montos de rescate exigidos y pagados.

Los sectores considerados objetivos incluyen instalaciones gubernamentales, salud pública y educación. Por el contrario, áreas como reactores nucleares, defensa, productos químicos y el agua siguen estando entre las menos atacadas. El estudio también identificó un aumento significativo en los montos de rescate exigidos, con demandas de más de 5 millones USD que crecieron sustancialmente en los últimos años.

La iniciativa es ampliamente utilizada por investigadores, gobiernos y profesionales de la ciberseguridad para la formación, el análisis de tendencias y el desarrollo de políticas de respuesta a incidentes. Sus mantenedores planean ampliar la cobertura de incidentes fuera del mundo occidental y mejorar la calidad de los datos disponibles. También consideran organizar desafíos anuales de inteligencia de código abierto (OSINT) para complementar la base de datos con información adicional.

El proyecto, disponible de forma gratuita previa solicitud, ha sido solicitado más de mil 500 veces y se ha convertido en un recurso valioso para comprender y mitigar las amenazas de ransomware contra infraestructuras críticas.

Cabe destacar que en numerosos artículos escritos para esta revista, ya habíamos comentado que las infraestructuras críticas en América Latina siguen siendo muy vulnerables, careciendo de estructuras básicas, como identificación de escenarios de ciberataques con el perfil de sus agresores identificados. El efecto final deseado: EFD. Sin inversión en estructuras básicas, las zonas seguirán secando hielo, es decir, seguirán patinando en la lucha contra los ciberataques.

Ciberseguridad en tecnología operacional; claves para proteger infraestructuras críticas

● La creciente digitalización y conectividad de estos sistemas los hace más vulnerables a ciberataques, lo que podría tener consecuencias devastadoras en infraestructuras críticas como energía, agua y transporte.

Dr. Gustavo Hernández
Académico y experto en ciberseguridad en LATAM
IPN/ITESM/Ciberlac/Coladca Internacional
México
Articulista invitado

Las infraestructuras críticas —como el suministro de agua, la energía y el transporte— son fundamentales para nuestra sociedad. Sin embargo, su creciente dependencia de la Tecnología Operacional (OT) las convierte en objetivos prioritarios para actores maliciosos. Este artículo explora principios esenciales para proteger entornos OT, desarrollados por organismos de ciberseguridad global como el Australian Cyber Security Centre (ACSC), proporcionando un marco para la toma de decisiones informada en contextos de alta complejidad técnica.

1. La seguridad como prioridad máxima
La seguridad en OT trasciende lo digital, afectando directamente la vida humana y el medio ambiente. Controles de ciberseguridad mal implementados pueden derivar en fallos catastróficos. Esto exige medidas como sistemas de recuperación predecibles y el desarrollo de arquitecturas capaces de operar bajo los estándares más altos, incluso en situaciones críticas. Además, la integración de la ciberseguridad como parte inherente de las estrategias de continuidad es esencial.

2. Conocimiento profundo del negocio
La defensa efectiva de OT empieza con un entendimiento detallado de los sistemas críticos, sus interdependencias y la arquitectura necesaria para protegerlos. Identificar procesos vitales permite diseñar controles de seguridad que garantizan la resiliencia operativa, minimizan interrupciones y optimizan recursos. Involucrar equipos interdisciplinarios de OT y TI es crucial para lograr una visión completa del ecosistema.

3. Protección estratégica de datos OT
Los datos OT, como configuraciones de controladores y diagramas de redes, representan una mina de oro para los adversarios, facilitando ataques dirigidos. Minimizar el acceso y la distribución de estos datos, implementar repositorios protegidos y monitorizar accesos son estrategias clave. Métodos como tokens canarios pueden alertar sobre accesos no autorizados y aumentar la capacidad de respuesta temprana.

4. Segmentación y segregación de redes
La separación efectiva entre redes OT, TI e internet es un principio básico, pero debe evolucionar para incluir protecciones contra interconexiones entre organizaciones y proveedores. La gestión y administración de sistemas críticos deben realizarse desde redes de alta seguridad para mitigar el riesgo de compromisos escalados. La segmentación debe aplicarse también dentro de la red OT, adaptándose a niveles de confianza y criticidad.

5. Seguridad en la cadena de suministro
La creciente interdependencia de dispositivos y servicios de terceros amplía las superficies de ataque en OT. Cada componente, desde periféricos hasta proveedores de servicios gestionados, debe ser evaluado rigurosamente. Esto incluye verificar la procedencia del firmware, asegurar firmas criptográficas y evitar prácticas que introduzcan vulnerabilidades, como conexiones directas a internet desde sistemas críticos.

6. El factor humano como primera línea de defensa
Los operadores y técnicos de campo son esenciales para la detección y respuesta a incidentes en OT. Invertir en capacitación, fomentar una cultura de ciberseguridad basada en la seguridad física e integrar la ciberseguridad en procesos operativos son estrategias esenciales. Además, es vital que las observaciones de posibles incidentes sean valoradas y respondidas sin generar barreras organizacionales.

En consideraciones finales, el panorama de la ciberseguridad en Tecnología Operacional (OT) está en constante evolución, impulsado por tendencias emergentes y desafíos globales. Según informes recientes, el año 2024 ha registrado un incremento sin precedentes en ciberataques, con pérdidas globales estimadas en 10,000 millones de euros, duplicando las cifras del año anterior[1].

La Inteligencia Artificial (IA) ha jugado un papel dual en este contexto. Por un lado, ha sido utilizada por ciberdelincuentes para perfeccionar y personalizar ataques, aumentando su precisión y efectividad. Por otro lado, la IA también se presenta como una herramienta defensiva crucial, capaz de detectar y mitigar amenazas de manera proactiva. Sin embargo, su implementación conlleva desafíos, como la necesidad de transparencia en los modelos utilizados y la gestión de posibles sesgos.

En respuesta a estas amenazas, la Unión Europea ha fortalecido su marco regulatorio con la Directiva NIS 2, que entró en vigor en octubre de 2024. Esta directiva establece requisitos más estrictos en materia de ciberseguridad para sectores críticos, incluyendo la implementación de autenticación multifactor, cifrado de datos y auditorías periódicas de vulnerabilidades. Se estima que alrededor de 100,000 nuevas empresas deberán cumplir con estas normativas, enfrentando sanciones significativas en caso de incumplimiento.

La protección de los sistemas OT se ha convertido en una prioridad estratégica. La creciente digitalización y conectividad de estos sistemas los hace más vulnerables a ciberataques, lo que podría tener consecuencias devastadoras en infraestructuras críticas como energía, agua y transporte. Organizaciones como el Instituto Nacional de Estándares y Tecnología (NIST) han destacado la urgencia de fortalecer la seguridad en OT, proporcionando guías actualizadas para abordar estas amenazas[2] .

En este contexto, es imperativo que las organizaciones adopten un enfoque proactivo y holístico en ciberseguridad, integrando tecnologías avanzadas, cumpliendo con las regulaciones vigentes y fomentando una cultura organizacional que priorice la seguridad en todos los niveles. La colaboración internacional y la inversión en capacitación continua serán fundamentales para enfrentar los desafíos presentes y futuros en el ámbito de la ciberseguridad en OT.

Referencia:

Australian Signals Directorate's Australian Cyber Security Centre. (2024). Principles of Operational Technology Cyber Security. Disponible en https://www.cyber.gov.au.
Australian Signals Directorate's Australian Cyber Security Centre. (2024). Principles of Operational Technology Cyber Security: Quick Reference Guide. Disponible en https://www.cyber.gov.au.
Cadena SER. (2024). ¿Qué cambia la directiva de la UE que mejora la ciberseguridad y ya aplican los Estados?. Disponible en https://cadenaser.com/cmadrid/2024/10/22/que-cambia-la-directiva-de-la-ue-que-mejora-la-ciberseguridad-y-ya-aplican-los-estados-ser-madrid-sur/.

Impacto transformador de la **computación cuántica** en la economía del Reino Unido

- El objetivo es permitir a los usuarios entrar en los edificios cuando sea necesario, al mismo tiempo de mantener a los invitados fuera de sitios no autorizados y espacios prohibidos.

Juan José Velásquez Olarte
CMO Quanpaths
Colombia
Articulista invitado

Bogotá, Colombia.- un informe reciente ha destacado el enorme potencial transformador de la computación cuántica en la economía del Reino Unido. Esta tecnología tiene el poder de revolucionar diversas industrias al resolver problemas complejos que los ordenadores clásicos no pueden abordar, lo que impulsará avances en Inteligencia Artificial, ciencia de materiales y farmacéutica.

Se espera que los ordenadores cuánticos sean millones de veces más potentes que los superordenadores actuales, permitiendo resolver problemas computacionales imposibles para la tecnología tradicional. Este avance podría generar mejoras significativas en múltiples sectores económicos y científicos. Industrias como las finanzas, salud y logística podrían beneficiarse enormemente gracias a simulaciones más rápidas, algoritmos de optimización y métodos de encriptación más seguros.

El informe sugiere que, si el Reino Unido logra la viabilidad comercial de la computación cuántica para 2035, la economía podría experimentar un aumento del 1% en la productividad ese año. Este crecimiento podría llegar al 4% en 2040, al 7% en 2045 y al 8% en 2050. Para ponerlo en perspectiva, un aumento del 8% en la productividad equivaldría a que cada trabajador produjera el equivalente a tres semanas adicionales de trabajo al año sin incrementar sus horas laborales. Estas ganancias podrían fortalecer la resiliencia económica del Reino Unido y sostener un crecimiento a largo plazo, especialmente en un entorno digital en constante evolución.

Sin embargo, el informe enfatiza que, para que el Reino Unido aproveche plenamente estas oportunidades y mantenga su competitividad global en el sector cuántico, será esencial un mayor apoyo gubernamental. La inversión en investigación, desarrollo y formación será clave para hacer de la computación cuántica una realidad comercialmente viable y beneficiosa para la economía del país. Los responsables políticos deberán considerar estrategias de financiación, colaboraciones con empresas tecnológicas líderes e iniciativas educativas para dotar a la fuerza laboral con las habilidades necesarias para aprovechar todo el potencial de la computación cuántica.

Además, no se deben ignorar las implicaciones éticas y de seguridad de esta tecnología. La capacidad de los ordenadores cuánticos para romper los códigos criptográficos actuales plantea preocupaciones sobre amenazas a la ciberseguridad, lo que hace crucial el desarrollo de métodos de encriptación post-cuántica. Garantizar un desarrollo y despliegue responsable de la computación cuántica será fundamental para maximizar sus beneficios mientras se mitigan los riesgos.

A medida que el Reino Unido avanza en esta frontera tecnológica, la inversión continua, la formulación estratégica de políticas y la colaboración entre sectores serán determinantes para el impacto que la computación cuántica tendrá en la economía del país. Si se aprovecha correctamente, esta tecnología podría allanar el camino hacia un futuro más innovador, eficiente y próspero para el Reino Unido.

BLINDAJES ETTS

CREAMOS LA SOLUCIÓN IDEAL PARA TI

Nos especializamos en **BLINDAJE** con un nivel de **excelencia** que asegura tu **protección** y completa **satisfacción.**

VEHÍCULOS TÁCTICOS

55 6010 7863

www.etts.com.mx

Visita nuestro sitio:

BLINDAJE

INDUSTRIA EN EXPANSIÓN, TECNOLOGÍA Y DESAFÍOS

▪ La Industria del blindaje en auge por inseguridad global: Con un aumento del 29% en la venta de vehículos blindados en México en 2023, el sector se expande a nivel mundial, consolidando al país como la segunda potencia de blindaje en Latinoamérica, detrás de Brasil.

Beatriz Canales Hernández

El blindaje es una herramienta importante para la seguridad global, tanto en el ámbito gubernamental como en el sector privado. A medida que las amenazas aumentan, gobiernos han reforzado sus estrategias de defensa, y en tanto que diferentes empresas están invirtiendo en tecnologías para proteger a sus fuerzas de seguridad, funcionarios y población vulnerable.

Hay regiones en las que el crimen organizado y el terrorismo representan un riesgo constante; los vehículos y equipos blindados han pasado de ser un recurso exclusivo de las fuerzas militares a convertirse en una necesidad básica para garantizar la operatividad de las agencias de seguridad y determinados sectores civiles.

En 2022, la industria mexicana del blindaje automotriz registró ventas de 3,500 unidades para el mercado nacional. Del total de transacciones, 65% correspondió al Nivel III, mientras que el 15% fue de Nivel IV, 16% de Nivel V y el restante porcentaje se destinó a blindajes superiores.

En este contexto, en México se impulsa la industria del blindaje con una ascendente demanda tanto del sector público como del privado. La creciente ola de violencia ha llevado a más ciudadanos y empresas a invertir en protección balística.

"Cada vez más personas buscan protección para sus hogares y vehículos. En particular, ha crecido la demanda de blindaje automotriz en niveles bajos, que protegen contra armas cortas y son adecuados para entornos urbanos", explica Leopoldo Cerdeira Morán, presidente de la Asociación Intercontinental de Blindadores (AIB).

El blindaje vehicular ha aumentado significativamente, con especial interés en Niveles II y III, ideales para la protección en la ciudad. En el sector logístico, muchas empresas han comenzado a blindar sus camiones ante el aumento de asaltos en carreteras.

El gobierno ha reactivado la adquisición de blindajes tácticos: "Durante el sexenio pasado hubo muy pocas adquisiciones, pero en 2024 se dieron nuevas licitaciones y compras de blindaje para las Fuerzas Armadas", señala Cerdeira Morán.

La tecnología ha permitido que los blindajes sean más ligeros y eficientes, agrega el especialista, quien señala que hace 30 años, un blindaje de Nivel II pesaba alrededor de 140 kg. Hoy, gracias a materiales avanzados como el kevlar, el peso se ha reducido sin sacrificar protección.

Sin embargo, la industria enfrenta el reto del blindaje clandestino, con talleres no certificados que ofrecen soluciones sin control de calidad. "El problema radica en el mercado clandestino. Existen talleres informales que instalan blindajes sin certificaciones, poniendo en riesgo la vida de los usuarios", advierte el presidente de la AIB.

Leopoldo Cerdeira Morán
Presidente de la AIB

Con una proyección de crecimiento del 50% anual, el blindaje en México sigue consolidándose como una necesidad más que una medida ostentosa. "La seguridad no es un lujo, es una inversión en tranquilidad", concluye el presidente de la AIB Leopoldo Cerdeira M.

Con la intensificación de las Fuerzas Armadas en la adquisición de vehículos blindados para enfrentar amenazas en zonas de alto conflicto, requieren blindaje no como una adquisición de fastuosidad, sino como una necesidad operativa para proteger a sus elementos en zonas de conflicto, como lo explica Gadi Mokotov, presidente del Consejo Nacional de la Industria de la Balística (CNB).

La tecnología ha avanzado al punto en que los blindajes no solo resisten impactos de alto calibre, sino que también protegen contra explosivos y ataques con drones.

Esta creciente inversión en blindaje por parte del gobierno mexicano se ha visto reflejada en múltiples sectores de seguridad pública.

Destacamos que, en el primer semestre de 2023, la venta de vehículos blindados en México se incrementó un 29% respecto al mismo periodo del año anterior, según datos de la Asociación Mexicana de Blindadores de Automotores (AMBA).

Desde la Guardia Nacional hasta cuerpos especializados de policía y Fuerzas Armadas, ha sido una pieza clave en la protección de sus efectivos. Se han adquirido unidades tácticas blindadas, especialmente para operativos en zonas de alto riesgo donde el crimen organizado mantiene presencia activa.

"La delincuencia ha evolucionado en sus métodos de ataque, y eso nos obliga a reforzar las estrategias de defensa. El blindaje no solo protege a los elementos de seguridad, sino que también ofrece mayor confianza y disuasión en las operaciones", afirma el presidente del CNB.

Gadi Mokotov
Presidente del Consejo Nacional de la Industria de la Balística (CNB).

El blindaje de aeronaves y embarcaciones también ha sido un tema de interés en la última década, con avances en materiales más ligeros y resistentes que permiten una mejor movilidad y protección sin comprometer el desempeño operativo.

El auge del blindaje en el sector privado

Si bien el blindaje gubernamental sigue siendo un pilar clave de la industria, el sector privado ha experimentado un crecimiento sin precedentes en los últimos años. La inseguridad en ciudades y carreteras ha llevado a empresarios, ejecutivos y ciudadanos comunes a invertir en protección balística para su movilidad diaria.

El sector privado ha experimentado un crecimiento en la demanda de servicios de blindaje, registrando un aumento del 12% con respecto a periodos anteriores. Del total de ventas de vehículos blindados en 2022, el 65% correspondió al Nivel III, mientras que el 15% fue de Nivel IV, el 16% de Nivel V y el restante porcentaje se destinó a blindajes superiores.

"Antes, el blindaje se limitaba a altos ejecutivos y funcionarios públicos. Hoy, vemos solicitudes de blindaje en ciudades donde nunca se había requerido", señala Mokotov. Esta tendencia se ha visto reflejada en un aumento de la demanda de vehículos blindados en estados como Nuevo León, Jalisco, Veracruz y Guanajuato, donde el crimen organizado ha incrementado su presencia.

Los vehículos más blindados en México siguen siendo camionetas SUV de alta gama como Chevrolet Suburban, Jeep Grand Cherokee y Toyota Land Cruiser, pero también ha crecido la demanda de blindaje en sedanes más accesibles como Volkswagen Jetta y Toyota Camry.

"El acceso a blindajes de calidad ya no es exclusivo de vehículos de lujo; ahora es posible blindar casi cualquier modelo sin comprometer su funcionalidad", señala Esteban Hernández López, presidente de la Asociación Mexicana de Blindadores de Automotores (AMBA).

Una de las tendencias más marcadas en los últimos años ha sido el blindaje de vehículos de carga y transporte de mercancías. Con el incremento de los asaltos en carreteras, especialmente en estados como Puebla, Veracruz y Tamaulipas, las empresas han optado por proteger sus unidades para minimizar pérdidas y salvaguardar la vida de sus operadores, comenta el directivo.

Esteban Hernández
Presidente de la AMBA

"La inseguridad en las carreteras ha aumentado drásticamente. Hemos visto casos donde transportistas han sido atacados con armas largas, lo que ha llevado a un aumento en la demanda de blindajes en el sector logístico", afirma Hernández López. En estos casos, los blindajes recomendados son Nivel IV y Nivel V, dependiendo del riesgo de la zona.

Es así como las empresas de transporte han comenzado a blindar no solo sus unidades, sino también sus instalaciones y centros de distribución, ante el temor de ataques coordinados por bandas criminales. En muchas zonas, los operativos de seguridad han resultado insuficientes, obligando a las compañías a tomar medidas de protección por su cuenta.

La tecnología e innovación en el blindaje son clave.

El desarrollo tecnológico ha sido estratégico para mejorar la eficiencia del blindaje sin comprometer la funcionalidad del vehículo. Las empresas buscan materiales más ligeros que permitan mantener el rendimiento y la seguridad.

"La tecnología nos permite fabricar blindajes más resistentes con menor peso, optimizando la movilidad y reduciendo el desgaste del vehículo", comenta Gadi Mokotov. La investigación en materiales como el kevlar de última generación y aleaciones metálicas ultraligeras ha sido fundamental en este proceso.

Uno de los mayores desafíos es la adaptación del blindaje a los vehículos eléctricos e híbridos. Estos modelos requieren técnicas especializadas debido a la presencia de baterías de alto voltaje y sistemas electrónicos avanzados.

Además, la implementación de blindajes inteligentes, que incluyen cristales con capacidades electrónicas avanzadas, sistemas de monitoreo y detección de impactos en tiempo real, ha comenzado a ganar popularidad en el mercado de protección personal.

¿Qué pasa en México?

México es el segundo mercado de blindaje más grande de Latinoamérica, detrás de Brasil. Sin embargo, se distingue por la calidad y profesionalización del blindaje, con un énfasis en la seguridad integral de los vehículos.

"Brasil lidera en volumen con más de 17 mil unidades blindadas al año, pero en México trabajamos con niveles más altos de protección y con estándares que nos han convertido en una referencia internacional", explica Gadi Mokotov.

El país también ha ganado reconocimiento con eventos como el Congreso del blindaje, donde expertos de diversas partes del mundo se reúnen para conocer las innovaciones en la industria.

El CNB trabaja con las autoridades para cerrar el acceso de materiales blindados a la delincuencia organizada, evitando que estos terminen en manos de grupos criminales.

Uno de los problemas más graves que enfrenta la industria es la proliferación de empresas clandestinas que ofrecen blindajes de baja calidad sin certificaciones: "Hay compañías que venden supuestos blindajes que no cumplen con los estándares de seguridad. Esto pone en riesgo la vida de los usuarios y genera competencia desleal", advierte Esteban Hernández, titular de la AMBA.

Las perspectivas de crecimiento para la industria del blindaje en México

Se proyecta una tendencia positiva, con un estimado de crecimiento del 15% para 2025. Se

espera que el mercado continúe en expansión, impulsado por la inseguridad y la necesidad de protección.

"Mientras la violencia y la impunidad sigan presentes, la demanda de blindaje continuará creciendo", concluye Gadi Mokotov, presidente del CNB.

Tendencias en el Blindaje

La integración de nuevas tecnologías, la mejora en la regulación del sector y la expansión hacia mercados internacionales serán los pilares para consolidar a México como un referente mundial en la industria del blindaje.

La industria del blindaje sigue evolucionando con avances en materiales como Kevlar EXO y Tensylon, desarrollados por DuPont para mejorar la protección balística con menor peso y mayor resistencia.

"El blindaje no es un lujo, sino una necesidad operativa", enfatiza Marcelo Fonseca, director de protección balística de DuPont en Latinoamérica.

El blindaje vehicular en México ha crecido más en el sector civil y empresarial que en el gubernamental en los últimos años. En 2023, se registraron aproximadamente cuatro mil 500 vehículos blindados en México, con una proyección de 5,500 a 6,000 unidades para 2024.

Con la creciente demanda, la industria enfrenta retos en regulación y calidad, ya que la proliferación de empresas sin certificaciones ha puesto en riesgo la seguridad de los usuarios: "No hay milagros en blindaje. Si el precio es demasiado bajo, hay que sospechar de la calidad", advierte Marcelo Fonseca.

Marcelo Fonseca
Director de protección balística
de DuPont en Latinoamérica

De esta manera, el blindaje en México ha pasado de ser un lujo para convertirse en una necesidad para distintos sectores de la sociedad. Esta es una industria en crecimiento y la constante innovación, y consolida al blindaje como un actor clave en el mercado. Sin embargo, el reto es garantizar productos de calidad, regulados y accesibles para quienes lo requieren.

Además, mientras la inseguridad persista, la demanda de blindaje continuará en ascenso, impulsada por nuevas tecnologías y regulaciones cada vez más estrictas.

Gestionando los riesgos asociados a los *stakeholders* (TPRM) desde la privacidad y protección de datos

"Quien tiene la información tiene el poder"
Thomas Hobbes. El Leviatán

Carmen Rincón
CPO
Venezuela
Articulista invitado

Caracas, Venezuela.- Mas allá de las consideraciones de seguridad y cumplimiento normativo (compliance), debe entenderse que cuando las organizaciones priorizan la gestión de riesgos e incluyen a las terceras partes interesadas o stakeholders a fin de evaluar una línea base de comportamiento, el desempeño previo y la mayor parte de los riesgos relacionados con cada uno de ellos, también se adentrarán en aspectos referidos a la privacidad y la protección de datos que de forma iterativa se producen en la cadena de valor de nuestros productos o servicios

Los tomadores de decisiones pueden guiarse hacia una gestión operativa robusta y eficiente mediante un enfoque holístico que aborde riesgos reputacionales y de contagio asociados con:

- Clientes (incluyendo los clientes de tus clientes, según la industria y normativa).
- Proveedores.
- Los competidores dentro de nuestra industria.
- Entes y autoridades gubernamentales.
- Redes sociales, publicidad y marketing.
- Comunidades de interés.

Una buena gobernanza corporativa, procesos uniformes y un enfoque basado en riesgos para evaluación, análisis y monitoreo, junto con una infraestructura que soporte transacciones constantes y datos en tiempo real, son esenciales. Este ecosistema contribuye a la escalabilidad y rentabilidad del negocio, determinando el valor empresarial y fomentando el crecimiento estratégico.

Entre las opciones de tratamiento para este tipo de riesgos, se sugiere:

- Involucrar a los dueños de procesos para evaluar exhaustivamente los activos de información de terceros en la matriz de riesgos.
- Garantizar relaciones comerciales basadas en transparencia y ética, sin comprometer la capacidad de hacer negocios.
- Tratar la información confiada con las mejores prácticas, incluyéndola en métricas operativas para evaluar riesgos asociados a datos de terceros.

Los stakeholders tienen el poder de influir en el éxito o fracaso de una organización, generando expectativas para mantener negocios éticos. En un entorno complejo, los negocios éticos dependen de un flujo continuo de datos e información en la cadena de valor, con políticas, normas y procedimientos adecuados para garantizar integridad, protección de la información, privacidad y confidencialidad.

Es útil realizar un autoanálisis estratégico con preguntas como:

¿La organización informa a los stakeholders sobre la recolección y uso de información privilegiada en procesos de compras y abastecimiento?

¿Las áreas de ventas y marketing recaban suficiente información de los clientes para evaluar riesgos?

¿Las encuestas de satisfacción del cliente obtienen datos segmentados y sensibles, comprometiéndose a su uso y resguardo adecuado?

¿La página web corporativa permite gestionar el consentimiento y borrar datos, dirigiendo a la política de privacidad y cookies aceptadas?

Ejemplos de consideraciones:

- Proveedores de servicios en la nube: Cualquier vulnerabilidad en la seguridad del proveedor o subcontratista puede afectar tus datos.
- Servicios de TI subcontratados: Subcontratar tareas por operatividad o costos introduce riesgos adicionales.
- Logística y cadena de suministro: Múltiples subcontratistas para el transporte y almacenamiento plantean sus propios riesgos.

Reflexiones finales:

1. Para ser un profesional integral en plena revolución tecnológica le conviene familiarizarse con los términos protección, seguridad y privacidad de datos, disciplinas diferentes con un objetivo común: Salvaguardar la información.
2. En Latinoamérica, los cambios legislativos en privacidad y protección de datos avanzan a diferentes ritmos. Algunos países siguen el modelo europeo RGPD, como Argentina y Brasil, mientras otros están legislando, como Chile, República Dominicana, Uruguay y Venezuela ya tienen una base constitucional.
3. La evaluación y selección de proveedores, políticas claras, monitoreo y auditoría continua, gestión de riesgos de ciberseguridad, capacitación y concienciación son clave para mantener no solo la reputación e integridad de la organización y sus relaciones comerciales sino su estabilidad financiera.

Gestión comunicacional en crisis: El rol decisivo de la seguridad corporativa en la resiliencia empresarial

Cintia Gutiérrez
Dos décadas en el ámbito de la seguridad física, tecnológica y operativa. Líder en entornos corporativos de alta exigencia. Es Gerente Operativa en Securion S.A. y preside el board de ASIS International Argentina.
Argentina
Articulista invitada

La nueva dimensión de la comunicación en tiempos críticos

Buenos Aires, Argentina.- En un escenario empresarial marcado por la volatilidad y la exposición constante a riesgos operacionales, cibernéticos y reputacionales, la comunicación se ha convertido en una herramienta crítica de supervivencia organizacional. Lejos de ser una función meramente informativa, la comunicación en contextos de crisis representa un eje estratégico que puede definir la continuidad o el colapso de una organización.

Las crisis ya no son eventos excepcionales, son realidades frecuentes en un mundo interconectado. Por ello, el diseño de protocolos comunicacionales debe integrarse plenamente dentro del Programa de Protección Organizacional (POA), tal como lo establece el marco internacional de ASIS International, bajo estándares como ISO 22361, ISO 22301 e ISO 27001.

La comunicación se reconoce como un factor transversal de gobernanza y resiliencia. No se trata únicamente de emitir mensajes, sino de garantizar coherencia, oportunidad y control en la circulación de información crítica. Esto implica contar con voceros entrenados, procedimientos preestablecidos y estructuras jerárquicas claras para actuar con precisión ante situaciones de emergencia.

"El silencio en una crisis puede ser tan dañino como una respuesta errónea. La anticipación y el liderazgo en la comunicación son vitales para contener el daño y preservar la confianza".

Desde la mirada del profesional de seguridad, la articulación entre seguridad física, tecnológica y comunicacional es imprescindible para una respuesta eficaz.

Uno de los desafíos más sensibles durante una crisis es gestionar la narrativa pública. En la era digital, donde las redes sociales amplifican versiones y distorsiones a velocidad exponencial, tener una narrativa sólida, empática y fundamentada en hechos verificables es esencial para preservar la reputación y mantener el control del mensaje.

Recomendaciones ISO 22361:2022:

- Identificar audiencias críticas.
- Usar canales confiables y segmentados.
- Mantener coherencia y transparencia.
- Alinear mensajes con los valores institucionales.

La gestión del mensaje debe ser dinámica y coherente, ajustándose a los cambios del contexto sin perder integridad.

Toda crisis implica disrupciones. Por eso, la comunicación debe vincularse estrechamente con los planes de continuidad del negocio (ISO 22301) y los protocolos de ciberseguridad (ISO 27001), especialmente frente a incidentes como:

- Ciberataques o ransomware.
- Filtraciones de datos sensibles.
- Fallos tecnológicos en infraestructuras críticas.

La coordinación entre seguridad, IT, asuntos legales y relaciones institucionales garantiza integridad comunicacional y resguardo legal.

La eficacia comunicacional no se improvisa, se entrena. El uso de simulacros integrales permite:

- Evaluar el tiempo de respuesta.
- Medir la eficacia de los canales utilizados.
- Validar la capacidad de los voceros institucionales.

ISO 22398 promueve estos ejercicios como parte del ciclo de mejora continua. Incluir escenarios realistas, stakeholders relevantes y presión mediática simulada hace que el entrenamiento se asemeje al contexto real de una crisis.

El cierre de una crisis debe dar paso a la reflexión. Analizar el desempeño de los equipos de comunicación permite:

- Corregir deficiencias.
- Reforzar buenas prácticas.
- Actualizar procedimientos.

En tiempos de crisis, comunicar con estrategia es proteger activos, personas y reputación. El rol del profesional es fomentar una cultura de preparación, liderazgo y adaptabilidad, asegurando que la comunicación no solo informe, sino que inspire confianza y facilite la recuperación.

"Las crisis no se pueden evitar, pero una comunicación acertada puede transformarlas en oportunidades de crecimiento institucional".

Siniestros aumentan 151% desde el 2021

▪ Esto debido a actividades por sismo, ciclones e incendios en el hogar. En el país, una de cada cuatro viviendas (24%) cuenta con algún tipo de cobertura ante diversos riesgos.
▪ Uno de cada cuatro incendios asegurados (25%) ocurren por corto circuito o falta de mantenimiento en instalaciones eléctricas.

Desde el año 2021, el número de siniestros en los hogares mexicanos causados por incendios, sismos o riesgos hidrometereológicos aumentó 151%, hasta superar los 42 siniestros asegurados cada día, en promedio, esto de acuerdo con los últimos datos disponibles de la Asociación Mexicana de Instituciones de Seguros (AMIS).

Al final de 2023, se registraron poco menos de 53 mil siniestros en viviendas aseguradas, dentro de un universo de poco más de 8.4 millones de hogares; esto representa el 24% de las viviendas en México, es decir, casi una de cada cuatro, de acuerdo con las cifras del último censo del Instituto Nacional de Estadística y Geografía (INEGI).

"El hogar no es solo donde vivimos, para muchas familias es un lugar de trabajo y donde convivimos más que nunca. Desde la pandemia, el tiempo en casa ha aumentado, pero también los riesgos: instalaciones eléctricas sobrecargadas, fugas y accidentes domésticos son cada vez más frecuentes. A pesar de esto, menos del 7% de los hogares en México están asegurados de manera voluntaria, dejando a millones de familias desprotegidas ante pérdidas por algún riesgo como incendio, sismo o ciclones", explica Carlos O. Jiménez, director de Daños y Autos de la AMIS.

Las principales causas de los incendios en el país son corto circuitos y falta de mantenimiento en instalaciones eléctricas, así como rayos, lluvias, ciclones y sismos. Estas agrupan el 30% de todos los siniestros en viviendas en México.

"El hogar es más que un espacio físico, es donde construimos nuestras vidas. La prevención y reducción de riesgos es esencial para tratar de evitar que ocurran; pero cuando suceden necesitamos herramientas que nos permitan los recursos para recuperarnos rápido: un seguro de hogar no solo protege el patrimonio, protege a quienes más amas frente a cualquier desastre. Nuestra casa lo merece, nuestra familia también", agregó Carlos Jiménez.

Acciones preventivas

En el caso de los corto circuitos e instalaciones eléctricas, es fundamental realizar un mantenimiento regular de las instalaciones para evitar siniestros. Esto se traduce en revisar que todos los cables y apagadores estén en buen estado, y se recomienda no sobrecargar los contactos múltiples. También es conveniente instalar dispositivos de protección como interruptores de descargas o diferenciales de voltaje, para prevenir corto circuitos.

En cuanto a las filtraciones de agua, se debe revisar periódicamente las tuberías y conexiones, y reparar cualquier fuga de inmediato, por menor que parezca.

Coberturas más comunes

Aunque la oferta de coberturas en el mercado es amplia, las pólizas más comunes ante siniestros en el hogar son:

- Incendio, rayo y explosión (cobertura básica)
- Daños por riesgos hidrometeorológicos
- Sismos y erupción volcánica
- Gastos extraordinarios
- Remoción de escombros.
- Responsabilidad Civil
- Asistencia en el hogar (plomero, cerrajero, entre otros)
- Cristales

Existen varios mitos en torno a los seguros de casa habitación que impiden que las personas protejan su patrimonio.

Por ejemplo, se cree que, debido a que una casa puede tener un valor 4 o 5 veces mayor que un auto, el seguro de casa será 4 o 5 veces el costo del seguro de auto, pero esto es falso. Los riesgos son diferentes, y las inversiones en protección también lo son. De hecho, hay seguros de casa que pueden ser más accesibles que los de algunos autos.

Otro mito común es pensar que si se renta una vivienda no hay pólizas adecuadas, cuando en realidad se puede proteger el mobiliario, electrodomésticos o equipos electrónicos. Por eso, es importante acercarse a agentes, compañías o plataformas digitales para conocer opciones y elegir la que mejor se adapte a las necesidades de cada persona.

Coordinación interinstitucional durante desastres

- Desafíos, lecciones aprendidas y mejores prácticas.

CPT Ariana P. Beaton Torres

Fue comisionada a través de la Universidad de Puerto Rico, Río Piedras. Tiene bachillerato en Comunicaciones de la Universidad del Sagrado Corazón. Graduada de la Army Logistics University en 2022.
En 2018 fue la primera oficial de EOD puertorriqueña tras completar su especialización en NAVSCOLEOD y sirvió en el 65th EOD en Alaska, apoyando misiones como Pacific Pathways y la Defense POW/MIA Accounting Agency.
Comandó la unidad multinacional de EOD y Military Working Dog en el Sinaí, Egipto, gestionando operaciones en 3,107 millas cuadradas. Se unió al séptimo Grupo de Fuerzas Especiales como oficial de operaciones EOD, apoyando operaciones de breaching y supervisando las operaciones de EOD para fuerzas especiales.
Condecoraciones: Meritorious Service Medal, Army Commendation Medal (2ª vez), Army Achievement Medal (4ª vez), Expert Soldier Badge y Explosive Ordnance Disposal Badge.

Puerto Rico
Articulista invitada

Carmen A. (Mely) Torres Rodríguez

Chief Visionary Officer y fundadora de On Point Strategy, firma de consultoría en cumplimiento regulatorio, manejo de desastres y desarrollo organizacional.
Experiencia en planificación estratégica y manejo de recursos, ha fortalecido organizaciones para acceder a fondos y maximizar su impacto.
Tras el huracán María, su firma fue la primera en responder localmente, liderando planes de manejo de emergencia y evaluaciones para asegurar respuestas rápidas.
Combina su experiencia con agencias federales con una visión estratégica, destacándose en liderar equipos multidisciplinarios y gestionar proyectos con impacto positivo.

Puerto Rico
Articulista invitada

San Juan, Puerto Rico.- La respuesta a desastres es un proceso complejo que involucra la participación de múltiples agencias gubernamentales, organizaciones no gubernamentales (ONG), líderes comunitarios y sector privado. Aunque cada uno de estos actores tiene un rol específico y valioso, la falta de coordinación eficiente entre ellos puede resultar en un uso ineficaz de recursos y respuestas desorganizadas que terminan afectando a las comunidades más vulnerables.

Este artículo explora algunos de los principales desafíos que enfrentan las agencias durante un desastre, así como las mejores prácticas para superarlos, con un enfoque en las lecciones que dejo el paso del huracán María.

1. Falta de comunicación clara y estructurada

Uno de los mayores obstáculos en la respuesta a desastres es la falta de una comunicación clara y estructurada entre las agencias participantes. Las diferencias en los sistemas de comunicación, jerarquías organizacionales y cadenas de mando pueden causar retrasos y malentendidos críticos. Durante el huracán María en Puerto Rico, uno de los principales retos fue la desconexión en las líneas de comunicación entre agencias federales y locales, lo que

llevó a respuestas descoordinadas y al mal uso de los recursos, como la entrega de ayuda no organizada por parte de ONG.

• Lección aprendida: Invertir en tecnologías de comunicación resilientes y plataformas colaborativas que aseguren que todas las entidades involucradas puedan compartir información en tiempo real es esencial. Además, es crucial actualizar los planes de comunicación durante la emergencia, estableciendo un enlace dedicado para las ONG, líderes comunitarios y gobierno. Estas medidas aseguran una respuesta más eficiente y ordenada.

2. Duplicación de esfuerzos y uso ineficiente de recursos

Otro desafío común es la duplicación de esfuerzos entre agencias, lo que puede dejar a ciertas áreas desatendidas.

Mejores prácticas: Es clave implementar un Centro de Operaciones de Emergencia (COE) como eje de coordinación, con un Sistema de Comando de Incidentes (ICS) que permita el seguimiento en tiempo real. Cada área, como transportación, logística y seguridad pública, debe tener un enlace en el COE para coordinar acciones.

Esto facilita una delegación eficiente de recursos y una mejor comunicación con el público a través de un portavoz designado. Además, mecanismos de retroalimentación y materiales multilingües ayudan a optimizar la respuesta, garantizando que todas las comunidades sean atendidas. **3. Diferencias en la capacidad de respuesta de las agencias**

Las agencias varían en su capacidad de respuesta, lo que a menudo lleva a desajustes en la colaboración.

• Lección aprendida: Realizar evaluaciones de capacidad previas a un desastre es fundamental. Estas evaluaciones permiten identificar las fortalezas y debilidades de cada entidad y diseñar planes de apoyo mutuo, asegurando que los recursos lleguen a donde más se necesitan y complementando las capacidades de las agencias más pequeñas con las de las más grandes.

4. Desafíos en la coordinación entre sectores públicos y privados

La integración del sector privado en la respuesta a desastres es crucial, pero la falta de preparación y acuerdos previos puede ser un obstáculo.

Mejores prácticas: Fundamental es establecer acuerdos de colaboración entre el sector público y privado antes de un desastre. En el caso del huracán María, la ausencia de preparación para colaborar con el sector privado resultó con demoras.

Desarrollar plataformas de cooperación que alineen las capacidades del sector privado con las necesidades del sector público puede facilitar una respuesta más rápida y efectiva. Además, los procesos de adquisición previos, basados en experiencias pasadas, aseguran una mejor respuesta.

5. Falta de entrenamiento y simulaciones conjuntas

Aunque cada agencia puede estar bien capacitada, la falta de simulaciones conjuntas puede crear brechas en la coordinación durante una emergencia.

• Lección aprendida: Realizar simulacros interinstitucionales anuales es crucial para afinar la respuesta conjunta ante desastres. Estos ejercicios permiten a las agencias identificar y corregir errores antes de una crisis real, fortaleciendo la cohesión entre entidades.

Hacia una respuesta coordinada y eficiente

Para concluir, la coordinación interinstitucional durante un desastre no es solo un desafío logístico, sino una necesidad para salvar vidas y maximizar el uso de recursos. A través de la implementación de tecnologías avanzadas, planificación previa, creación de marcos de colaboración y entrenamiento conjunto, las agencias pueden superar los obstáculos y asegurar una respuesta más rápida y efectiva. Solo una coordinación eficiente puede garantizar que ninguna comunidad se quede atrás en momentos de crisis.

sky world
HI TECH SECURITY & LOGISTICS

RASTREO SATELITAL GPS Y SISTEMAS DE SEGURIDAD

Somos una empresa mexicana creada en 2007 con el objetivo de brindar una **solución al alto índice de robo de vehículos y transporte de carga en México**, teniendo como principal objetivo prevenir el delito y salvaguardar la seguridad de nuestros clientes así mismo brindarle los mejores beneficios

- Seguridad efectiva
- Control de accesos
- Reducción de costos
- Monitoreo 24/7

55 3095 3001
ventas@skyworld.com

www.skyworld.com.mx

De Guardaespaldas a Gestor de riesgos: La evolución de la Protección Ejecutiva

Kevin Palacios
CSSM, CPOI, CPO, CPP, PSP, PCI
IFPO - Latin America Regional Director
Ecuador
Articulista invitado

Introducción

Quito, Ecuador.- El asesinato de Brian Thompson y el fallido ataque contra el entonces expresidente Donald Trump en 2024, hicieron evidentes fallas en la concepción de la protección ejecutiva (EP). Ambos eventos demostraron que, en un mundo donde las amenazas son cada vez más dinámicas, la seguridad personal no puede depender únicamente de la reacción ante un ataque. La protección ejecutiva tradicional, basada en la presencia disuasiva de un guardaespaldas armado, ha evolucionado hacia un enfoque basado en la gestión de riesgos.

EPRM: Nuevos paradigmas en protección ejecutiva

El Executive Protection Risk Management (EPRM) no es solo un marco de gestión, sino un cambio de paradigma en la manera de gestionar la protección de individuos de alto riesgo. Alineada con normas internacionales como la ISO 31000 (Gestión de Riesgos) y la ASIS SRA (Apreciación de Riesgos en Seguridad), el EPRM propone una visión estructurada, sistemática para la toma de decisiones basada en datos en EP.

El marco EPRM se basa en un ciclo continuo de identificación, análisis, evaluación y tratamiento de riesgos, asegurando que las decisiones de protección se basen en gestión de calidad y estén alineadas con los objetivos estratégicos del ejecutivo y su organización. Dentro de este marco, es fundamental definir cuatro niveles de gestión:

- EPM (Executive Protection Manager): Responsable de la gestión estratégica de la seguridad.
- EPL (Executive Protection Leader): Líder del equipo táctico que implementa medidas de protección.
- EPA (Executive Protection Agent): Agentes de seguridad operativos encargados de la protección en el terreno.
- Ejecutivo (Protegido o "Principal"): La persona cuya seguridad es el foco de las estrategias de protección.

El marco EPRM nos muestra que ya no se trata solo de reaccionar ante amenazas, sino de anticiparlas, mitigarlas y gestionarlas operativa – táctica y estratégicamente para minimizar su impacto.

Redefiniendo protección ejecutiva

La protección ejecutiva se define ahora como medidas para mitigación de riesgos diseñadas para garantizar la seguridad de individuos expuestos a riesgos elevados debido a su empleo, estatus, patrimonio, afiliaciones o ubicación geográfica. Estas medidas priorizan protección de elementos críticos como:

- **Persona:** La integridad física del protegido.
- **Información:** Datos en temas personales y organizacionales.
- **Tiempo:** Minimización de interrupciones y retrasos que afecten su productividad.
- **Reputación:** Evitar crisis de imagen.
- **Entourage:** Seguridad del entorno que rodea al protegido (familia, equipo de trabajo, etc.) y demás activos valiosos del protegido.

Bajo este enfoque, la protección ejecutiva se convierte en un pilar de la continuidad del negocio, asegurando que el ejecutivo pueda operar con normalidad sin que la seguridad sea una barrera para sus actividades.

Conclusión: De la reacción a la prevención

El asesinato de Brian Thompson y el intento de magnicidio contra Donald Trump demuestran que los modelos tradicionales de protección ejecutiva han quedado obsoletos. La seguridad ya no puede depender únicamente de la capacidad de reacción ante una crisis; debe basarse en la anticipación, gestión de riesgos y planificación estratégica.

El modelo EPRM representa la evolución de la protección ejecutiva hacia una disciplina que integra seguridad y gestión de calidad. Con un enfoque basado en datos, metodologías internacionales y medidas preventivas, la protección ejecutiva deja de ser un costo operativo para convertirse en una inversión en la continuidad del negocio.

En un mundo donde la incertidumbre es la norma, el éxito no está en responder al peligro, sino en evitar que este se materialice. La suerte no es una estrategia; la gestión de riesgos sí lo es.

Si quieres profundizar en la Gestión de Riesgos en Protección Ejecutiva (EPRM) puedes adquirir el primer tomo de la serie de libros EPRM, aquí: https://amzn.to/418SilH.

un ecosistema tecnológico integral

- *Firma lidera con radios portátiles de última generación, ofreciendo claridad, durabilidad y conectividad en entornos exigentes.*
- *Conecta comunicaciones críticas, centros de mando y seguridad por video para una gestión más eficiente.*
- *Soluciones escalables que se adaptan a las demandas futuras, protegiendo personas y activos estratégicos.*

Más allá de los radios portátiles, Motorola Solutions ofrece un conjunto integral de tecnologías diseñadas para fortalecer la seguridad pública y privada.

Su enfoque se centra en soluciones para:

- Comunicaciones críticas: Sistemas que garantizan conectividad confiable en situaciones de emergencia.
- Centros de mando: Plataformas que integran datos en tiempo real para mejorar la toma de decisiones.
- Seguridad por video: Tecnología avanzada que combina monitoreo visual con análisis inteligente para detectar amenazas potenciales antes de que ocurran.

Iván Kraljevic, ingeniero senior de preventa para América Latina y el Caribe, explica que estas herramientas son escalables y adaptables, atendiendo desde necesidades locales hasta proyectos a nivel estatal o nacional: "La tecnología de Motorola permite a los operadores trabajar en perfecta sincronía, asegurando que cada segundo cuente en situaciones críticas".

Motorola Solutions se encuentra en el centro de la seguridad pública, y se ha convertido en un aliado estratégico para instituciones gubernamentales y empresas privadas. Sus soluciones conectan a fuerzas policiales, servicios médicos, bomberos y centros de llamadas de emergencia, creando un ecosistema colaborativo que mejora la respuesta ante emergencias.

Un ejemplo claro es su integración de sistemas de video con análisis predictivo, que no solo registra eventos, sino que también alerta sobre comportamientos sospechosos en tiempo real. Esto permite a las organizaciones anticiparse a posibles amenazas, reduciendo riesgos y protegiendo vidas.

Compromiso con la innovación

La firma mantiene su compromiso de ofrecer tecnología de vanguardia. Sus dispositivos y sistemas no solo responden a las necesidades actuales, sino que están diseñados para adaptarse a las demandas futuras, pues "la seguridad ya no es solo un servicio; es una inversión estratégica en tecnología que redefine la manera en que protegemos a las personas y los activos", afirma Kraljevic

Se enfatiza que Motorola Solutions no es simplemente un proveedor de tecnología, sino un socio estratégico para las empresas que transforma su comunicación y la seguridad. Sus radios portátiles de dos vías, combinados con soluciones integrales para la gestión de emergencias, redefinen los estándares en sectores clave.

Desde la fábrica hasta la primera línea de respuesta en emergencias, las herramientas de la firma son sinónimo de confiabilidad y eficiencia con comunicación efectiva y altos niveles de seguridad. Motorola Solutions establece de esta manera un estándar de lo que significa estar verdaderamente conectado y protegido.

Gestión de la seguridad corporativa. Habilidades blandas

Alfredo Yuncoza. CSSM. CPOI. CPO
Presidente del Consejo Consultivo Latino de IFPO.
Venezuela

Las habilidades blandas constituyen un activo estratégico para los profesionales de la gestión de la seguridad corporativa. Estas competencias, inherentemente interpersonales y emocionales, no solo optimizan la ejecución de tareas, sino que también fortalecen las relaciones interinstitucionales. En el siguiente apartado se exponen las diez habilidades blandas más demandas en este perfil profesional.

Inteligencia emocional

La inteligencia emocional (IE) se define como la capacidad de identificar, evaluar y gestionar tanto las emociones propias como las de los demás. En el contexto de la seguridad corporativa, esta habilidad se torna esencial para abordar situaciones críticas, incluyendo incidentes y conflictos interpersonales. La IE permite a los profesionales del área responder de manera efectiva ante crisis, optimizando la comunicación y la colaboración entre equipos, lo que resulta en un manejo eficaz de conflictos y una resolución constructiva de disputas. Esto no solo reduce tensiones, sino que también promueve soluciones que benefician a todas las partes involucradas.

La implementación de una alta IE dentro de las organizaciones contribuye a crear un clima laboral positivo, fomentando un ambiente inclusivo que incrementa la satisfacción laboral y disminuye la rotación de personal.

Además, facilita la continuidad operacional al permitir una gestión adecuada de las emociones en situaciones críticas, asegurando que los procesos se mantengan funcionales. La mejora en las relaciones interpersonales derivada del desarrollo de la IE también minimiza errores que podrían comprometer la seguridad organizacional. Asimismo, los empleados que cultivan su inteligencia emocional experimentan un crecimiento personal significativo, lo que se traduce en un aporte valioso al éxito colectivo de la organización.

Comunicación efectiva

La comunicación estratégica se erige como un componente esencial en la gestión proactiva de riesgos de las organizaciones. Establecer canales de comunicación fluidos y transparentes no solo facilita la identificación y mitigación efectiva de amenazas, sino que también promueve una cultura de seguridad integral que permea todos los niveles de la empresa.

Los gestores de seguridad deben ser capaces de adaptar sus mensajes a diferentes audiencias, lo que implica comprender las particularidades y necesidades de cada grupo. Esta capacidad de personalización es crucial para maximizar el impacto de las iniciativas de seguridad y garantizar que todos los empleados, desde la alta dirección hasta el personal operativo, estén debidamente informados y comprometidos.

Además, la escucha activa se convierte en una herramienta indispensable en este proceso. Recoger y considerar las opiniones y preocupaciones de todos los actores involucrados no solo fortalece la confianza en los mecanismos de seguridad, sino que también permite

alinear los objetivos de seguridad con las necesidades y prioridades del negocio. De este modo, se crea un entorno donde la seguridad no es vista como una carga, sino como un elemento integrador que contribuye al éxito organizacional.

Resolución de problemas

La eficacia en la resolución de problemas dentro del ámbito de la seguridad se ve significativamente potenciada por el establecimiento de una cultura organizacional que prioriza la colaboración, la innovación y la mejora continua. Al integrar equipos multidisciplinarios y fomentar un entorno que estimule la creatividad y la generación de ideas, las organizaciones tienen la capacidad de desarrollar soluciones más sólidas y sostenibles que abordan de manera integral los desafíos existentes.

Asimismo, la adopción e implementación de herramientas y tecnologías avanzadas, como el análisis de datos y la inteligencia artificial, no solo agiliza los procesos de resolución de problemas, sino que también optimiza la calidad de las decisiones tomadas. Estas tecnologías permiten a las organizaciones analizar grandes volúmenes de información en tiempo real, identificar patrones y tendencias, y prever posibles riesgos, lo que resulta en una gestión proactiva y efectiva de la seguridad. En conjunto, estos elementos crean un ciclo virtuoso que impulsa la resiliencia organizacional y mejora continuamente los resultados en materia de seguridad.

Adaptabilidad

La adaptación de estrategias de seguridad se ha convertido en un requisito fundamental en el contexto empresarial actual, caracterizado por su dinamismo. En este entorno, los especialistas en seguridad deben exhibir una agilidad constante para hacer frente a las transformaciones del panorama de amenazas y a las variaciones dentro de la organización.

El dinamismo del contexto empresarial moderno implica que las amenazas a la seguridad están en constante evolución, lo que requiere una vigilancia continua y una capacidad de respuesta rápida y efectiva. Los profesionales de la seguridad deben estar preparados para identificar y mitigar riesgos emergentes, adaptando sus estrategias y tácticas a medida que surgen nuevas amenazas.

Además, las variaciones dentro de la organización, como cambios en la estructura corporativa, la adopción de nuevas tecnologías y la expansión a nuevos mercados, también demandan una adaptación constante de las estrategias de seguridad. Los especialistas deben ser capaces de evaluar y ajustar sus enfoques para asegurar que las medidas de seguridad sean adecuadas y efectivas en todo momento.

Liderazgo

El liderazgo en el ámbito de la seguridad se define como la capacidad de articular una visión clara y concisa que guíe los esfuerzos del equipo hacia el cumplimiento de objetivos compartidos. Un líder efectivo en seguridad no solo debe ser un comunicador hábil, sino también un estratega que inspire confianza y colaboración entre los miembros del equipo. Esto implica establecer metas comunes y fomentar un sentido de pertenencia y responsabilidad colectiva. La alineación de los esfuerzos del equipo es esencial para crear un entorno donde la seguridad sea una prioridad compartida, y donde cada individuo se sienta empoderado para contribuir a la protección de la organización.

Un líder en seguridad debe desarrollar e implementar estrategias proactivas que permitan identificar, evaluar y mitigar riesgos de manera efectiva. Esto incluye la realización de auditorías regulares, la capacitación continua del personal y la implementación de políticas que promuevan comportamientos seguros. Fomentar una cultura de seguridad basada en la prevención es fundamental, ya que no solo reduce la probabilidad de incidentes, sino que también mejora la moral y el compromiso del equipo. En este contexto, el liderazgo en seguridad no se limita a cumplir con normativas, sino que se convierte en un motor para la innovación y la mejora continua dentro de la organización.

Empatía

La empatía, desempeña un papel fundamental en la gestión de la seguridad dentro de las organizaciones. Esta habilidad permite a los líderes establecer relaciones interpersonales sólidas y de confianza con sus colaboradores, lo que es esencial para fomentar un ambiente laboral seguro y colaborativo. Al comprender las percepciones individuales de los empleados respecto a los riesgos y las medidas de seguridad implementadas, los gestores pueden diseñar e implementar estrategias de mitigación más efectivas. Esto no solo contribuye a reducir la probabilidad de incidentes, sino que también fortalece la resiliencia organizacional ante posibles adversidades.

Además, la práctica de la escucha activa y el interés genuino por el bienestar del personal son componentes clave para desarrollar una cultura de seguridad robusta. Proporcionar apoyo emocional en situaciones difíciles no solo ayuda a los empleados a sentirse valorados y comprendidos, sino que también promueve un sentido de pertenencia y compromiso con las políticas de seguridad. En este contexto, la empatía se convierte en una herramienta poderosa que permite a

los líderes gestionar no solo los aspectos técnicos de la seguridad, sino también el factor humano, esencial para el éxito sostenible de cualquier organización.

Trabajo en equipo

La gestión efectiva de riesgos requiere un enfoque colaborativo que supere las barreras entre departamentos. Al promover la colaboración multidisciplinaria, las organizaciones pueden identificar y mitigar de manera más eficiente las amenazas a la seguridad. Esta sinergia no solo facilita el intercambio de conocimientos y experiencias, sino que también optimiza la utilización de recursos, lo que conduce a una gestión de riesgos más integral y proactiva.

Provocar un entorno donde diferentes áreas trabajen en conjunto permite a las organizaciones abordar los riesgos desde múltiples perspectivas, enriqueciendo así el proceso de toma de decisiones. Al integrar diversas disciplinas y habilidades, se fortalece la capacidad para anticipar y responder a los desafíos, garantizando una protección más robusta y efectiva frente a posibles incidentes.

Creatividad e innovación

En un entorno empresarial caracterizado por su constante evolución y por la aparición de nuevas amenazas, la capacidad de generar ideas originales y de implementar soluciones disruptivas es crucial. Estas prácticas permiten a las organizaciones anticiparse a los riesgos emergentes, y también fortalecen su resiliencia, asegurando que puedan adaptarse y prosperar en un contexto de incertidumbre.

Fomentar un ambiente que facilite la expresión de ideas innovadoras y que promueva una cultura de aprendizaje continuo se convierte en un imperativo estratégico para las empresas que buscan mantenerse a la vanguardia en seguridad. La creación de espacios donde los colaboradores se sientan motivados a compartir sus perspectivas y a experimentar con nuevas propuestas es fundamental para impulsar la innovación. De este modo, las organizaciones no solo mejoran sus protocolos de seguridad, sino que también desarrollan una mentalidad proactiva que les permite enfrentar los desafíos del futuro con confianza y eficacia.

Gestión del tiempo

La gestión efectiva del tiempo es un pilar fundamental en la construcción de una postura de seguridad corporativa proactiva. Al integrar la gestión del tiempo en las estrategias de seguridad, las organizaciones pueden optimizar la asignación de recursos, priorizar las tareas críticas, y responder de manera más eficiente ante incidentes. A través de técnicas como el análisis de riesgos basado en el tiempo, la planificación de contingencias detalladas y la implementación de sistemas de monitoreo proactivos, es posible identificar y mitigar proactivamente las amenazas a la seguridad. Además, al fomentar una cultura de seguridad en la que la gestión del tiempo sea una prioridad, las organizaciones pueden fortalecer su resiliencia y minimizar el impacto de los incidentes inevitables. En última instancia, la gestión del tiempo no solo es una herramienta operativa, sino una estrategia estratégica para proteger los activos más valiosos de la organización.

Persuasión e influencia.

Los líderes transformacionales se distinguen por su capacidad para influir y persuadir a otros hacia el logro de una visión compartida. Esta habilidad facilita la implementación efectiva de iniciativas de mejora continua, así como también es crucial para cultivar una cultura de seguridad proactiva dentro de las organizaciones. Al articular una visión clara y convincente, estos líderes son capaces de motivar e inspirar a sus equipos, fomentando un entorno en el que cada miembro se siente valorado y comprometido con los objetivos comunes.

Por otra parte, los líderes transformacionales empoderan a sus colaboradores para que tomen decisiones informadas y asuman la responsabilidad de su propio entorno laboral. Este enfoque no solo mejora la moral del equipo, sino que también promueve una mayor participación en las prácticas de seguridad, lo que a su vez conduce a resultados excepcionales. Al integrar estos principios en su liderazgo, se establece un ciclo virtuoso donde la confianza y la colaboración se traducen en un desempeño superior en materia de seguridad, beneficiando tanto a los empleados como a la organización en su conjunto.

Conclusiones

En resumen, las habilidades blandas representan un recurso fundamental para los profesionales involucrados en la gestión de la seguridad corporativa. La integración efectiva de estas competencias interpersonales y comunicativas no solo mejora la protección de los activos organizacionales, sino que también incrementa la productividad y el bienestar general del personal. Estas habilidades permiten a los profesionales establecer relaciones más sólidas y colaborativas dentro de la organización, lo que resulta en una respuesta más ágil y efectiva ante situaciones de riesgo.

Además, al promover una cultura de seguridad proactiva, los especialistas en seguridad contribuyen de manera significativa al cumplimiento de los objetivos estratégicos de la empresa. La capacidad de comunicarse claramente, resolver conflictos y liderar equipos es esencial para implementar políticas que sean aceptadas y adoptadas por todos los niveles de la organización. Este enfoque no solo minimiza las vulnerabilidades, sino que también fomenta un ambiente laboral donde todos los empleados se sienten responsables y comprometidos con la seguridad.

En consecuencia, el desarrollo y fortalecimiento de habilidades blandas en el ámbito de la gestión de seguridad corporativa no deben ser subestimados. Invertir en la capacitación en estas áreas puede resultar en una mejora sustancial en la eficacia operativa y en el clima organizacional, lo que a su vez se traduce en un mayor éxito en el cumplimiento de las metas empresariales a largo plazo.

LABORATORIO DE PROSPECTIVA ESTRATÉGICA PARA PROFESIONALES DE SEGURIDAD

CLAUDIA ÁLVAREZ

PROFESORA DE HABILIDADES DE PENSAMIENTO CRÍTICO (IESA)

MALENA PINTO

PHD. INVESTIGADORA SENIOR EN PENSAMIENTO DE FUTUROS (IESA)

MODALIDAD ONLINE

CUPO LIMITADO A 15 PARTICIPANTES
19 DE MAYO AL 09 DE JUNIO 2025
INFORMACIÓN: +584123993265 / AY.ARCUSGROUP@GMAIL.COM

¡Para el acervo y fomento a la lectura!

Nadie comprende mejor los principios de liderazgo que sustentan el éxito mundial de "Apropiación Extrema" (Extreme Ownership) que sus autores, Jocko Willink y Leif Babin. Con el respaldo de su reconocido equipo de consultoría en Echelon Front, han creado un libro de ejercicios complementario diseñado para maximizar el aprendizaje del libro original. Este recurso de cerca de 90 páginas ofrece herramientas esenciales, orientación práctica y perspectivas profundas para llevar tu comprensión de *Apropiación Extrema* a un nivel superior, ayudándote a triunfar tanto en el ámbito profesional como personal.

Características destacadas del libro:

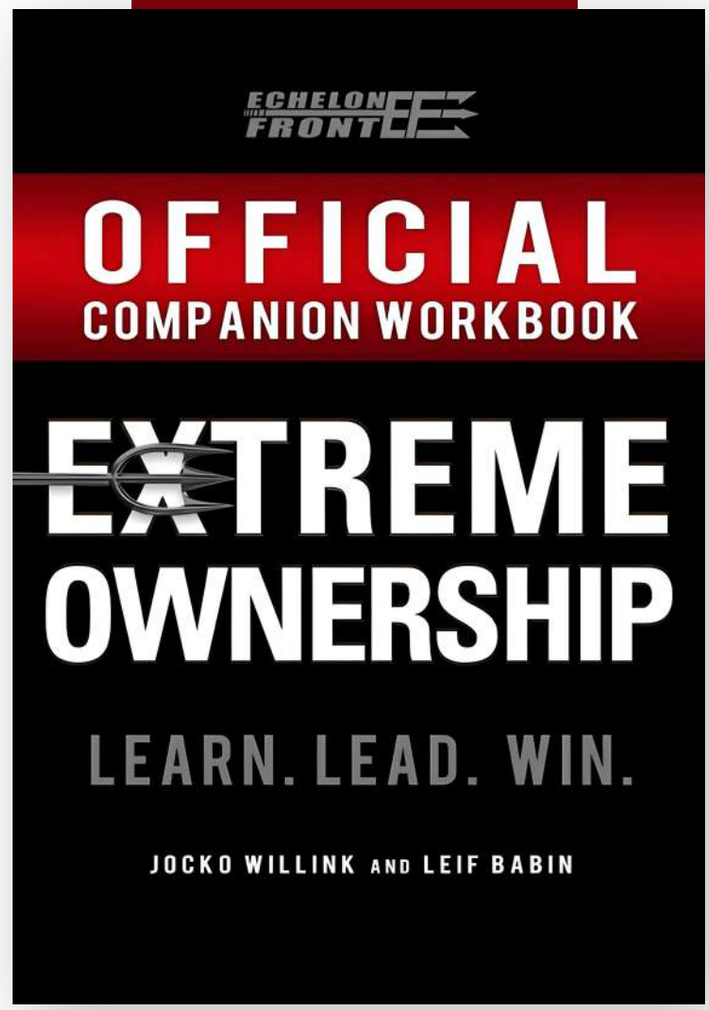
Glosario personalizado: Una sección exclusiva para entender términos y frases clave.

Ejercicios prácticos: Incluye implementaciones con preguntas clave y simulacros de acción inmediata que desafían tus habilidades de liderazgo. Además, cuenta con amplias páginas dedicadas para tomar notas.

Desgloses detallados por capítulo: Cada sección del libro original es analizada facilitando su aplicación práctica.

Método probado: Basado en las mismas lecciones y enfoques utilizados en las conferencias presenciales y la Extreme Ownership Academy en línea de Echelon Front.

Este libro es una herramienta imprescindible para quienes buscan aplicar los principios de liderazgo de *Apropiación Extrema* en su día a día, fortaleciendo su capacidad para liderar con éxito en cualquier entorno.



Libro blanco sobre la función de compliance

Con motivo del décimo aniversario de la Asociación Española de Compliance (ASCOM), la entidad ha presentado la edición 2024 de su Libro Blanco sobre la función de compliance, una versión revisada y puesta al día respecto a la edición original de 2017.

Este documento actualizado incorpora avances significativos en el ámbito del compliance, manteniendo su objetivo fundamental: servir de guía a los profesionales de la función de compliance para delimitar con precisión el alcance de sus responsabilidades y, en consecuencia, las expectativas que los distintos operadores jurídicos, económicos y sociales pueden depositar en ellos.

El Libro Blanco se estructura de forma clara y accesible, evitando ambigüedades que puedan dificultar la comprensión de la función de compliance y del papel de sus responsables en cualquier contexto organizativo. Además, sus directrices se adaptan al marco jurídico aplicable y a las particularidades de cada organización, facilitando así su consulta y aplicación práctica.

El libro en su versión digital puede ser obtenido gratis en la web de ASCOM: asociacioncompliance.com

Tu opinión es muy importante, recomienda otras lecturas

FEINDEF
FERIA INTERNACIONAL
DE DEFENSA Y SEGURIDAD DE ESPAÑA

Madrid. España
12, 13 y 14 mayo 2025

FEINDEF 25

IV Edición de la Feria Internacional de Defensa y Seguridad de España

IFEMA MADRID

Organiza
Fundación Feindef

Con el apoyo institucional de
GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

Contacta con nosotros
o **reserva tu stand**
comercial@feindef.com

feindef.com

ESS+®
FERIA INTERNACIONAL
DE SEGURIDAD

Del 27 al 29
de agosto
Bogotá-Colombia

Tecnología que protege

Un espacio donde usted podrá:

- **Posicionar su marca** entre los líderes que mueven la industria.
- **Generar contactos** clave para nuevas oportunidades de negocio.
- **Participar** en la mayor red de networking del sector.

Reserve su stand en
securityfaircolombia.com
o escaneando el código QR

GREMIOS ALIADOS

ORGANIZAN

MEDIOS ALIADOS