MAYO, 2024

CONNECTASIS225

Comunidad de Profesionales de la Seguridad en Colombia

ASIS EUROPA 2024

en la experiencia de un afiliado

Modelos de competencias en Seguridad Corporativa

¿QUÉ ES UN

SISTEMA DE SEGURIDAD?

DOXXING:

Un tipo de ataque que sin ser ilegal (aún) puede arruinar tu vida

PRUEBAS DE CONFIABILIDAD ¿AVANZAS CON LA TECNOLOGÍA O TE QUEDASTE EN EL TIEMPO?

ASIS INTERNATIONAL® | Bogotá Chapter

MAYO, 2024

CONNECTASIS225

Comunidad de Profesionales de la Seguridad en Colombia

CONTENIDO

03
Editorial

06
¿Qué es un SISTEMA DE SEGURIDAD?

09
Pruebas de confiabilidad ¿Avanzas con la tecnología o te quedaste en el tiempo?

11
ASIS Europa 2024 en la experiencia de un afiliado

14
Modelos de competencias en Seguridad Corporativa

17
Doxxing: Un tipo de ataque que sin ser ilegal (aún) puede arruinar tu vida

CREACIÓN DE LA COMUNIDAD DE AMÉRICA LATINA Y EL CARIBE EN ASIS CONNECTS

Palabras del Chair LACRB - ASIS International

Por: Pablo Colombres, CPP

Estimados miembros del Capítulo 255 Bogotá de ASIS International,

Es para mí un gran honor dirigirme a ustedes en nombre de la Junta Regional de ASIS International para América Latina y el Caribe.

Quiero compartir con ustedes la creación de la Comunidad de América Latina y el Caribe en ASIS Connects. Con esta iniciativa, nuestro objetivo es promover un mayor compromiso, transparencia y colaboración en toda la región. Al fortalecer la conexión entre la junta, los voluntarios y los miembros, aspiramos a impulsar la misión de ASIS International en América Latina y el Caribe.

También es importante compartir información relevante con ustedes. Siguiendo la recomendación del Grupo de Trabajo de Gobernanza 2023, la Junta Regional de LACRB se estableció el 1 de enero de 2024. Los distinguidos miembros de la LACRB son:

- Pablo Colombres, CPP (Chair)
- Marco Vega, CPP (ViceChair)
- Tatiana Scatena (Secretary/Treasurer)
- Basil Bewry, CPP
- Helbert Calderón, CFE, PCI, PSP, CPP
- Alvar Orellana McBride, CPP
- Servio Camey
- Dora Cortés, CPP
- Carlos Contreras
- Alexander Lyle

La LACRB celebra reuniones mensuales a través de Zoom, con la participación de representantes de la sede central. Nuestras actividades han incluido sesiones de orientación e intercambio de liderazgo en enero, seguidas de reuniones en febrero y marzo.

Para el año 2024, la LACRB tiene como objetivo alcanzar diversos objetivos, que incluyen:

- Establecer el marco de gobernanza para la junta regional.
- Implementar una estructura de comités para respaldar las operaciones regionales.
- Desarrollar e implementar métricas para apoyar el nuevo Plan Estratégico de ASIS.
- Promover la comunicación transparente dentro de la región.

Cuatro comités han sido aprobados por el Grupo de Trabajo:

- Comité de Membresía
- Comité de Capítulos
- Comité de Aprendizaje y Eventos
- Comité de Gobernanza y Finanzas

Es importante tener en cuenta que estos comités no se instalarán hasta enero de 2025. Nuestra estructura tradicional de liderazgo regional (ARVP, RVP y SRVP) permanece vigente, y estamos comprometidos en garantizar una transición fluida a los nuevos roles.

Además, hemos aprobado el Plan de Comunicación de la LACRB, que establece nuestros canales de comunicación y protocolos oficiales:

- El inglés será el idioma principal de comunicación a nivel de la junta.
- ASIS Connects será nuestro principal canal oficial de comunicación, con información relevante publicada trimestralmente.
- Se llevará a cabo una reunión anual de membresía de LAC en persona durante el evento Global GSX.
- Todos los grupos de redes sociales se considerarán no oficiales para comunicaciones oficiales.

Quiero asegurarles que estamos comprometidos en construir una junta transparente y accesible que sirva los mejores intereses de todos los miembros regionales.

Antes de concluir, quiero expresar mi gratitud a todos los líderes voluntarios por sus invaluables contribuciones a ASIS International y a la profesión.

Muchas gracias.

Cálidos saludos,

PABLO COLOMBRES, CPP®
CHAIR LACRB - ASIS INTERNATIONAL

AGRADECIMIENTO ESPECIAL

A Nuestros Patrocinadores:

ORGANIZACIÓN G.D.C
GESTIÓN, DESARROLLO Y CRECIMIENTO EMPRESARIAL

SECURITY COLOMBIA

casmar®

SRR Ltda
SEGURIDAD PRIVADA

PROSINTE
Protección y Selección Integral

TRI CLICK

SICUREX
INSTITUTO DE SEGURIDAD METIS

GRUPO CONSULTOR 360

ANDRÓSS
CAPACITACIÓN ESTRATÉGICA PARA LA PREVENCIÓN DE PÉRDIDAS

SD
SEGURIDAD DIGITAL

¿QUÉ ES UN SISTEMA DE SEGURIDAD?

Por: Carlos A Abondano M

Identificados, analizados, valorizados los riesgos de seguridad para la organización, y definidos por ella cuáles se van a intervenir y con qué prioridad, se pasa a la fase de tratamiento de riesgos que es el proceso de selección y puesta en aplicación de medidas para modificar el riesgo. "El tratamiento del riesgo puede implicar evitar el riesgo al decidir no comenzar o no continuar con la actividad que da origen al riesgo; aceptar el riesgo o aumentarlo en búsqueda de una oportunidad; eliminar la fuente de riesgo; modificar la probabilidad; modificar las consecuencias; compartir el riesgo con otra parte o partes (lo que incluye contratos y el financiamiento del riesgo); y retener el riesgo mediante una decisión informada" [1]

Una medida ampliamente utilizada para modificar los riesgos de seguridad es la de implementar un sistema de seguridad. ¿Qué es un sistema de seguridad?

Un sistema de seguridad es un conjunto de partes o elementos que interactúan entre sí para alcanzar un objetivo común: modificar la probabilidad de que se materialicen riesgos de seguridad - a través de acciones de prevención - y modificar las consecuencias si a pesar de las acciones preventivas se materializa un riesgo.

Las partes o elementos que componen un sistema de seguridad se pueden clasificar en cuatro grupos:

- Normatividad
- Personas
- Medios
- Procedimientos

Gráfica SILLA DE CUATRO PATAS
Adaptación de la imagen presentada por José Ignacio Andrés (Instructor AVSEC acreditado por la Agencia Española de Seguridad Aeroportuaria – AESA -. Director y Jefe de Seguridad Privada) en la Ponencia: Seguridad Aeroportuaria, del curso Director de Seguridad, transmitida vía webinar desde Alicante el 11 de marzo de 2021

La gráfica muestra una analogía de un sistema de seguridad con una silla de cuatro patas, cada pata es un grupo de los elementos de un sistema de seguridad, y nos sentamos seguros en la silla cuando tenemos las cuatro patas completas y en perfecto estado. Igual ocurre con un sistema de seguridad. Es eficaz para alcanzar su objetivo cuando se tienen los cuatro grupos completos y en perfecto funcionamiento y además cuando se dirige y controla adecuadamente.

En el grupo denominado NORMATIVIDAD se deben contemplar las leyes, decretos, resoluciones (sean globales, nacionales o locales) relacionadas con el sector al cual pertenece la organización que se quiere proteger con ese sistema de seguridad, estándares de seguridad que se adopten como referencias (ejemplo ISO 18788, ISO 9000, BASC etc.), políticas, reglamentos y normatividad de la propia organización para empleados, proveedores, y otras partes interesadas.

[1] NTC- ISO 3100 – 2001 02 16, Términos y Definiciones, Numeral 2.25

En el grupo denominado PERSONAS se incluye la alta dirección de la organización (que debe liderar la gestión de riesgos), y las personas que la organización designe como responsables de la gestión de las operaciones de seguridad (Ver ISO 18788 – 2015, proceso 5, Liderazgo). Además, todas las personas de la organización y de sus partes interesadas hacen parte del sistema de seguridad, no solo aquellos que llevan el rótulo "seguridad" en su camisa, gorra, uniforme. Y el personal específicamente asignado a las actividades de seguridad, debe ser competente y certificado.

En el grupo MEDIOS, se incluyen los medios técnicos activos o pasivos que se vayan a utilizar según los recursos disponibles y el diseño del sistema de protección que se va a utilizar (Ver artículo "Sistemas de Seguridad: diseño y evaluación" por Mary Lynn García, MS, CPP), preferiblemente utilizando los más capaces (generalmente los de última generación)

En el grupo PROCEDIMIENTOS se incluyen todos los procedimientos operativos (ejemplo procedimiento de control de acceso) y protocolos cuando es del caso (ejemplo protocolo de comunicaciones), y planes como el plan de seguridad, plan de emergencias, planes de contingencia y demás relacionados con manejo de crisis y continuidad del negocio.

Un buen ejemplo de un sistema de seguridad (como lo mencioné en mi artículo anterior "Contratación de Sistemas de Seguridad Física") es el Sistema de Seguridad de la Aviación - AVSEC – que se encarga de prevenir, mitigar y controlar los riesgos asociados con los actos de interferencia ilícita para la gestión de la seguridad hacia los pasajeros, las aeronaves e infraestructura asociada. La seguridad de la aviación cuenta con normatividad muy robusta, que incluye sanciones muy fuertes para quien la incumpla, con personal altamente capacitado y certificado en todas las áreas administrativas, de soporte, y de operaciones incluidas las de seguridad, utiliza medios físicos activos y pasivos de última generación, y todos los procedimientos operativos están normalizados.

Invito al lector a que reflexione cuáles son los elementos que debe reunir en cada grupo (normatividad, personas, medios, procedimientos) un Sistema de Seguridad Física, o un Sistemas de Seguridad de la información, o de ciberseguridad, o de seguridad de personas, o de seguridad y transporte de valores, o de seguridad hospitalaria, o de seguridad petrolera por mencionar solo algunos de los muchos sistemas de seguridad.

Un "sistema de seguridad integral" es un conjunto de sistemas de seguridad que actúan interrelacionados para alcanzar el objetivo de seguridad integral que se ha propuesto la organización. Cada grupo de elementos de ese sistema integral (normatividad, personas, medios, procedimientos) está formado por los correspondientes elementos que aporta cada sistema de seguridad que se está integrando.

No perder de vista que un sistema se define como una entidad con límites y con partes interrelacionadas e interdependientes cuya suma es mayor a la suma de sus partes. *El mal funcionamiento o ausencia de una parte del sistema* afecta a las demás y, con esto, al sistema completo. Se convierte en una VULNERABILIDAD del sistema, en éste caso vulnerabilidad del sistema de seguridad.

Desafortunadamente los conceptos básicos de lo que es un sistema de seguridad son desconocidos por muchos jefes de seguridad de las organizaciones o por quienes hacen sus funciones y debido a ello no tienen la visión holística que requiere la planificación, implementación, el monitoreo y el mejoramiento continuo del sistema. Muchos tienen una mirada reduccionista, y creen que el sistema de seguridad son solo los elementos tecnológicos, o solo la empresa de seguridad que contrataron, o solo alguna de las partes del sistema, y cuándo se presentan siniestros, son reacios a asumir su responsabilidad por la falta de contemplar e incluir todos los elementos que requiere el sistema. Su responsabilidad por las vulnerabilidades del sistema de seguridad.

Por ejemplo, algo tan simple como desarrollar un manual de seguridad para contratistas, puede solucionar muchos problemas de seguridad. Volviendo a la analogía de la silla, la falta de un manual de seguridad para contratistas puede ser la pata que le falta a una organización para hacer robusto su sistema de seguridad. La ausencia de ese manual puede ser la vulnerabilidad de su sistema de seguridad. ¿Y por qué no se tiene ese manual? La respuesta común es que ese jefe de seguridad ni siquiera ha descubierto la necesidad de desarrollarlo o considera que elaborarlo no es parte de sus responsabilidades: "es responsabilidad del área de contratación".

Por supuesto que la ignorancia de lo que es un sistema de seguridad y las implicaciones de la falta de una mirada sistémica de la seguridad también aplica a otros directivos de la organización, no sólo al jefe de seguridad. ¿Por qué sucede con tanta frecuencia esa miopía reduccionista de los directivos con relación a la seguridad? Creo que en su formación académica (pre y posgrado) nunca se aborda el tema. Y esto a pesar de que desde 1918, Henry Fayol - Teoría Clásica de la Administración – destacó que una de las seis funciones básicas de una organización para lograr la eficiencia es "la seguridad", siendo las otras cinco la administración, las operaciones, las finanzas, la contabilidad, y la comercialización. Esas otras cinco se han desarrollado a pasos gigantescos mientras que la función de la seguridad se relegó a los "servicios generales junto con el aseo, la lavandería, la jardinería etc." y solo la estudiamos los profesionales de la seguridad. Sorprende que muchas organizaciones están certificadas en uno o varios sistemas de gestión, y sin embargo no tienen comprensión de lo que es un sistema de seguridad y las partes que lo componen.

Pero, y que desafortunado, muchos profesionales de la seguridad tampoco comprendemos lo que es un sistema de seguridad. En artículos sobre el tema que además son publicados en revistas de seguridad, los autores sufren esa miopía reduccionista de centrarse solo en hablar de los medios tecnológicos y su evolución, o solo del rol de las personas etiquetadas como "de seguridad", eventualmente de los procedimientos, muy pocos incluyen la normatividad y muy escasos los que ven el sistema en forma holística.

Para los profesionales de la seguridad, asesores, consultores, los que debamos implementar y o evaluar sistemas de seguridad, resulta imperativa la mirada sistémica, siendo lo mínimo tener claridad de qué es un sistema, tipos de sistemas y las leyes que lo gobiernan (no se revisan en este artículo) y qué es un sistema de seguridad, su objetivo y las partes que lo componen.

¿Está en desacuerdo con este artículo? Agradezco sus comentarios a cabondano@outlook.com

PRUEBAS DE CONFIABILIDAD

¿AVANZAS CON LA TECNOLOGÍA O TE QUEDASTE EN EL TIEMPO?

Por: John Sierra

El proceso de selección de personal es el elemento primordial para prevenir el fraude corporativo; un óptimo proceso de selección, implementa políticas para minimizar este riesgo a través del reconocimiento de debilidades, que conducen a incrementar dicho riesgo y de la consecuente identificación de modalidades para su comisión. Por ello, la seguridad empresarial implica un diseño de políticas que conlleven estrategias conducentes a prevenir todo acto corporativamente inviable, moralmente controvertible y jurídicamente sancionable. Esta política, debe garantizar la contratación del aspirante más confiable.

El fraude es un riesgo latente en todas las compañías, prevenir este riesgo debe ser uno de los objetivos primordiales de una organización para alcanzar los propósitos inherentes a su visión y misión. La prevención, se debe dar desde la iniciación de la etapa de selección, donde el defraudador encuentre un obstáculo para llevar a cabo su accionar, restringiendo así el otorgamiento de la oportunidad de poder infiltrarse fácilmente por la ausencia de controles, acordes a la criticidad en las funciones de los cargos dentro de una organización. A menor oportunidad de fraude menor es la posibilidad de su comisión; actividades que suelen ignorarse en la mayoría de empresas.

Una de las medidas utilizadas en la prevención del fraude empresarial es la aplicación de las pruebas de confiabilidad, de las cuales tenemos mucho que aprender. Si bien hay varias tecnologías para realizar las pruebas de confiabilidad, cada una de ellas tiene detractores que descalifican su eficiencia a la hora de elegir el candidato más confiable para la empresa.

Sin embargo hay temas más profundos que se deben tener en cuenta, como las garantías que ofrecen cada una de las tecnologías en el resultado de las pruebas, la idoneidad del examinador que realiza la prueba, los entregables al solicitante de la prueba, el marco legal que se debe cumplir y los derechos que tiene sobre la información quien contrata los servicios de estas pruebas; aspectos que deben quedar muy especificados en el momento de utilizar este servicio, para no tener sorpresas desagradables cuando se requiera contar con una segunda opinión o control de calidad.

Para conocer cuál es la prueba más idónea debemos identificar cual es nuestra necesidad y el costo beneficio en la prevención del fraude empresarial.

Por otra parte, consultar las fuentes de información oficiales y no creer en supuestos infundados que intentan opacar la efectividad de diferentes tecnologías de verificación de la verdad y que al no tener argumentos frente a los mismos, lo tachan de ineficaz, evitando avanzar en las tecnologías que mejoran las herramientas de simplicidad en ahorro de tiempo, facilitando su realización de manera virtual, sin que el examinado se sienta vulnerado en sus derechos personales y por el contrario se sienta más a gusto desde el confort de su espacio.

Es el caso del intento de desprestigiar la efectividad de la tecnología CVSA Análisis Computarizado de Estrés en Voz, con unos supuestos estudios avalados por una institución educativa en los Estados Unidos de América, los cuales fueron desvirtuados en los tribunales de la Florida, cayendo todo el peso de la Ley sobre las difamaciones de la eficacia del CVSA,

terminando en sentencia e indemnización a favor de su fabricante y en contra de la empresa Dektor Corp. y Arthur Herring; indemnización de casi 1 millón de dólares. (*)

Sentencia frente a la cual, el Tribunal del Distrito de los Estados Unidos- Distrito Sur de la Florida se pronunció decretando entre otras cosas, lo siguiente:

Los demandados, sus accionistas, directores, funcionarios, agentes, servidores, empleados, sucesores, cesionarios, afiliados, empresas conjuntas y cualquier otra persona en concierto activo, en contacto con ellos, tienen PROHIBIDO PERMANENTEMENTE:

Enviar o transmitir correos electrónicos o cualquier tipo de texto, que contenga comentarios o declaraciones falsas o despectivas sobre la tecnología CVSA.

Difundir cualquier declaración negativa con relación a la supuesta imprecisión/confiabilidad de CVSA, entre las que se destacan:

- Sugerir que el Demandante y/o sus productos son ineficaces y la supuesta superioridad probada de otras tecnologías sobre la del CVSA.
- Que las agencias de aplicación de la ley que utilizan el CVSA lo hacen atendiendo a intereses particulares.
- Que la efectividad del CVSA equivale a lanzar una moneda al aire.
- Que los procedimientos utilizados en el CVSA (como puntuación numérica, DSR [Respuesta retardada al estrés], llamadas en frío, kinésica, FACT y DBR - Eliminación de barreras de defensa) no tienen sustancia o credibilidad real.
- Fallas de diseño graves en el CVSA que producen patrones defectuosos/resultados incorrectos; por un supuesto estudio de 2007.
- Hacer cualquier declaración oral (ya sea en persona, por teléfono o de otro modo) a cualquier entidad (incluida cualquier agencia de aplicación de la ley o agencia gubernamental) o persona que contenga comentarios o declaraciones falsas o despectivas sobre el CVSA.
- Publicar o republicar cualquier sitio web, blog u otro escrito accesible a través de Internet que contenga comentarios o declaraciones falsas o despectivas sobre el CVSA

  Se le ordena al demandado eliminar de forma inmediata todas las publicaciones en los sitios web que se enumeran en la sentencia; Igualmente, no cooperarán ni ayudarán a ninguna persona a reproducir dicha información.

De esta manera, queda claro que la credibilidad en la tecnología CVSA, Análisis Computarizado de Estrés de Voz, la cual está disponible en Colombia, es confiable, no invasiva, con una alta tasa de precisión, sin vulnerar el respeto por los derechos y la dignidad humana, permitiendo realizar pruebas de manera presencial y virtual sobrepasando las barreras de tiempo y lugar; optimizando así los tiempos de respuesta y los costos de operación para el cliente final.

¿Y tú, le das espacio a las difamaciones infundadas por otras tecnologías que quieren monopolizar el mercado, sesgando el avance tecnológico o aplicas pruebas de confiabilidad eficientes para prevenir el fraude empresarial optimizando costos de operación?

(*) TRIBUNAL DE DISTRITO DE LOS ESTADOS UNIDOS – DISTRITO SUR DE LA FLORIDA
Caso No. 18-80994-Civ-Brannon
Demandante: SERVICIOS FEDERALES NITV, LLC
Demandados: CORPORACIÓN DEKTOR y ARTURO HERRING-

John Sierra

Director de la empresa Grupo Consultor 360 SAS. Administrador de empresas con especialización en administración de la seguridad, cuenta con diplomados en Gestión Integral de riesgos, Gerencia de seguridad, Gerencia de recursos humanos, es Piloto certificado RPA, Examinador certificado CVSA, Un apasionado por la gestión del riesgo, Comprometido en la creación de estrategias para la prevención del fraude empresarial.

https://www.linkedin.com/in/john-fredy-sierra-blanco-48b62756/

ASIS EUROPA 2024

EN LA EXPERIENCIA DE UN AFILIADO

Por: Martín Eduardo Tarazona Santos

Tuve la oportunidad de participar del ASIS EUROPA 2024, un evento muy enfocado en GeoRisks y Resiliencia, con ponentes de la más alta experiencia y calidad que compartieron información importante y de tendencia para minimizar los riesgos tratados.

Considero muy relevante la intervención del Señor General (Ret) Tom Middendrdorp no solo como activista si no también como consejero de la oficina de cambio climático y Ejército Holandés permitiendo entender la circunstancia y probables riesgos globales en el corto y mediano plazo.

En cuanto a insights de interés, dos tipos de temporadas que afectarán el mundo como grandes sequías e inundaciones por largas temporadas de lluvias. Este fenómeno influenciará las migraciones masivas y traerá consigo una cadena de acciones criminales.

Por otro lado, la sensación de temor geopolítico a raíz de diferentes conflictos en el mundo prevé un conflicto bélico de proporciones globales terminando uno de los periodos de paz más duraderos en la historia contemporánea reciente luego de la segunda guerra mundial.

La autopista de la Internet y la ciberdelincuencia enumera la atención sobre probables problemas de mayor crecimiento para las corporaciones teniendo la obligación de buscar medios y condiciones para proteger su información valiosa para un plan de continuidad del negocio y esto hace pensar un poco el lugar geográfico donde se encuentran la gran mayoría de servidores de almacenamiento de la información y que por acción del cambio climático podrían ser afectados por causa inminente que se avecina.

Sinceramente queda mucha reflexión sobre lo que dejamos de pensar y sí lo que debemos enfrentar como compañía de soluciones de seguridad corporativa.

El inmenso networking y workshop durante el evento permite alimentarse de experiencia de escenarios similares bajo otra perspectiva mejorando el entendimiento y las mejores prácticas para implementar en nuestra realidad.

Asimismo, al tener la oportunidad de conversar y escuchar las ponencias de la NEWGEN en ASIS pude ver la capacidad, conocimiento y ganas que tienen todos estos jóvenes de aportar a este mundo de la seguridad. Todos preparándose para unas carreras muy exitosas y buscando poder aportar de alguna forma a todos aquellos que los rodean.

Finalmente, ASIS busca que exista una equidad de género en todos los cargos existentes en la seguridad, logra esto a través de distintos conversatorios que buscan visibilizar la desigualdad laboral que existe actualmente, busca que se conozcan las cifras actuales y las metas a futuro para todas aquellas mujeres que quieren crecer en este mundo de la seguridad.

Gracias a los organizadores, a todos los expositores y gracias ASÍS Europa.

Martín Eduardo Tarazona Santos

Oficial (Ret) del Ejército de Colombia.
Magister en Seguridad y Defensa de la Escuela Superior de Guerra de Colombia.
Consultor y Director de operaciones en compañías de Crisis & Seguridad.
Fundador y Country Manager de 3+ Security Colombia, nombrada como uno de los TOP principales proveedores de soluciones en Gestión de Riesgo en Latinoamérica por la revista CIO Review.
ASIS Chapter Officer

https://www.linkedin.com/in/martin-tarazona-3954121b7/

ASIS INTERNATIONAL
Advancing Security Worldwide®
Panamá Chapter 235

ASIS INTERNATIONAL® Women in Security Community

V FORO
WOMEN IN SECURITY
LATAM & CARIBBEAN 2024

"PROTEGIENDO EL PRESENTE, FACILITANDO EL FUTURO"

1 Y 2 DE AGOSTO 2024 | SHERATON GRAND PANAMÁ

EJES TEMÁTICOS

- Conflictos Geopolíticos y Sociales
- Liderazgo y Resiliencia
- Innovación y Ciberseguridad
- Sostenibilidad y Seguridad Humana

REGISTRO ABIERTO WWW.WISLATAM.ORG

DiDi · BE SAFE INTERNACIONAL · Control Risks · AFIMAC · DOMINICAN WATCHMAN · COLPRYST · PINKERTON® · PROTEGIDA · GIF FRAUD & SECURITY · ORGANIZACIÓN G.D.C. GESTIÓN, DESARROLLO Y CRECIMIENTO EMPRESARIAL · GRIFFON

MODELOS DE COMPETENCIAS EN SEGURIDAD CORPORATIVA

Por: Jakson Phillips, CPP®, PCI®, PSP®, SRMP

Por allá, en el año 2008, cuando hacia la transición del mundo militar al corporativo, eran tantas las incertidumbres que ondeaban en mi ser, y es que no solo era en mi mente, también en mi comportamiento que a vivas luces se ponían de manifiesto en cada acción. Como por ejemplo, una de ellas era, ¿estaré preparado, como militar de 11 años de experiencia, para encajar y estar a la altura del compromiso que apenas enfrentaba? Decenas de respuestas, pero eso sí, cada una cargada de positivismo, de; ¡yo si puedo,¡ pensaba, si superé la formación militar y estos muy experimentados 11 años, ¿que podría salir mal en la vida civil?, es así como en el argot militar se le conoce al mundo de quienes no portan un uniforme castrense, en el argot militar. ¿Muchos temores? Si, por supuesto, pero siempre con la convicción de querer hacer las cosas de la manera correcta y satisfacer las ansias personales de triunfar…

Me encontré con cosas, términos, documentos, gente, procesos, y muchas otras más, que para un militar normalmente no son comunes. Lo principal fue durante mi proceso de captación y selección, al ver todas los requisitos que exigían para esa posición, lo que me tranquilizaba era mi fe, mis ganas de triunfar, y el haber sido formado militarmente. Al leer la descripción del cargo y los requisitos, me di cuenta que estaban perfilados hacia el ser un profesional militar o proveniente de algún organismo de seguridad del estado, además de tener contactos y relacionamiento con personas instituciones de interés, eso era lo que más prevalecía a la hora de haberme seleccionado para ocupar esa posición en la industria petrolera.

Ya iniciando mis labores seguía encontrando esas cosas desconocidas, y apliqué lo que es ser militar, que aunque no conocemos ciertas situaciones para llevar a cabo el cumplimento de una orden, nos ocupamos de hacer esa evaluación inmediata, tipo operación de inteligencia, y conocer todo lo necesario para ejecutar lo encomendado. Empecé a coincidir y a conocer a diferentes colegas de organizaciones y corporaciones, teniendo en común dos cosas principalmente, ser militar en situación de retiro y gerenciar o estar a cargo de equipos que gestionan la seguridad de personas y activos, eso fue grandioso porque entre otros ventajas, empecé a conocer buenas prácticas, nuevas terminologías, y entendiendo más en detalle cómo funciona la seguridad corporativa.

Una vez, en el año 2009, asistiendo a una capacitación en seguridad, escuché por primera vez que me hablaban de los modelos de competencias, y me llamó poderosamente la atención. Ahondé en su concepto y desde allí entendí lo que significa, y cuanto orden pone esto a nuestras actividades, pero no solo hablando de seguridad, sino también en todas las profesiones y actividades ejecutadas por el ser humano.

Un modelo de competencia es un marco estructurado que describe las habilidades, conocimientos y comportamientos necesarios para desempeñarse de manera eficaz en un determinado rol o campo profesional. Estos modelos suelen identificar las competencias claves que se requieren para tener éxito en una función específica y proporcionan una guía para el desarrollo profesional y la evaluación del desempeño. Los modelos de competencia pueden variar según la industria, el sector y el nivel organizacional, y se utilizan para definir estándares de excelencia y establecer expectativas claras para los profesionales.

Los modelos de competencia se han usado durante años en diferentes campos y sectores. El concepto de modelos de competencia ha sido desarrollado y redefinido por numerosos investigadores, académicos y profesionales a lo largo del tiempo, por lo que es difícil atribuirlo a un solo pionero. Sin embargo, se puede destacar a **David McClelland** como una figura importante en el desarrollo de modelos de competencia. McClelland, un psicólogo estadounidense, fue pionero en la identificación y estudio de las competencias y habilidades en el ámbito laboral. Su trabajo en la década de 1970 sobre la teoría de la motivación y la identificación de competencias clave, como la necesidad de logro, la necesidad de poder y la necesidad de afiliación, influyó en el desarrollo posterior de modelos de competencia en diversos campos.

Ya un par de años después, 2010, empecé a ver como en la corporación donde trabajaba, desarrollaron y aplicaron algo que aunque a veces se confunde con los modelos de competencia, son diferentes totalmente, y hablo de los perfiles de cargo, los cuales estaban detalladamente descritos en un documento, revisado por cada dueño o responsable de proceso, es decir, los gerentes, luego por los responsables del departamento de calidad, y un par de revisiones más, por Recursos Humanos y Gerencia País, hasta tener el documento final que era publicado en el share point de la corporación, reposando el documento físico en los archivos de Recursos Humanos. Pero ¿y qué pasó con estos modelos de competencia en ese entonces? bien, la realidad es que nunca existieron...

Una diferencia entre Modelos de competencias y los perfiles de cargo es, que un perfil de cargo describe las responsabilidades, tareas, requisitos y expectativas asociadas con un puesto específico dentro de una organización. Mientras que un modelo de competencias identifica las habilidades, conocimientos, comportamientos y atributos personales que se consideran importantes para el desempeño exitoso en un campo o rol específico.

En resumen, mientras que un perfil de cargo describe las responsabilidades y requisitos específicos de un puesto de trabajo, un modelo de competencias identifica las habilidades y atributos personales necesarios para tener éxito en cualquier rol dentro de un campo o industria. Los perfiles de cargo se centran en el qué se espera que haga un empleado, mientras que los modelos de competencias se centran en el cómo debe hacerlo.

Para el mundo de la seguridad corporativa, esto es muy importante, al punto de que podríamos decir que es el faro que alumbra el camino a donde tenemos que llegar cuando iniciamos el proceso de captación y selección de esa persona que cubrirá es posición deseada, ser exitosos, tanto para el contratado, como para la corporación que contrata a ese profesional. Hablando en términos de prácticas comerciales, garantizar un retorno a la inversión (ROI).

Dice un gran colega y amigo, a quien considero una de las personas muy preparadas en temas de ASIS International, y otros más, "*en ASIS está todo lo que necesitamos para ejecutar nuestros trabajos*", y me refiero a los estándares, guías, documentos de referencias, contactos, buenas prácticas, entre otros recursos, entonces, ¿por qué no consultar qué nos tiene ASIS respecto a modelos de competencias? Para esto, hago referencia al documento Standard Senior Security Executive 2022, el cual, en su apartado número 6, establece cual debería ser el modelo de competencia de un profesional senior de seguridad.

Las competencias esenciales de los **Senior Security Executives (SSE)** incluyen, pero no se limitan a:

- **Pericia en seguridad**: seguridad física, seguridad del personal, protección de activos de información, investigaciones, prevención de pérdidas, etc.
- **Profundo conocimiento y práctica empresarial**: comprensión sólida de la estrategia empresarial, mercados, métricas financieras, métodos de producción, distribución, etc.
- **Habilidades de liderazgo**: pensamiento estratégico, comunicación efectiva, integridad, responsabilidad, influencia, delegación, capacidad de toma de decisiones, comprensión y motivación de otros; y
- **Inteligencia emocional**: autoconciencia, autorregulación, motivación, empatía y habilidades sociales.

El liderazgo de un programa de seguridad multifacético también requiere conocimientos generales, incluido un historial relevante a nivel senior dentro de una función de riesgo, gobierno o seguridad. Es fundamental comprender, asignar valor y articular los diversos riesgos y amenazas que enfrenta una organización de manera que los líderes empresariales puedan entender y evaluar. En resumen, los especialistas en SSE son ingeniosos, creíbles y alineados con el liderazgo ejecutivo.

Hay competencias adicionales de los SSE, y están enumerados en el modelo de competencia de seguridad empresarial que se muestra en ese estándar SSE de ASIS. El modelo, desarrollado por el Grupo de Educación Apollo y la Universidad de Phoenix y validado en asociación con la Fundación ASIS, fue publicado y respaldado por el Departamento de Trabajo de los Estados Unidos en 2015. El modelo está diseñado para ayudar a los esfuerzos de desarrollo de la fuerza laboral para preparar a los trabajadores de seguridad, desde analistas de inteligencia hasta ejecutivos de seguridad senior. En 2020, el modelo se revisó para incorporar habilidades fundamentales de salud y seguridad en el lugar de trabajo del Programa de Fuerza Laboral del Instituto Nacional de Seguridad y Salud Ocupacional (NIOSH).

De manera tal, que hoy en día no basta tener en nuestras organizaciones o corporaciones, un perfil de cargo y un modelo de competencia, que sólo establezca “haber sido militar o policía, con contactos en instituciones, entre otros”...

Mi invitación a todos los profesionales, tanto de seguridad, así como a todos aquellos que están involucrados en los procesos de Recursos Humanos, captación, selección y/o contratación del responsable de seguridad corporativa, para que busquen adoptar las buenas prácticas, seguir y aplicar estándares ya aprobados y reconocidos en el mundo de la seguridad corporativa. Se nos haría menos complejo y con la garantía de estar haciendo las cosas con marcos de referencias, legales, aceptados y ya con resultados científicamente comprobados.

En resumen, los modelos de competencias son herramientas valiosas para la gestión de recursos humanos, ya que facilitan la toma de decisiones relacionadas con la selección, desarrollo y gestión del talento en una organización. Además son herramientas útiles que nos proporcionan y ayudan a tener claridad en las expectativas, selección y reclutamiento, desarrollo profesional, evaluación de desempeño, promoción y ascensos, cultura organizacional, entre otros beneficios.

Jakson Phillips, CPP®, PCI®, PSP®, SRMP

+13216559679 | jaksonphillips@gmail.com | contact@elevenpdsecurity.com

Profesional certificado en Gestión de Seguridad y Gestión de Riesgos Empresariales de Seguridad, Seguridad Física, Seguridad de la Información, Continuidad del Negocio y Gestión de Crisis, Investigaciones, Seguridad de la Información, con amplia experiencia en la industria de la Hospitalidad, Petróleo y Gas, Seguridad Pública, Comercio Minorista, Cadena de Suministro, y en contextos humanitarios en medio de conflictos armados y ambientes calurosos, entre otros

https://www.linkedin.com/in/jakson-phillips-cpp%C2%AE-pci%C2%AE-psp%C2%AE-88245b55/

DOXXING:
UN TIPO DE ATAQUE QUE SIN SER ILEGAL (AÚN) PUEDE ARRUINAR SU VIDA

Por: Yelena Castañeda Useche

Muchas veces creemos que nuestra vida es menos interesante que la de una celebridad y por esto compartimos información personal, participamos de retos tipo "cuestionario de cosas que no sabes de mi" y sin darnos cuenta nos hacemos vulnerables ante las personas - no siempre hackers - que quieren hacernos daño.

Y si, tal vez no tiene nada qué ocultar, pero sus datos son tan propios e importantes que pueden ser utilizados con demasiada facilidad para dañar su reputación. Por ejemplo, ¿ha notado que cuando sucede un choque, una imprudencia al volante o un enfrentamiento entre conductores, con solo la placa del auto hay personas que encuentran y publican el nombre completo, la cédula, el lugar de trabajo y hasta el Google Maps de su residencia?

Pues esto es lo que se llama doxxing. El nombre viene como abreviación de la palabra docs o documentos en inglés a *dox* y consiste en la **filtración de información identificadora** de una persona (como su nombre real, dirección, lugar de trabajo o datos financieros) la cual se **divulga sin permiso de la víctima**. Su objetivo es dañar la reputación online de la persona afectada, causándole daños emocionales, psicológicos y en ocasiones también atenta contra su seguridad física.

El Doxxing consiste en la filtración de información identificadora de una persona (como su nombre real, dirección, lugar de trabajo o datos financieros) la cual se divulga sin permiso de la víctima.

En la actualidad todos podemos ser víctimas de esta práctica, pues gracias al internet estamos a la vez más conectados pero también más divididos en nuestras opiniones y esto da lugar a que entre facciones contrarias realicen este tipo de ataques, llevando incluso a víctimas de este ataque a decisiones contra su propia vida cuando las amenazas trascienden la frontera de lo digital y pasan a lo presencial.

El Doxxing tiene como origen la búsqueda de la identidad de los llamados "hackers" de los 90s y 2000s, cuando su anonimato era clave para sus actividades, y el doxxing venía a ser ese "quitar la máscara del villano". Pero actualmente con la facilidad de la tecnología para encontrar datos, documentos y fotografías, aunado al bajo perfil de seguridad que maneja el común de los usuarios en redes sociales y plataformas, está haciendo que esta práctica sea más común de lo que era hace algunos años, incluso, según un estudio realizado en UK, más del 19% de las personas han participado o han sido víctimas de uno de estos ataques.

Imagine que usted fue a un restaurante, no le gustó el servicio y calificó el servicio como deficiente en la aplicación Google Negocios. El dueño del restaurante, ofendido, responde al comentario con la dirección de su casa y otros datos privados suyos para presionarlo a que retire la mala reseña de la plataforma. Esta es otra forma como se está aplicando esta práctica del doxxing, para generar presión social sobre las personas.

Lo más grave es que en la mayoría de países esta práctica no está reglamentada ni prohibida, ni es considerada como delito, porque las mismas plataformas permiten la difusión de este tipo de contenidos y de datos personales de sus usuarios. No es algo que se prohiba por defecto en las plataformas de redes sociales, sino que a partir de denuncias de los usuarios se toman las decisiones de eliminar estos datos personales.

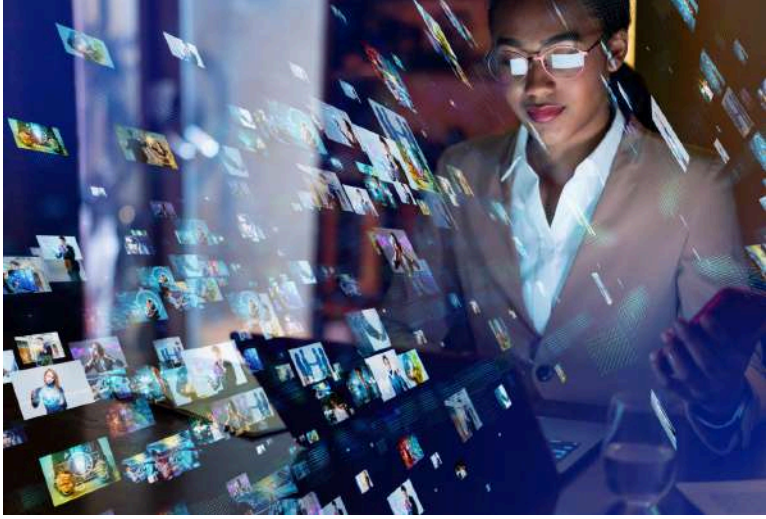
¿Entonces, qué hacer ante esta amenaza? Empecemos por afrontar que no hay una solución definitiva, pues actualmente todos tenemos un rastro digital e incluso de forma pasiva ya existe información suficiente.

Acciones que pueden ayudarle a prevenir un ataque de doxxing:

Tener cuidado con lo que publica en redes sociales.
Revise que las fotos que publica no tengan información que pueda identificar donde vive, la placa de su casa o de su auto, el uniforme de colegio de sus hijos, la empresa donde trabaja y otros datos que pueden parecer inocuos pero tienen alto potencial para hacerle daño.

Utilice contraseñas seguras y active la autenticación de dos pasos.
Cree contraseñas con al menos mayúsculas, minúsculas, números y símbolos, evite usar la misma contraseña para varias cuentas, cámbielas con regularidad y active la autenticación en dos pasos para dificultar el acceso a sus dispositivos.

Maneje distintas cuentas de correo electrónico según el propósito.
Establezca una cuenta de correo profesional diferente a su cuenta personal. En la profesional lleve la comunicación de su negocio o su trabajo y en la personal los correos con amigos, familiares y contactos cercanos. Evite usar nombres, apellidos y fechas en la identificación de su correo electrónico.



Revise la configuración de privacidad en las redes sociales.
Establezca quién puede ver, comentar o descargar sus publicaciones, evalúe si la información que comparte es demasiada.

Proteja su dirección IP con una VPN.
Una VPN toma el tráfico de Internet del usuario, lo cifra y lo envía a través de uno de los servidores del servicio antes de dirigirse a la red pública de Internet, lo que le permite navegar de forma anónima.

Mantenga actualizado su antivirus.
Cuando tiene un buen software antivirus y de detección de malware y lo actualiza permanentemente puede evitar brechas en la seguridad que lo exponen a ataques de este tipo.

Elimine los perfiles obsoletos, que ha dejado de usar, y borre la información que previamente había compartido allí.

Revise los permisos que entrega a las aplicaciones.
La manera más sencilla en la que pueden acceder a la información de su dispositivo, con su propia aprobación, es a través de los permisos de las apps, así que al descargar una nueva aplicación siempre cuestiónese si realmente esa aplicación necesita esos datos que le pide para funcionar.

Deje de participar de retos y cuestionarios en línea.
Que parecen inofensivos pero sin darse cuenta reciben información que puede ser usada incluso como preguntas de seguridad para descubrir sus contraseñas.

Evite involucrarse en peleas y conflictos en redes sociales y foros.
Sea cuidadoso con sus expresiones en foros, comentarios o redes sociales como X o Threads y evite enredarse en polémicas que pueden escalar y dar razones a otros para ser atacado.

Una práctica para comprobar el nivel propio de vulnerabilidad al doxxing que propone Kaspersky es revisar la información que encuentra sobre sí mismo:

- ☐ Busque su nombre en Google y en Webmii.
- ☐ Realice una búsqueda de imagen inversa.
- ☐ Audite sus perfiles de redes sociales, incluida la configuración de privacidad.
- ☐ Compruebe si su cuenta de correo ha sido parte de una filtración de datos
- ☐ Revise la hoja de vida que tiene publicada en Linkedin y en otras plataformas, ¿tiene en ella la información de su domicilio, correo electrónico personal y número de celular?
- ☐ Configure las alertas de Google para su nombre completo, teléfono, dirección y otros datos de importancia. Si estos datos aparecen en línea de forma repentina, puede ser un ataque de doxxing

Después de esto, ¿en qué nivel está su vulnerabilidad al doxxing?

Yelena Castañeda Useche

Asesora & Consultora de Redes Sociales, Marketing y Estrategia Digital.
Fundadora y CEO de la Agencia de Marketing Digital Triclick.co

Administradora de Empresas egresada de la Universidad de San Buenaventura, cuenta con más de 20 años de experiencia en empresas de Oil&Gas y Multinacionales. Ha laborado en empresas como: Omnitempus Ltda, Compass Group, Montinpetrol y Quimpac de Colombia S.A.

https://www.linkedin.com/in/yelenacastanedau/

Síganos y comparta
con sus contactos las
publicaciones de
ASIS COLOMBIA,

+57 310 477 0280

secretario@asiscolombia.org.co

www.asiscolombia.org.co

asis-colombia

asiscolombia

¡Unidos somos más fuertes!