NEWS LETTER

Perú Edición **01/2023**

ASIS INTERNATIONAL® | Lima, Peru Chapter

Editorial

ASIS PERÚ inicia sus actividades en el año 2023, con mucho entusiasmo y pero también con mucha responsabilidad.

Nuestro capítulo asume el reto de trabajar para que sus miembros puedan tener un soporte a través de las actividades consideradas en el plan de trabajo 2023, alineado al enfoque de ASIS International realizando actividades con el fin de proponer acciones de valor a sus miembros.

En esta edición se incluyen iartículos de interé y actividades realizadas por nuestro capítulo. Asimismo, información sobre eventos de la región.

Bienvenidos a nuestro renovado Neswletter ASIS PERÚ

ASIS International

SOMOS UNA COMUNIDAD GLOBAL Y DIVERSA

Fundada en 1955, ASISInternational es una comunidad global de profesionales de la seguridad, cada uno de los cuales tiene un papel en la proteccion de los activos: personas, propiedades y/o informacion. Nuestros miembros respresentan practicamente todas las industrias en los sectores publicos y privado y organizaciones de todos los tamaños.

Desde los gerentes de nivel de entrada hasta los CSOs y CEOs, desde los veteranos de seguridad hasta los consultores y aquellos en transicion de las fuerzas de la ley o el ejercito, la comunidad ASIS es global y diversa

"Juntos Somos Más Fuertes"

Beneficios ASIS Capítulo, Lima - Perú

Formar parte de ASIS Perú significa tener adicionalmente los siguientes beneficios:

- Acceso preferencial Reuniones Mensuales, donde se realizarán
- conferencias y/o paneles con expertos y líderes en la materia a tratar.
- Precios especiales y descuentos en cursos y eventos realizados o avalados por la Asociación.
- Participar en diferentes foros y eventos para interactuar y mantener contacto permanente con otros colegas del medio, de manera que puedan compartir experiencias y mejores prácticas.
- Asesoría para cumplir los procesos de certificación y recertificación CPP, PSP y PCI.
- Apoyo y seguimiento en los trámites necesarios ante ASIS Internacional para su certificación y recertificación.
- Participación en Comités de trabajo con temas especializados.
- Acceso a beneficios y/o descuentos para los miembros de ASIS Capítulo 222, Lima - Perú por medio de Alianzas e intercambios con otras organizaciones.

PALABRAS DEL PRESIDENTE

Maurice Frayssinet

Permítanme agradecer a todos los miembros por haberme elegido como Presidente del capítulo ASIS Lima – Péru para el periodo 2023.

Es un honor que recibo con mucha responsabilidad. Me acompaña en la directiva un gran equipo profesional, comprometido, ético y responsable que junto con cada uno de los miembros, trabajaremos por el beneficio de nuestro capítulo y de ASIS Internacional.

En ASIS PERÚ somos miembros que agrupamos prácticamente todas las industrias en los sectores público y privado, y organizaciones de todos los tamaños en el sector de la seguridad y en ese sentido tenemos el compromiso como directiva 2023 de continuar promoviendo servicios de valor agregado a nuestros miembros, impulsando la investigación académica, el mejoramiento continuo de la seguridad y el incremento de los profesionales certificados.

Trabajaremos juntos para fomentar e impulsar un camino hacia un futuro mejor para nuestro capítulo soportado en la participación activa de sus miembros y sus respectivas comunidades.

"Juntos somos más fuertes"

COMUNIDAD WOMEN IN SECURITY

Propuesta plan de seguridad ciudadana, basado en una metodología de oferta y demanda

Gabriela Zuñiga

WIS Liaison, Comunidad Women In Securitty, ASIS PERÚ. Profesional en Derecho y Ciencias Políticas por la Universidad San Martín de Porres. Cuenta con amplia experiencia en Seguridad Ciudadana y Fiscalización (Distritos de San Isidro, Miraflores, La Victoria y Ventanilla). Con especialización en Seguridad Ciudadana (Israel) y Seguridad Bancaria (USA).Experiencia en Seguridad Bancaria habiendo tenido la responsabildad de la Seguridad en el Banco de la Nación del Perú.

DETERMINACIÓN DE LA DEMANDA

Para la aplicación de esta metodología, es necesario entender el concepto de "**Vigilancia Ciudadana**", el mismo que está referido a "todas aquellas funciones preventivas, disuasivas y de control que desarrollan los recursos dependientes de la Gerencia de Seguridad Ciudadana (o la que haga sus veces) de los diversos distritos de Lima Metropolitana y el Callao, destinadas a satisfacer las demandas de seguridad de las personas residentes y población flotante, que garanticen la convivencia pacífica y el desarrollo normal de sus actividades.
Esta demanda contempla aspectos de fiscalización, tránsito, eventos extraordinarios, de defensa civil, y otras acciones que sean necesarias para llevar tranquilidad, paz, calma y calidad de vida a las personas que se encuentren dentro de la jurisdicción de sus respectivos distritos.

DETERMINACIÓN DE LA OFERTA

Se debe entender por oferta a todos aquellos **recursos disponibles** para el funcionamiento del Sistema de Vigilancia, ello implica el recurso humano, los vehículos, motos, bicicletas, los módulos de vigilancia, cámaras de vigilancia, entre otros.

DETERMINACIÓN DEL ÍNDICE DE COBERTURA DE SEGURIDAD CIUDADANA

Para la aplicación de esta metodología, es necesario como primer paso obtener **el índice de Cobertura de Seguridad Ciudadana**, que está determinado por el cociente entre la oferta y la demanda.

Para lo anterior, se requiere que todos los factores de la demanda y todos los recursos de la oferta, sean llevados a una unidad de medida convencional (UMC).

Para que los recursos de seguridad ciudadana realmente puedan ser suficientes para alcanzar el equilibrio o nivel crítico de vigilancia, de tal forma de satisfacer las demandas en seguridad de la ciudadanía, deben alcanzar un valor 1, si este valor es menor, habrá déficit de recursos y, por el contrario, si el valor es mayor a 1, habrá superávit de recursos.
Esto nos permitirá emplear eficientemente el presupuesto asignado en la adquisición e implementación de los recursos de seguridad ciudadana necesarios.

COMUNIDAD WOMEN IN SECURITY

Propuesta plan de seguridad ciudadana, basado en una metodología de oferta y demanda

ESTRATEGIAS A TENER EN CUENTA PARA SU IMPLEMENTACION

1. Realizar un diagnóstico situacional del distrito en función de los factores de victimización, fiscalización y tránsito.
2. Reorganizar el mapa de seguridad ciudadana del distrito por sectores, de acuerdo al diagnóstico realizado.
3. La sectorización debe guardar relación con el de las Comisarias del distrito a fin de garantizar la interoperabilidad.
4. Realizar cambios relevantes en la gestión y procesos en la organización; para ello, se propone cambios en las funciones de los serenos, con una visión moderna de la seguridad y con un alto grado de gestión de los recursos que se poseen.

Por lo general se observa que cada uno de los serenos tienen funciones aisladas. En la práctica el de tránsito no asume responsabilidades de fiscalización ni seguridad y en forma viceversa.

En consecuencia, al tener un concepto transversal de la seguridad ciudadana se propone UNIFICAR las funciones de los serenos de Serenazgo, Tránsito, Fiscalización para tener una mayor cobertura del servicio.

Bajo esta visión y en el marco de la prevención, esta metodología debe articularse con los sectores de educación y salud. En el primer caso, 9 de cada 10 delincuentes no ha cuentan con estudios primarios ni secundarios completos, solo cuentan con oficios y mayormente provienen de familias disfuncionales y de alta violencia familiar.

De otro lado, debemos entender que la delincuencia es un problema de salud pública que atenta no sólo a la salud física sino también a la mental, ya que afecta el bienestar y calidad de vida de las personas. Las faltas y delitos no atentan sólo a las víctimas, sino también a los victimarios.

ASIS INTERNATIONAL® Women In Security Community

Fuente: https://www.asis.org.pe/blog/item/232-propuesta-plan-de-seguridad-ciudadana-basado-en-una-metodologia-de-oferta-y-demanda

COMUNIDAD NEXTGEN

Protección de Activos Críticos Nacionales

Michael Regalado Varea CPP®, PSP®, AMBCI

Superintendent of Security (Hudbay Perú)
Gerente de Operaciones y Evaluación de Riesgos (LAMSEC Risk Management)
Steering Committee Member – Petrochemical, Chemical, and Extractive Industry Security

Ejecutivo sénior con formación Naval Militar. Máster en Risk Management, Supply Chain Management y MBA en Administración y Dirección de Empresas, Licenciado en Ingeniería Industrial y en Ciencias Marítimo-Navales.

Con 15 años de experiencia en Security, Operaciones y Recursos Humanos. Capacidades de excelencia operacional integrada, perspectiva con orientación global, liderazgo, planificación estratégica y conocimiento técnico

¿Qué son Activos Críticos Nacionales?

Los Activos Críticos Nacionales (ACN) son el conjunto de las actividades esenciales de un país, aquellas de las que se depende para garantizar un correcto funcionamiento de una nación en lo que respecta a servicios básicos. Estos elementos esenciales son complejos y están interconectados. Todos ellos clasificados en sectores estratégicos y críticos, tales como los siguientes (entre otros):

Industria Energética	Transporte	Salud	Centros de Investigación
Industria Nuclear	Gestión del agua y desagüé	Industria Química	Entes Públicos
TIC	Alimentación	Telecomunicaciones	Educación

Protección de los Activos Críticos Nacionales

La protección efectiva de los ACN demanda nuevos retos para la seguridad privada. Todas y cada uno de los ACN, requieren una gestión de riesgos con un enfoque de seguridad integral la cual permita identificar adecuadamente los activos, amenazas, vulnerabilidades y riesgos asociados, pudiendo así diseñar un Programa de Seguridad Patrimonial acorde a la necesidad real, evitando contar con sistemas sobredimensionados o inferiores a lo idóneo; soportado por la definición de una política de seguridad acorde. Estableciendo medidas que mitiguen estos riesgos y permitan contar con soluciones tecnológicamente avanzadas para contrarrestar cualquier amenaza, siendo de extrema importancia.

Debemos pensar de manera global, aunque actuemos de local. Es primordial que se realice una conjunción armonizada entre el sector de seguridad privada, pública, empresas de servicios, instaladoras, integradoras y proveedores de seguridad; estando preparados para participar activamente en este Programa.

COMUNIDAD NEXTGEN

Protección de Activos Críticos Nacionales

La seguridad de los ACN (física y cibernética) es la protección de las estructuras y sistemas destinados a proteger las infraestructuras críticas. La gran mayoría de ACN están interconectadas con la tecnología de la información, volviéndose muy vulnerables al sabotaje, al terrorismo e incluso a la contaminación si no se protegen adecuadamente.
Es una responsabilidad conjunta de las administraciones y de los operadores responsables del funcionamiento de los servicios esenciales. Si bien este planteamiento puede considerarse común para cualquier parte del mundo, la aplicación práctica de las soluciones de seguridad para ACN tienen que ser evaluadas de manera particular de acuerdo con la coyuntura de cada país, en adición de la rápida evolución de las amenazas y los riesgos a los que están sometidas.
Lejos de convertirse en un freno o enemigo para el negocio del operador crítico, la seguridad se convertirá en un elemento generador de valor, garantizando la continuidad de los servicios y suministros de las infraestructuras críticas.

Riesgos para la seguridad de los Activos Críticos Nacionales (ACN)

Existen diversos tipos de catástrofes que pueden amenazar los ACN de un país, desde atentados hasta las catástrofes causadas por la naturaleza. Estos son algunos de los principales riesgos:

- Ataques terroristas (Estos activos son objetivos claves)
- Espionaje (Virtual o físico)
- Crimen organizado (Bandas criminales nacionales e internacionales)
- Vulnerabilidad del espacio aéreo y/o marítimo (Tanto contra los vehículos como los sistemas que los controlan)
- Armas de destrucción masiva (Poder altamente destructivo e inesperado)
- Catástrofes naturales (Eventos climáticos y pandemias)
- Vulnerabilidad del ciberespacio (Cibercrimen, ciber espionaje y ciberguerra)

Las naciones dependen del funcionamiento continuo y esencial de nuestras infraestructuras críticas. Los daños accidentales o deliberados pueden:

- Amenazar la seguridad nacional
- Causar víctimas masivas
- Debilitar la economía considerablemente
- Dañar la moral y la confianza del público

COMUNIDAD NEXTGEN

Protección de Activos Críticos Nacionales

Vulnerabilidad de los ACN

- Los componentes de las infraestructuras críticas con décadas de antigüedad incrementan exponencialmente los riesgos de seguridad al proporcionar acceso a innumerables vulnerabilidades, bien conocidas en un amplio espectro de aplicaciones utilizadas en las organizaciones actuales. La protección y la seguridad de las infraestructuras críticas son en parte propiedad del sector privado y están gestionadas por él. Es esencial garantizar que las prioridades de seguridad física y cibernética no se pierdan en la maximización de los beneficios. Muchos proveedores de seguridad también subcontratan funciones fuera de sus competencias básicas, lo que da lugar a vulnerabilidades adicionales. Estas podrían incluir la pérdida de control y visibilidad.

Consideraciones para la gestión de riesgos de ACN – PERÚ

- Se cuenta con un reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales.
- Se cuenta con una norma técnica para la Protección de los Activos Críticos Nacionales.
- Estos documentos establecen los lineamientos y criterios para poder gestionar los riesgos de ACN. Así mismo determina las capacidades y responsable por sector.
- Detallan el alcance y funciones de las Fuerzas Armadas y la Policía Nacional de Perú
- Establece la elaboración e implementación, por parte de los operadores de los ACN, del Plan Sectorial de Seguridad para la Protección de los Activos Críticos Nacionales.

Marco Normativo

- Decreto Supremo que aprueba el Reglamento para la Identificación, Evaluación y Gestión de Riesgos de los Activos Críticos Nacionales (ACN). DECRETO SUPREMO (N° 106-2017-PCM)
- Norma Técnica para la Protección de los Activos Críticos Nacionales – ACN. Resolución N.° 011-2022-DINI-01

Fuente: https://www.asis.org.pe/blog/item/231-proteccion-de-activos-criticos-nacionales

ARTÍCULO DE COLABORACIÓN

El valor de las certificaciones de ASIS International

Jakson Phillips CPP, PSP, PCI

Abogado, con estudios de post grado en Derecho Penal y Criminología.
CPP ®, PCI® y PSP® por ASIS International, Triple Corona y Profesional Certificado en Gestión de Riesgos de Seguridad (SRMP) - Nacional por International NGO Safety and Security Association (INSA).
Militar retirado de la Guardia Nacional de Venezuela, con 11 años de servicio.
11 años de coordinación y gerencia de las actividades de seguridad en Petrex, S.A. a company of SAIPEM, una corporación italiana de petroleo y gas, con operaciones en Venezuela, y otros paises de Sur America.
Oficial de Seguridad de País Heartland Alliance International _ ONG Humanitaria de U.S.A. en Colombia.
Consultor de Seguridad para una Federación Humanitaria Inglesa, International Planned Parenthood Federation (IPPF) para las Americas y el Caribe.
Miembro de la actual Junta Directiva del Capitulo Caracas de ASIS International NextGen Liasson.
Facilitador del programa de formación CSO de la Organización GDC, para la preparación de profesionales que pretenden certificarse con ASIS International

Cuando inicié mi labor en seguridad corporativa, apenas dejando colgado mis uniformes militares en el closet de mi casa, muchos sentimientos encontrados y cientos de pensamientos pasaban por mi mente, tanto del pasado, como del presente y por su puesto del futuro.

Los que más recuerdo eran:

“¿Estaré tomando la mejor decisión?, ¿Me irá a ir bien acá?”

Y otra, una afirmación, la cual me hacía continuar el emprendimiento en el camino de la seguridad corporativa era:

“Tú eres militar y has trabajado en la seguridad de instalaciones petroleras, así que, si vas a poder, si lo lograrás”.

Por supuesto, las mayores dosis de energía y positivismo me las suministraba el amor por y de mi familia. El querer verlos bien, sin necesidades y con la satisfacción de poder estar y comer bien, y poder tener salud, distracciones, viajes, estudios, y por supuesto, libertad y felicidad.

Hoy, a casi, quince años de haber dado ese paso e iniciar la transición de lo militar al mundo de la seguridad corporativa, entiendo miles de cosas, y las respuestas a casi todos esos cientos de pensamientos han ido llegando a mi vida.
Pasado ya casi una década y media, conozco varios estándares en seguridad, y decidí Certificarme con ASIS International. Esto me ha cambiado profesional y personalmente, sigo aprendiendo y cada día me doy cuenta de que el estudio, el aprendizaje, nos acerca más al logro de los objetivos que tenemos como profesionales de la seguridad.
Colega, eres tú quien debe elegir que certificación o que estudio realizar, yo elegí el de ASIS International, y continúo aprendiendo de otros estándares, de otras organizaciones y de varios colegas con quienes constantemente compartimos mejores prácticas y experiencias.

Si te garantizo que te facilitará el entendimiento de los procesos en gestión de seguridad, también te posicionará en un mejor lugar a la hora de participar en procesos de captación y selección justos, sin sesgos, sin amiguismos y donde los seleccionadores valoren la meritocracia, respeten las políticas internas y la legislación local vigente. Finalmente, si un seleccionador (a) conoce el valor de una Certificación Profesional de Seguridad y sobre todo de ASIS International, entonces, es allí donde te dará el valor que realmente tiene toda persona certificada.

Fuente: https://www.asis.org.pe/blog/item/229-el-valor-de-las-certificaciones-de-asis-international

ARTÍCULO DE COLABORACIÓN

AVATAR 2. Reflexiones y recomendaciones para los profesionales de seguridad y control

Jeimy Cano, Ph.D, CFE

- IT Business scientist
- IT Security and Computer Forensic Expert
- Information security governance consultant
- Corporate Education advisor
- Systemic Thinker

Specialties: Computer and digital forensic, information security management, IT Governance, Systemic Thinking, Data privacy, Corporate compliance, Cyber security, Corporate education

Dicen los militares que en los conflictos todo es distracción y engaño. Recientemente luego de haber visto la última producción de James Cameron ("AVATAR. El camino del agua") se advierten algunas estrategias y lecciones que los ejecutivos de seguridad/ciberseguridad deben recordar con el fin de tratar de mantenerse un paso delante de los retos de sus adversarios.
Sin pretender hacer un "spoiler" de la cinta cinematográfica, se presentan a continuación algunas reflexiones tomadas de diferentes momentos de esta película, como elementos claves a tener en cuenta por los profesionales de seguridad/ciberseguridad para avanzar en la comprensión del adversario y sus estrategias.

1. El adversario tiene motivación y una misión, por lo tanto persistirá de diferentes maneras para lograr su objetivo. Esta primera consideración habla de las amenazas que son persistentes (avanzadas o no avanzadas) que se generan por cuenta de una misión, que leído en lenguaje militar se trata de la razón de ser de una operación (que lleva en sí misma una orden) y por lo tanto todo los implicados saben que deberán utilizar todos los medios disponibles para lograr la encomienda. No hacerlo es desobedecer una orden, y comprometer la esencia misma del orgullo de los participantes, que termina con deshonra y afectando la autoestima de los operadores. Estudiar al adversario, sus motivaciones y misiones permite al profesional de seguridad establecer el marco de trabajo y operación que se requiere para enfrentar al atacante y reconocer sus modos de acción para movilizarse, y así pactar con el incierto que se genera, sus estrategia de disuasión, defensa, contención y respuesta requeridas, más allá de una posición de víctima que sólo se prepara para atender un incidentes y dar cuenta de su nivel de aseguramiento del proceso de gestión de eventos adversos de seguridad, y mostrar su cumplimiento normaTivo.

2. El adversario usará un tercero para provocarte y que muestres lo que tienes, para tomar sus posiciones. Los atacantes no sólo son pacientes y estudiosos de sus futuras víctimas, terminan perfilando sus estrategias de defensa y respuesta con el fin de cerrar posibles formas de acción frente a eventos que estén más allá de su preparación. Por tanto, las organizaciones que están ajustadas y enmarcadas exclusivamente en sus buenas prácticas terminarán posiblemente "acorraladas" en sus propios procesos, pues el agresor conoce claramente el siguiente movimiento que hará y por tanto, se adelantará y creará una situación aún más retadora que deje sin oxígeno al equipo de atención de incidentes, y con más dudas que certezas a los ejecutivos corporativos y de seguridad de la información. En este sentido, el equipo ejecutivo y táctico de seguridad deberá desarrollar escenarios retadores y exigentes que pongan a prueba la capacidad de respuesta de la organización, como una forma de experimentar en primera persona el mismo incierto que se puede generar por cuenta de un ataque desconocido y crear la zona de volatibilidad, que implica sacar a la organización de la zona cómoda de los estándares, y superar la falsa sensación de seguridad que pueden generar las tecnologías de seguridad y control actualmente instaladas.

3. El adversario conoce y explora su territorio, usa la tecnología disponible y se apoya con terceros para lograrlo. El agresor por lo general, a parte de la motivación que ya trae, cuenta con los recursos necesarios para avanzar y contar con la información que requiere para identificar y sondear de la mejor forma el perímetro de defensa y establecer los tiempos de respuesta de la organización con el fin de conocer el espacio de tiempo que tiene para actuar y no ser detectado. El reto está en tener los suficientes radares e inteligencia avanzada para descifrar y descubrir la estrategia de defensa que se ha planteado en la víctima y

ARTÍCULO DE COLABORACIÓN

AVATAR 2. Reflexiones y recomendaciones para los profesionales de seguridad y control

desde allí establecer la forma de operación que se mimetice con la dinámica de la operación de su objetivo Frente a esta realidad, se plantea un juego de inteligencia y contrainteligencia que lleva a la organización a un nuevo nivel el ejercicio de protección, pues en la medida que pueda deteriorar y comprometer los intentos de recolección de información de su adversario, podrá manejar y ajustar sus estrategia de disuasión, confusión y distracción, para crear tanto incierto como el que el atacante quiere lograr cuando ejecute de forma exitosa su posible ataque. De esta forma la corporación podrá avanzar y posicionar una ventaja estratégica mientras puede observar y contener posibles efectos de las agresiones que tenga preparadas el adversario.

4. El adversario sabe dónde te duele y sabrá cómo hacerte daño, no subestime el valor de tus activos. El agresor sabe y conoce muchas veces mejor que la misma organización, cuáles son los activos más importantes y sensibles que ella tiene. En este sentido, hace la exploración en el entorno de la valoración de dichos activos, sabiendo cuáles son los de mayor facilidad de monetización y cuáles los de mayor valor para otros, con lo cual establece con claridad prioridades y mercados donde estos activos será más apreciados y por lo tanto, mejor recibidos y comprados por terceros de quiénes se desconoce su agenda o motivación. La información es un activo estratégico que tiene muchos usos ilegítimos que terminen afectando los derechos de otros.

5. El adversario no teme equivocarse para lograr su objetivo, sacrifica a sus aliados para asegurar su misión. El agresor puede terminar cegado por su motivación y llevar hasta el extremo sus operaciones aun sabiendo que podrá ser identificado, más no capturado. El atacante no actúa sin plan y sin conocer los riesgos que va a asumir con sus acciones, es un ejercicio de operaciones definidas que muchas veces termina cambiando en medio de la zona de conflicto. En este sentido, el adversario “no tiene reglas” por lo que puede quebrar las alianzas y comprometer a sus propios aliados para lograr el cumplimiento de la misión. Esto crea mayor escenario de inestabilidad que podrá ser contraproducentes para sus planes e inesperado para su posible víctima.

6. Las organizaciones deberán estar preparadas para asumir escenarios asimétricos de operaciones cibernéticas, las cuales podrán venir de diferentes lados y puntos de acción, de frentes amigos (posiblemente troyanizados vía la cadena de suministro), basados en desinformación creíble de terceros de confianza o posiblemente de acciones de personal interno debidamente distraído y engañado para generar mayor ruido y confusión que lleve a la organización a la inestabilidad, incierto y caos, escenario ideal para el adversario para concretar su agenda y pasar desapercibido en medio del descontrol y las acciones erráticas de la organización.

Reflexiones finales

Estas cincos declaraciones tomadas de la dinámica de la reciente producción de James Cameron, sólo son una excusa para explorar y profundizar en el estudio del adversario, una forma pedagógica para expandir una ventana de aprendizaje que permita a la función de seguridad y control mantenerse alerta, vigilante y entrenada para encontrarse con la incertidumbre y la volatilidad que representa el contexto actual para las organizaciones modernas.

Un adversario cada vez más entrenado, motivado y con aliados establece una amenaza cada vez más compleja y poco visible, dada su capacidad de mimetización con la realidad circundante que termina creando en las áreas de seguridad y control un superávit de futuro y paranoia, que muchas veces termina funcionando en contra de su propia misión: defender la promesa de valor de las empresas ajustada al apetito de riesgo de la compañía.

El reto más que contar con mayores y mejores tecnologías de seguridad y control, es establecer un equilibrio dinámico con la inevitabilidad de la falla, un pacto con el incierto de la materialización de una vulnerabilidad, con el fin de crear espacios de respuesta resilientes que preparen a la empresa como un todo, para mantenerse operando y viable en el mediano y largo plazo a pesar de la materialización exitosa de eventos cibernéticos inesperados.

Fuente: https://www.linkedin.com/posts/jeimy-cano-ph-d-cfe-3aa253_ciberlideraxgo-activity-7016151383665975296-Xgvl?utm_source=share&utm_medium=member_ios

LANZAMIENTO DE LIBRO:

Herbert Calderón Alemán CPP, PSP, PCI

Vicepresidente Regional Senior Grupo 8 (Sudamérica) - ASIS International

Certtficado CPP, PSP, PCI por ASIS International. Certificado como Examinador de Fraudes CFE – ACFE. Magister en Seguridad y Defensa Nacional (Colombia) Past President ASIS Perú. Actualmente Director de Seguridad Patrimonial en Consorcio Constructor Metro 2 Lima - CCM2L.

Erróneamente planteamos que el proceso de producción de toda operación de bienes o servicios, es un proceso aislado y diferente al de seguridad o protección patrimonial. Sin embargo un sistema competente preserva y protege a la operación.

En las líneas de mi texto describo experiencias y soluciones totalmente propias o de mi autoría, para ayuda no solamente a los profesionales del rubro sino a todos en general en la empresa.

ASIS INTERNATIONAL | LATAM

SAVE THE DATE

II CONGRESO ASIS **LATAM**

SEGURIDAD SIN LÍMITES

"Juntos somos más fuertes"

26 y 27 de octubre 2023, Lima - Perú

swissôtel LIMA

ASIS INTERNATIONAL® | Lima, Peru Chapter

1er WORKSHOP 2023

- Estado de la Ciberseguridad y Ciberdefensa en el Perú
- Ingredientes de seguridad para preservar toda operación productiva

ACCESO LIBRE

SÓLO PARA MIEMBROS ASIS

Registro: administración@asis.org.pe

www.asis.org.pe

18 febrero (9:00 a 12:30)

EDIFICIO TORRE BEGONIAS

Sala Sum 1 Calle Begonias 415 piso 2 - San Isidro

ASIS INTERNATIONAL® | Lima, Peru Chapter

1er WORKSHOP 2023

Sábado 18 de febrero

PUBLICACIONES EN REDES

El sábado 11 de febrero se realizó la primera reunión de coordinación de nuestra Comunidad WIS (Women In Security) de ASIS Lima, Perú - Chapter. 🇵🇪
Felicitaciones y éxitos para este 2023!

El 03 de febrero en el Leadership Exchange, ASIS International se premió como Senior Regional Vice President (SRVP) del año a:

- Marco Antonio Vega. CPP (SRVP Grupo 7)
- Herbert CALDERON, CPP, PCI, PSP (SRVP Grupo 8)

Un importante premio como reconocimiento a un gran trabajo realizado por la profesionalización de la seguridad y su liderazgo voluntario en LATAM & CA.

NEWSLETTER

ASIS INTERNATIONAL | Lima, Peru Chapter

Perú Edición **01/2023**

Directiva 2023

ASIS PERÚ

Presidente
Maurice Frayssinet Delgado

Vicepresidente
Jorge Quevedo Hermoza

Secretaria
Patricia Fernández Muriel

Tesorero
Cristian Valenzuela Morales

www.asis.org.pe
informes@asis.org.pe

CERTIFICACIONES ASIS INTERNATIONAL

CPP Certified Protection Professional
Board Certified in Security Management

Certificado en Protección Profesional (CPP)

Es la certificación que proporciona pruebas demostrables de los conocimientos que posee el profesional de seguridad en las ocho áreas estratégicas que define ASIS.
La certificación CPP es acreditada y respaldada por la Junta de Certificaciones de ASIS en Gestión de Seguridad.

PCI Professional Certified Investigator
Board Certified, ASIS International

Certificado de Investigador (PCI)

Es la certificación que proporciona pruebas demostrables de los conocimientos y la experiencia que se posee en el manejo de los casos, recolección de evidencias, así como en la elaboración de informes y testimonios para respaldar los hallazgos.
Los profesionales que obtienen el PCI son acreditados por la Junta de Certificación de ASIS en Investigaciones.

PSP Physical Security Professional
Board Certified, ASIS International

Certificado de Profesional en Seguridad Física (PSP)

Es la certificación que proporciona pruebas demostrables de los conocimientos y la experiencia que se posee en evaluación de la amenaza y análisis del riesgo, en los sistemas integrados de seguridad física, y en la adecuada identificación, implementación y permanente evaluación de las medidas de seguridad.
Los profesionales que obtienen la certificación PSP son acreditados por la Junta de Certificación de ASIS en Seguridad Física.

APP Associate Protection Professional
Board Certified in Security Management Fundamentals

Profesional de Protección Asociado (APP)

Es la certificación que proporciona el primer "peldaño" en la escala de carrera de gerente de seguridad. Al obtener la aplicación, sus colegas y supervisor le mostrarán que ha dominado los cuatro dominios de esta aplicación.

Síguenos en: