NEWSLETTER

Perú Edición **10/2019**

Editorial

La región 8C de ASIS International realizará este 07 y 08 de noviembre en Santiago de Chile el VIII Encuentro Regional de Seguridad el cual tiene como tema central la Protección de Infraestructuras Críticas.

Contará con expositores internacionales y como invitada especial la Presidenta Mundial de ASIS International señora Christina Duffey, CPP.

ASIS PERÚ prepara una importante delegación a la cual te invitamos a unirte.

Asimismo, durante este mes continuamos con las actividades de beneficio de nuestros miembros y la comunidad de seguridad. Así como también nuestro apoyo institucional eventos como el de ASBANC BIS-2019 y compartimos artículos que abordan temas de Riesgo, Métricas e informes, Amenazas Hibridas en Infraestructuras Críticas y Seguridad de nuestro Patrimonio Cultural.

ASIS International

SOMOS UNA COMUNIDAD GLOBAL Y DIVERSA

Fundada en 1955, ASIS International es una comunidad global de profesionales de la seguridad, cada uno de los cuales tiene un papel en la protección de los activos: personas, propiedades y / o información.

Nuestros miembros representan prácticamente todas las industrias en los sectores público 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 transición de las fuerzas de la ley o el ejército, la comunidad ASIS es global y diversa.

"La mayor organización de promoción de la profesión de seguridad en todo el mundo".

INDICE

LA SOCIEDAD DEL RIESGO

Al decir de ULRICK BECK, en su obra la Sociedad del Riesgo, en la antigüedad fueron las religiones las que entregaban certezas antes los riesgos, luego fue la ciencia; sin embrago en la actualidad, mas ciencia no significa necesariamente más Seguridad. Así, el riesgo característico de nuestra época invade el ámbito mismo de la ciencia.

Esto hace que el individuo moderno desconfíe de la ciencia y se vea en la necesidad de movilizarse para poder tomar parte de las decisiones riesgosas que tradicionalmente han estado en manos de los expertos (políticos y científicos).

Es interesante este planteamiento sociológico de Beck en su libro La sociedad del Riesgo, siendo cada vez más incierta su administración, especialmente en escenarios complejos.

Resulta una necesidad imperiosa que los profesionales dedicados a la Seguridad y a Gestión de los Riesgos estén a la vanguardia del conocimiento que les permita aportar análisis y decisiones inteligentes para hacer de su trabajo, de cara a la transformación digital, un aporte real y seguro a la sociedad toda.

Estar a la vanguardia, para los profesionales de la Seguridad, no solo significa aquello referido a la actividad cognitiva, sino que, tan importante como aquello, es ejercer un verdadero LIDERAZGO en sus organizaciones, esto significa sumar al conocimiento, el desarrollo de Talentos, mejorar la Actitud frente a las acciones y preocuparse del Entorno de cada persona en la organización, trabajando el empoderamiento cada día; saliendo de la zona de confort y siempre dispuestos a mejorar el rendimiento, dándole un sentido al Trabajo.

En ese sentido ASIS International promueve y desarrolla actividades a nivel global en beneficio de la comunidad de profesionales de Seguridad.

Y un evento especial es el que se llevará a cabo el 7 y 8 de noviembre, el VIII Encuentro de Profesionales de Seguridad de la Región 8 C de ASIS International, integrado por todos los países del Cono Sur de América, el cual se ocupará de tratar el tema central “PROTECCIÓN DE INFRAESTRUCTURAS CRITICAS Y COMUNIDADES RESLIENTES, entregando a los profesionales de la Seguridad las herramientas para, siempre, estar enfrentando los Riesgos anticipadamente.

Invito a informarse e inscribirse en:
www.encuentroregionalasis.cl

Alfredo Iturriaga Neumann, CPP
Director Académico
VIII Encuentro Regional de Profesionales
Región 8 C - ASIS International

BIS 2019

BUSINESS INNOVATION SUMMIT

CUMBRE DE LA INNOVACIÓN

CÁMARA DE COMERCIO DE LIMA

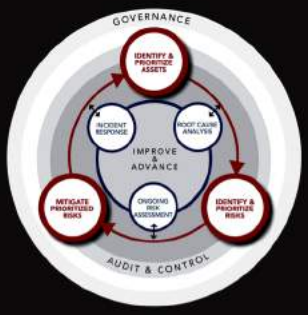
06 Y 07 DE NOVIEMBRE

Organiza: asbanc — Asociación de Bancos del Perú

Apoyo Institucional: ASIS International — Perú Chapter

Principales temas:

- Desarrollo de CSIRT
- Tecnología G5
- Computación cuántica
- Identidadd en el ciberespacio
- IoT (Intenet of Things)
- Ciudades Inteligentes
- Innovación
- Innovación
- Criptomonedas
- AI – Artificial Intelligence
- Rol del Reglador / Procesos de transformación digital / Star Ups
- Ciberseguridad en el marco de la Alianza del Pacífico



WORKSHOP IV

02 DE OCTUBRE DE 2019

ESRM
Enterprise Security Risk Management

LA GESTIÓN EMPRESARIAL DE LOS RIESGOS DE SEGURIDAD (ESRM) : UN ENFOQUE HOLÍSTICO A LA SEGURIDAD

Las organizaciones están continuamente expuestas a una serie de amenazas en evolución que crean una multitud de riesgos de seguridad. Los riesgos de seguridad para la empresa no se han visto ni administrado de manera consistente a través de principios y procesos definidos de administración de riesgos. Un enfoque coherente y holístico permitirá a las organizaciones gestionar eficazmente los riesgos de seguridad y los impactos en el negocio. ESRM necesita estar completamente integrado en los procesos corporativos en todos los niveles de la empresa y por cada profesional de riesgos de seguridad. Por lo tanto, el público es cualquier persona involucrada en la identificación, comprensión y / o gestión de riesgos de seguridad, incluyendo:

- Líderes empresariales: los ejecutivos y gerentes de toda la organización obtendrán una mejor comprensión de las mejores prácticas aceptadas por la industria relacionadas con la gestión del riesgo de seguridad empresarial.
- Profesionales de seguridad: los profesionales de seguridad de todos los niveles encontrarán en estos principios de ESRM un conjunto de prácticas comunes y repetibles que ayudarán a identificar, cuantificar, priorizar y administrar el riesgo de seguridad de manera consistente.
- Profesionales de auditoría y riesgos: este documento proporcionará un marco común de prácticas generalmente aceptadas relacionadas con la gestión de riesgos de seguridad en una empresa.

El ESRM es un proceso de administración utilizado para administrar de manera efectiva los riesgos de seguridad, tanto de forma proactiva como reactiva, en una empresa. ESRM evalúa continuamente el alcance completo de los riesgos relacionados con la seguridad para una organización y dentro de la cartera completa de activos de la empresa. El proceso de gestión cuantifica las amenazas, establece planes de mitigación, identifica las prácticas de aceptación de riesgos, gestiona incidentes y guía a los propietarios de riesgos en el desarrollo de esfuerzos de remediación.

Nuestro agradecimiento a:
Carlos Ramírez CAE, CPP, CPO, CAMS, CICA, CSSM
Herbert CALDERON, CPP, PCI, PSP, CSMP®M.ISMI,CFE

DEMUESTRE EL VALOR DE SU PROGRAMA: CREE UN INFORME DE MÉTRICAS DE SEGURIDAD CONVINCENTE

Desarrollar y mantener una gestión de riesgos de seguridad de alta calidad o un programa de resiliencia empresarial requiere la dedicación de aquellos de nosotros encargados de estas responsabilidades. Se necesita planificación, revisión, mejora continua. En mi artículo a principios de este año sobre la comunicación del riesgo de seguridad a los ejecutivos de negocios, hablé sobre la necesidad de proporcionar información cuantitativa y objetiva para su audiencia comercial. Entonces, ¿cómo les demuestras eso? Si se parece a miles de directores de programas en nuestra industria, intentará comunicar que está haciendo un buen trabajo a través de un Informe de métricas. Si usted es como miles de patrocinadores ejecutivos en todas nuestras empresas, su respuesta a estos informes bastante tradicionales es a menudo ... "¿Y qué?"

El propósito de las métricas

¿Por qué tantos de nosotros en administración de programas pasamos tanto tiempo recolectando, organizando y presentando datos, solo para que nuestros informes sean descartados con poca o ninguna atención prestada?

El propósito de un informe de métricas es (o debería ser) educar al lector; para decirles algo que necesitan saber; para informarles de algo que tendrá un impacto en sus vidas (negocios o de otro tipo). ¿Tus informes hacen eso? ¿Tiene algún informe o comunicación diaria / semanal que realmente le guste leer? ¿Qué tienen en común? ¿Qué los hace valer tu tiempo?

Un ejemplo personal de un informe que me encanta y espero recibir es un informe financiero *. Cada mañana me entero de las tendencias y direcciones en los mercados del día anterior, recibo algunas noticias rápidas y digeribles sobre lo que causó esas tendencias y lo que podrían significar para mí en el futuro, y luego recojo uno o dos puntos de datos interesantes que no esperaba, pero que me enseñan algo, no obstante.

Eso es. Muy simple. Me da información sobre un tema que impacta mi vida y mis activos. Puede hacer lo mismo con su informe a sus partes interesadas sobre cómo está impactando sus activos. Mi ejemplo ni siquiera es un "informe corporativo", ¡pero es un GRAN informe! No se sienta atado a los métodos tradicionales de informes que ha visto en su organización. Si encuentra la manera correcta de conectarse con su audiencia, estarán más inclinados a leer su informe.

Cuando desarrolle un informe de métricas, puede hacerse algunas preguntas:

- ¿Quién es la audiencia para mi informe?
- ¿Que es lo que les importa?
- ¿Qué aspectos de mi programa afectan las cosas que les importan?
- ¿Qué datos mostrarán ese impacto y demostrarán el valor para ellos?

Adaptando su informe a su audiencia

En general, cuando diseña un informe para una audiencia ejecutiva, querrá escribirlo a nivel estratégico, en lugar de táctico. Una buena regla es que cuanto más "alto" esté su público en la organización, "más grande" debe ser la imagen. Los detalles de eventos y acontecimientos individuales darán paso a gráficos e imágenes que muestran tendencias a lo largo del tiempo o puntos de referencia en comparación con organizaciones similares.

Si su audiencia ejecutiva está en I + D o marketing, y está muy interesado en el riesgo de robo interno de propiedad intelectual, ¿qué puede proporcionarles que muestre el valor de lo que está sucediendo en su programa?

La métrica de la cantidad de dispositivos perdidos o robados y la tendencia de esas pérdidas a lo largo del tiempo es buena para mostrar la eficacia de su programa. Si tiende esos datos y los correlaciona con las horas / fechas / ubicaciones de cualquier sesión de entrenamiento que realice, aún mejor.

El mismo tipo de historia se puede mostrar con datos relacionados con cualquier actividad de mitigación y el riesgo que está mitigando. ¿Ha instalado un nuevo sistema de control de acceso para responder a un riesgo de intrusión externa? Todas estas historias, si están respaldadas por datos, muestran más a las partes interesadas de sus activos que simplemente informar sobre la cantidad de horas trabajadas por el equipo de seguridad o un recuento de la cantidad de veces que se completó una actividad como una patrulla.

DEMUESTRE EL VALOR DE SU PROGRAMA: CREE UN INFORME DE MÉTRICAS DE SEGURIDAD CONVINCENTE

Fuentes de datos

¿Qué lleva a la pregunta de dónde podría encontrar esos datos? Si no realiza un seguimiento de los incidentes, los tipos, los tiempos y el resultado de ellos, está en desventaja. Si no está siguiendo de cerca las actividades que realiza su equipo para mitigar los riesgos para la empresa, también tendrá dificultades para contar la "historia de valor".

Los datos que pueden ayudar a contar su historia están en todas partes, en todos los sistemas. Simplemente necesita saber dónde y cómo encontrarlo, luego juntarlo para hablar directamente sobre las cosas que le interesan a su audiencia.

Fuentes de datos:

- Registros electrónicos del sistema de seguridad.
- Planes y objetivos de negocios.
- Propietarios de negocios de activos clave / críticos
- Listas de inventario de activos
- Evaluaciones de riesgo
- Resultados del ejercicio BCP / DRP
- Informes de incidentes.
- Revisiones post mortem
- Informes de operación en curso.
- Inteligencia de código abierto

La recopilación de estos datos se logra más fácilmente en una de las muchas plataformas de software en el mercado diseñadas para rastrear y recopilar esta información. Los informes manuales y el seguimiento con hojas de cálculo e informes manuales de incidentes hacen que recopilar y adaptar informes a su audiencia sea mucho más difícil.

Definitivamente vale la pena invertir en un buen sistema de gestión y seguimiento de incidentes porque le ayuda a recopilar métricas "buenas". ¿Qué es exactamente una métrica "buena"? Los datos ideales para incluir en un informe deben ser:

- Repetible (se puede recoger más de una vez)
- Sin jerga (su audiencia no debería necesitar un manual de seguridad para leerlo)
- Medido constantemente (tiene un método para recolectarlo que se sigue regularmente)

Todo esto se ve facilitado por una buena gestión y herramientas de software de informes.

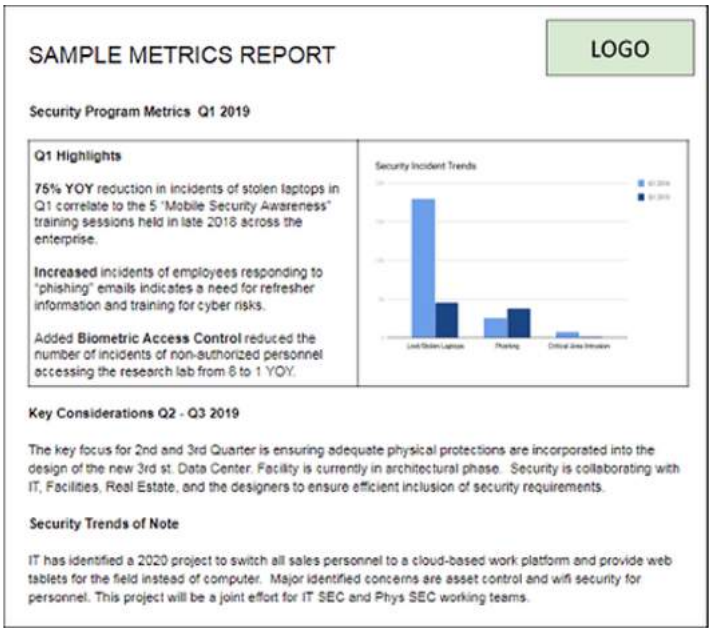
Diseñando el Informe

Al crear informes para una audiencia de nivel ejecutivo, tenga en cuenta que han recibido muchos otros informes de métricas ese mismo día y que solo tienen unos minutos para darles a cada uno de ellos. Algunos consejos para diseñar los informes y cómo decidir exactamente qué poner en ellos:

- Asegúrese de que sus datos tengan una razón para estar en el informe: está comunicando el punto deseado al lector.
- Asegúrese de que sea claro, conciso y relevante.
- Use gráficos para presentar la información numérica tanto como sea posible, en lugar de tablas y cuadrículas.
- Mantenga las narraciones cortas y al punto.
- Presente datos similares en un horario regular para mostrar tendencias a lo largo del tiempo
- Use solo información actualizada en los informes, evite las estimaciones tanto como sea posible.

Ejemplo

Aquí hay un ejemplo rápido de un posible informe del equipo de seguridad al director de tecnología. Las tendencias se centran en cuestiones de TI y tecnología, y se ajustan a lo que nuestro CTO imaginario ha expresado su interés. Es una página, pero les brinda los datos que necesitan saber para comprender que el departamento de seguridad está haciendo lo que se le encarga.



SAMPLE METRICS REPORT

LOGO

Security Program Metrics Q1 2019

Q1 Highlights

75% YOY reduction in incidents of stolen laptops in Q1 correlate to the 5 "Mobile Security Awareness" training sessions held in late 2018 across the enterprise.

Increased incidents of employees responding to "phishing" emails indicates a need for refresher information and training for cyber risks.

Added **Biometric Access Control** reduced the number of incidents of non-authorized personnel accessing the research lab from 6 to 1 YOY.

Security Incident Trends

Key Considerations Q2 - Q3 2019

The key focus for 2nd and 3rd Quarter is ensuring adequate physical protections are incorporated into the design of the new 3rd st. Data Center. Facility is currently in architectural phase. Security is collaborating with IT, Facilities, Real Estate, and the designers to ensure efficient inclusion of security requirements.

Security Trends of Note

IT has identified a 2020 project to switch all sales personnel to a cloud-based work platform and provide web tablets for the field instead of computer. Major identified concerns are asset control and wifi security for personnel. This project will be a joint effort for IT SEC and Phys SEC working teams.

Rachelle Loyear

Enterprise Security Risk Management

Es la actual gerente de programa del programa ASIS ESRM, es miembro y presidente reciente del ASIS Crisis Management and Business Continuity Council, y es miembro del ASIS IT Security Council. Es Gerente Certificado de Seguridad de la Información (CISM) a través de ISACA, Master Professional Continuity Professional (MBCP) a través de DRI International, Miembro Asociado de Business Continuity International (AFBCI), y Certificado Profesional de Gestión de Proyectos (PMP) a través del Project Management Institute (PMI)

WEBINAR VII

LAS CERTIFICACIONES:
HERRAMIENTAS EN LA CONDUCCIÓN
DE RIESGOS EMPRESARIALES

16 DE OCTUBRE DE 2019
Hora: 16:00 pm

WEBINAR VIII

SEGURIDAD EN AGRO EXPORTADORA
(REGIÓN ICA - PERÚ)

23 DE OCTUBRE DE 2019
Hora: 16:00 pm

WEBINAR IX

ENTREVISTAS ÉTICAS

13 DE NOVIEMBRE DE 2019
Hora: 16:00 pm

LAS NUEVAS AMENAZAS SON HÍBRIDAS

En un entorno dinámico y complejo como el actual, es obligatorio una gestión eficaz de la información que nos permita conocer los hechos precisos en el momento exacto y tener la capacidad de actuar sobre ellos. Esta necesidad de información se ha desarrollado técnica y estratégicamente a lo largo de los siglos, hasta consolidarse en la implantación de **unidades de inteligencia y Ciberseguridad integral** en las organizaciones tal y como hoy se conocen.

Una combinación de amenazas convencionales y no convencionales orientadas a la desestabilización de nuestra forma de vida, y cuya identificación y atribución resultan especialmente complicadas, este tipo de acciones son aquellas perpetradas tanto por Estados como por actores no estatales.

Un ataque masivo y coordinado hacia uno o más sectores críticos establece una condición importante y crítica para una nación, pone en juego su estabilidad y la confianza de la ciudadanía en el Estado para enfrentarse a estas amenazas. Esto hace de las infraestructuras críticas un objetivo de ataque para aquellos agentes que pretendan influir o debilitar a una nación.

La importancia de la Ciberseguridad y la Seguridad Integral en las Infraestructuras Críticas.

El número de incidentes detectados en los operadores de servicios esenciales está aumentando en los últimos años. Esto se debe, en parte al uso de técnicas de IT en sistemas OT, sin concurrir en los mecanismos de defensa que los primeros integran, haciendo que estas infraestructuras sean más eficientes pero, a su vez, más vulnerables a ataques. Una problemática específica de los sistemas industriales que se tiene que tomar es el hecho que en un principios no han sido diseñados para considerar los aspectos de **Seguridad Integral** y **Ciberseguridad**.

Otros aspectos como la obsolescencia de los sistemas o la falta de actualizaciones o de parches sobre las vulnerabilidades detectadas contribuyen a su vez a aumentar el riesgo para las infraestructuras.

El Estado, para lograr defenderse de estas amenazas híbridas debe cambiar su concepto de seguridad tradicional, dando paso a una defensa integral, en la que se protejan su soberanía en el espacio digital y la protección de los derechos de sus ciberciudadanos frente a las amenazas emergentes en el escenario de una vida más digital y gobernada por la información.

La convergencia IT/OT, esto es la integración de los sistemas de tecnología de la información (IT), utilizados para computación centrada en datos, con sistemas de tecnología operacional (OT), utilizados para supervisar eventos, procesos, dispositivos y realizar ajustes en las operaciones empresariales e industriales.

La conexión de IT y OT, dentro de un marco de Ciberseguridad y Seguridad Integral, aporta grandes beneficios. Al liberar la enorme cantidad de datos que los sistemas OT genera, pasamos de la automatización a la optimización; para esto es necesario poder acceder en tiempo real a todo el contenido y a la información que se crea.

Gracias a esta integración, se produce una mejora en la producción y organización de los sistemas, así como una mejora en el flujo de información y el uso que se da a esta. El proceso de toma de decisiones se vuelve más ágil y eficiente, aumentando la satisfacción tanto del cliente, por la calidad del producto y servicio recibido, como por parte de los participantes, que disponen de un sistemas más eficaz y eficiente.

Dependencia de tecnologías emergentes (IIoT) en las infraestructuras críticas.

Todos estos dispositivos dotados de conectividad a Internet forman parte de lo que se conoce como Internet de las Cosas, o IoT (por sus siglas en inglés **Internet of Things**).

El Internet of Things (IoT) o Internet de las Cosas ha comenzado a formar parte de la vida cotidiana de la sociedad: hogares inteligentes, la educación inteligente, el cuidado de la salud inteligente, los wearables, el Internet de los Vehículos (IoV) y otras industrias, incluso las infraestructuras críticas hacen gran uso de esta tecnología jugando un papel fundamental en su transformación digital y en la hiperconexión de sus elementos en una era de conectividad de dispositivos industriales.

El ecosistema Industrial de las Cosas (IIoT) en las infraestructuras críticas incluye dispositivos, redes, plataformas y aplicaciones que requieren múltiples medidas de protección de la seguridad en cada capa, así como capacidades de inteligencia y de análisis de la seguridad de la totalidad de los datos para aprovechar la sinergia entre los dispositivos y la nube.

Aquí podemos encontrar sensores, actuadores y otros dispositivos controladores como PLC (Programmable Logic Controller), RTU (Remote Terminal Unit) o IED (Intelligent End Device), que han evolucionado a lo largo del tiempo.

LAS NUEVAS AMENAZAS SON HÍBRIDAS

La situación actual, aumentan los ciberataques dirigidos en las infraestructuras críticas.

La falta de visibilidad en la superficie de ataque es el mayor problema para evitar los ataques.
Las organizaciones necesitan visibilidad de sus entornos convergentes de TI-OT, IIoT para, no solo identificar dónde existen vulnerabilidades, sino también priorizar cuáles remediar primero.
La falta de personal y la dependencia de los procesos manuales obstaculizan su capacidad para remediar vulnerabilidades. Debe ser afrontado conjuntamente por equipos multidisciplinares. La Ciberseguridad y la Seguridad Integral que deben proporcionar estos dispositivos (IIoT) debe ser más elevada, ya que son usados en el entorno industrial, donde un fallo de seguridad podría representar un riesgo a gran escala. Por este motivo, es imprescindible mejorar la seguridad para evitar que los atacantes puedan conseguir información o haya problemas en infraestructuras críticas.

Nuevos retos para la Protección 360º de las Infraestructuras Críticas.

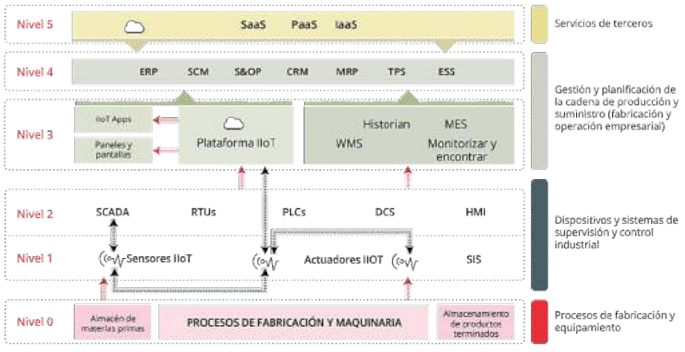
Las **campañas híbridas** son multidimensionales, combinando medidas coercitivas y subversivas, utilizando herramientas y tácticas tanto convencionales como no convencionales. Han sido diseñadas para ser difíciles de detectar y atribuir.
La **convergencia de TI / TO** es un proceso que ya se ha iniciado, al igual que el empleo de **Tecnologías emergentes IIoT**. Cuanto antes lo asuman las infraestructuras críticas y pongan esfuerzos para llevarlo a cabo de forma satisfactoria mejor posicionadas estaran de cara al futuro. Las dificultades para conseguirlo serán muchas, riesgos de seguridad, pero las ventajas finales compensarán el esfuerzo necesario.
La inclusión de los sistemas TO dentro de las redes TI permite ahorrar tiempo a la hora de realizar mantenimientos de rutina y llevar a cabo estas tareas de forma remota desde un panel de control central. Estas tecnologías también permiten nuevos modelos predictivos que posibilitan identificar debilidades, corrigiendo los problemas o reemplazando los dispositivos antes de que supongan un coste elevado en tiempo y dinero debido a un fallo.
La creación de **unidades de Inteligencia y Ciberseguridad integral** se constituye como una herramienta imprescindible para las infraestructuras críticas. Cualquier precaución es poca si hablamos de seguridad en dispositivos conectados a la red corporativa de una organización, por muy inofensivo que pueda parecer.

Es necesario comprender que cualquier dispositivo que se conecte a la red es susceptible de ser comprometido, sobre todo si existe una carencia de medidas de seguridad. El primer paso es ser conscientes de la existencia del peligro y posteriormente, implementar las medidas de seguridad necesarias a la prevención, detección de incidentes, mejorativas de la capacidad de resiliencia y por último recuperación temprana de las infraestructuras.
Grupo INV es la firma global y multinacional especializada con el propósito de ofrecer la mejor Seguridad integral, Ciberseguridad e Inteligencia de extremo a extremo a las organizaciones..

INCIBE: Modelo tradicional con entornos Ti y TO separados

Marco lógico de jerarquía de control según el modelo de Purdue

Modelo de referencia de alto nivel, Fuente: Good Practices for Security of Internet of Things in the context of Smart Manufacturing (ENISA)



Mikel Rufián Albarrán

Director Global de Ciberseguridad & Inteligencia - INV SYSTEMS PERU

Graduado en PDD (Programa de Desarrollo Directivo) por el IESE Business School, la Universidad de Navarra y Graduado en Ciencias Criminológicas y de la Seguridad por la Universidad San Pablo CEU, es Criminólogo especializado en Inteligencia Criminal (CRIMINT). Diplomatura en Criminología y un diploma específico en Criminalística. Es, asimismo, Detective y Director de Seguridad habilitado por el Ministerio del Interior y autorizado por la Dirección General de Policía, Graduado en dirección de Seguridad por la misma Universidad. Completó su formación con varios Masters, cursos y títulos de Postgrado en diversas materias de Inteligencia, Seguridad y Defensa, Terrorismo & Contraterrorismo, en técnicas de Análisis, en Social Media Business e Intelligence (SOCMINT), CM y Marketing 360º, Gestión y Desarrollo de Estrategias. Monitorización avanzada y analítica web

MACHU PICCHU PATRIMONIO CULTURAL Y SU SEGURIDAD

Machu Picchu es una ciudadela inca ubicada a 2490 metros sobre el nivel del mar, en el valle del río Urubamba, descansa sobre una formación rocosa, que sirve de enlace entre las montañas Hayna Picchu y Machu Picchu, así mismo, este antiguo santuario se erige en la cara oriental de la Cordillera central de los Andes peruanos.

Sus desarrolladas técnicas de terrazas agrícolas, así como su arquitectura, considerada como una de las más avanzadas por sus métodos de piedra pulida y la forma de traslado hasta el punto donde se le construyó, lo convierten en una morada inca famosa por sus sofisticadas paredes de piedra seca que combinan enormes bloques, así como los edificios fascinantes que se relacionan con las alineaciones astronómicas y sus vistas panorámicas. El uso exacto que tuvo sigue siendo un misterio en la actualidad.

De igual forma, sus atributos únicos en el mundo entero, así como sus majestuosa vista, hicieron que el 7 de julio de 2007, luego de una votación mundial que convocó a millones de electores, el público afirmara por gran mayoría declararla igualmente como una de las 7 maravillas del mundo moderno, hecho que se formalizó a través de una ceremonia que se llevó a cabo en Portugal.

Machu Picchu recibe cada día a miles de visitantes de todas partes del mundo, algunos deciden ingresar utilizando los trenes, otras escogen una de las rutas de senderismo más increíbles del planeta e ingresan por el camino inca. La pequeña ciudad de Aguas Calientes es la ciudad ubicada al pie de la ciudad inca de Machu Picchu, y como todas ciudades turísticas de América del sur atrae gente indeseable, nacional y extranjera, aunque son pocos los casos de delitos comprobados.

Amenazas al Santuario

Existen muchas amenazas para el Santuario: el turismo excesivo considerando la relativa fragilidad del sitio, la generación de desechos sólidos, las prácticas agrícolas insostenibles, sobrepastoreo e incendios forestales, la erosión agravante, los deslizamientos de tierra que amenazan constantemente, la extracción de minerales, introducciones de plantas exóticas, la planta hidroeléctrica con sus líneas de transmisión de energía, la ausencia de evaluaciones de impacto ambiental, security, la falta de estudios de vías de acceso alternativas al Camino Inca en exceso, la tenencia incompleta física y legal de las tierras, la multitud de partes interesadas y el complicado sistema de gestión.

Resumiendo las amenazas:

- Sobrecarga del camino Inca.
- Central hidroeléctrica y líneas de transmisión de energía.
- Desechos sólidos.
- Quemas e incendios forestales.
- Agricultura y ganadería.
- Derrumbes o deslizamientos.
- Extracción de piedra para artesanía y arena.
- Caza furtiva.
- Saneamiento físico y legal de terrenos incompleto por descoordinación institucional.
- Moda de algunos turistas de tomarse fotografías desnudos en el complejo arqueológico del Machu Picchu y luego colgarlas en blogs.

Sistema de Seguridad

Las autoridades de turismo en la región de Cusco firmaron acuerdos para aumentar la seguridad de visitantes nacionales y extranjeros, además de incrementar el cuidado del patrimonio arqueológico y natural, en el santuario de Machu Picchu y también los sectores más importantes del Camino Inca. Se instalaron cámaras de vigilancia recientemente lo cual le permitirá un mayor cuidado del maravilloso patrimonio arqueológico del santuario, brindar mayor protección y apoyo a todos los visitantes así como también prevenir excesos que han ocurrido en ese lugar de intensa energía espiritual, donde algunos visitantes se han dejado llevar por la euforia, celebrando rituales religiosos que llegaban al nudismo y otras faltas contra el pudor.

La aplicación de seguridad “Tourism Police Peru” es una aplicación gratuita que está conectada con la central de control del Corredor Turístico preferencial, y le servirá para reportar cualquier emergencia que pueda tener. Al momento de reportar una emergencia, esta app envía automáticamente su ubicación, generando una respuesta inmediata de las unidades cercanas a su posición. Está disponible para smartphones y tabletas con sistema Android.

Herbert CALDERON, CPP, PCI, PSP, CSMP®M.ISMI,CFE

Director de Seguridad Patrimonial. en Consorcio Constructor Metro 2 Lima - CCM2L

Amplia experiencia en gestión corporativa de seguridad. Cuenta con las tres certificaciones ASIS Internacional. Certificado en Protección CPP, Certificado en Investigaciones PCI y Certificado en Seguridad Física PSP. Certificado como Examinador de Fraudes CFE – ACFE. Especialista en Administración de la Seguridad y Magister en Seguridad y Defensa Nacional en Colombia. Past President ASIS Perú y ARVP Región 8C ASIS Int. Gerente Corporativo de Seguridad Integral del Grupo Gloria, Director Académico del Centro de Estudios de Seguridad.

NEWSLETTER

Perú Edición **10/2019**

DIRECTIVA

Percy Quispe **MBA, CIP**
Presidente

Martín Gálvez
Vicepresidente

Luis González **CPP, PSP**
Secretario

Carlos Prado
Tesorero

ASIS INTERNATIONAL
Perú Chapter

+51 953 387 766
informes@asis.org.pe
www.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 Managememt 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: