Newsletter

ASIS INTERNATIONAL Perú Chapter

ASIS Perú

Edición Especial **8/2019**

Editorial

Renovados con el reconocimiento logrado por ASIS PERÚ, elegido por ASIS International como ganador a nivel Global del 2019 IB Hale Chapter of the Year Award. Sólo posible con el trabajo y continuo apoyo de nuestros miembros, consejo consultivo, comités y directiva. La premiación será en el marco del GSX (Chicago, IL. del 8 al 12 de setiembre).

También en agosto se desarrollo en Cartagena, Colombia el II Foro Latinoamericano de Mujeres en Seguridad (WIS-2019) evento que se consolida como un referente en Seguridad cuya primera edición fue el 2018 en Lima - Perú.

Asimismo, durante este año ASIS PERÚ realizó diferentes actividades entre las que destaca el I Foro de Jóvenes Profesionales, evento que fue todo un éxito y logró convocar a más de 200 profesionales de Seguridad. En ese sentido en esta edición compartimos artículos que abordan como la tecnología nos afecta y lo importante de la comunicación y colaboración.

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

- **II Foro Latinoamericano de Seguridad** 04
- **Foro Jóvenes Profesionales** 07
- **Juegos Panamericanos & Parapanamericanos** 11
- **ASIS PERÚ - Resumen de Actividades 2019** 12
- **La Agenda 2030, las tecnologías exponenciales y la colaboración entre sectores** 03
- **Ciberdefensa y Ciberespacio** 06
- **¿Cómo la neuroseguridad y la seguridad por diseño afecta a la seguridad privada?** 08
- **Inteligencia de Amenazas, dando un paso por delante** 10

ASIS PERÚ fue elegido como el ganador del 2019 I.B. Hale Chapter of the Year Award

OTORGADO POR ASIS INTERNATIONAL

Este premio reconoce anualmente a nivel global al Capítulo más destacado en su grupo y que ha realizado la contribución más significativa a ASIS y a la profesión de seguridad durante el año.

Acompáñanos a la ceremonia de recepción del premio.
Martes 10 de septiembre, de 8:30 a 10:00 am.
Global Security Exchange en Chicago, IL

ASIS International and the ASIS Foundation

Dear Percy Quispe,

I am pleased to inform you that your Chapter has been selected as a winner of the 2019 I.B. Hale Chapter of the Year Award. Congratulations! We are truly grateful for the work you've done this year and look forward to celebrating your accomplishments.

We would like to invite you, and representatives from your chapter, to join us at a new ASIS Awards Reception to be held on Monday, 9 September, from 4:00 – 5:30 pm at Global Security Exchange (formerly ASIS Seminar) in Chicago, IL. The reception is open to all GSX all-access pass attendees and we certainly hope you and your fellow chapter members will join us in celebrating this accomplishment.

CPO© Oficial Certificado de Protección

Felicitamos al
Sr. Júlio Huamán
miembro de ASIS PERÚ
por ser el ganador de la **BECA CPO©**

Otorgado por ASIS FOUNDATION

CPO
Certified Protection Officer
OFICIAL DE PROTECCIÓN
CERTIFICADO
IFPO

LA AGENDA 2030, LAS TECNOLOGÍAS EXPONENCIALES Y LA COLABORACIÓN ENTRE SECTORES

La Agenda 2030 para el Desarrollo Sostenible es un documento que traza el plan de acción para aminorar los desequilibrios ambientales, económicos y sociales; su contenido explora la ruta de un nuevo modelo de desarrollo que busca la prosperidad y bienestar, mediante 17 Objetivos (ODS) acompañados de 169 metas, que se fundamentan en los siguientes ejes conceptuales:

- **El enfoque de derechos**: implica el cumplimiento de los compromisos de los Estados asumidos en su legislación interna y en la normativa internacional.
- **Igualdad sustantiva y cierre de brechas:** se debe avanzar hacia sociedades más igualitarias, solidarias y cohesionadas.
- **Promoción del empleo pleno y productivo y de calidad:** el pleno empleo es imprescindible para lograr la igualdad y sostenerla en el largo plazo.
- **Perspectiva de género:** la eliminación de la desigualdad entre mujeres y hombres es un eje transversal que exige la superación de los roles tradicionales basados en la división sexual del trabajo.
- **Responsabilidades comunes pero diferenciadas:** las obligaciones de los países en materia ambiental, económica y social deben ser proporcionales a sus niveles de desarrollo.
- **Progresividad y no regresividad**: es necesario establecer criterios claros de progresividad en el cumplimiento de las metas y no aspirar sólo a cambios incrementales simples o marginales.
- **Indivisibilidad e interdependencia**: la Agenda 2030 debe ser un conjunto integrado y no una suma de objetivos y metas aislados.
- **Participación ciudadana:** Es necesario construir una nueva ecuación entre Estado, mercado y sociedad", en un contexto de diálogo entre sector público y privado y actores sociales.
- **Transparencia y rendición de cuentas:** el acceso a información pertinente, suficiente y oportuna es un requisito fundamental para consolidar gobiernos abiertos.

La complejidad de la Agenda 2030 precisa financiamiento, innovación e incorporación de tecnología; y principalmente colaboración entre sectores (Sector público, sector privado, sociedad civil, académica y medios de comunicación). En este sentido, las tecnologías exponenciales, son una propuesta factible, a través de las cuales, se catalizan resultados y beneficios.

En 1965 Gordon Moore, cofundador de Intel "afirmó que el número de transistores por centímetro cuadrado en un circuito integrado se duplicaba cada año y que la tendencia continuaría durante las siguientes dos décadas. Diez años después, modificó esta afirmación y predijo que el ritmo bajaría aproximadamente cada 18 meses.

Es decir, la tecnología aumenta a una velocidad imposible de seguir y se supera constantemente. Para Peter Diamandis, existen seis Ds (Six Ds) que explican cómo funcionan las tecnologías exponenciales:

1. Digitalización (*Digitized*).
2. Engañoso (*Deceptive*).
3. Disruptivo (*Disruptive).*
4. Desmonetización (*Demonetized*).
5. Desmaterialización (*Dematerialized*).
6. Democratización (*Democratized*

En conclusión, el impacto de la tecnología es impresionante en nuestra región, se mueve con rapidez y acierto. No obstante, la misma requiere una mejor conexión con las actuales políticas públicas, lo cual es una oportunidad para que el sector privado colabore con el sector público, en generar marcos normativos que impulsen una mayor seguridad, inclusión digital e innovación exponencial.

Moisés Benamor

Jefe de Instituciones Representativas
Departamento de Sustentabilidad Democrática y Misiones Especiales
Secretaria para el Fortalecimiento de la Democracia
Organización de los Estados Americanos – OEA

II FORO LATINOAMERICANO DE MUJERES EN SEGURIDAD

1 y 2 DE AGOSTO 2019

ASIS INTERNATIONAL

IIFOROWIS2019

"EQUIDAD FACTOR DE CONFIANZA QUE GENERA SEGURIDAD"

El II Foro Latinoamericano de Mujeres en Seguridad se realizó el 1 y 2 de agosto en la ciudad de Cartagena de Indias, Colombia. Evento que convocó a más de 200 personas, hombres y mujeres, unidos por su pasión por la Seguridad. Dos días intensos de compartir conocimientos, experiencias y buenas prácticas. Liderado por mujeres bajo el lema "Equidad factor de confianza que genera Seguridad".

Evento resaltado por su calidad de ponentes y temática, entre las principales exposiciones se abordó Equidad, Innovación, Inteligencia Artificial, Ciberseguridad, ESRM, retención de talento entre otros.

Destacó la entrevista de Peter O'Neil (CEO ASIS International) a la Sra. Marta Lucia Ramírez, Vicepresidenta de Colombia, y a las señora Niorin O'Sullivan, Subsecretario General de Seguridad de las Naciones Unidas.

Gladys Andrich, Directora de Relaciones Institucionales de ASIS PERÚ y Milagros Céspedes (WIS Liason – ASIS PERÚ) cumplieron exitosamente con representarnos.

II FORO LATINOAMERICANO DE MUJERES EN SEGURIDAD

1 y 2 DE AGOSTO 2019

Apoyar, inspirar y promover, los tres pilares de WIS se pusieron de manifiesto en el II Foro Latinoamericano Women In Security.

El Consejo Fundador Women In Security LATAM liderado por María Teresa Septien (México), Tatiana Scatena (Brasil), Sonia Andrade (Colombia), Andrea Herrera (Colombia), Gladys Andrich (Perú) y Milagros Céspedes (Perú) fue una pieza fundamental para la realización del II Foro WIS. Asimismo, a través de su labor tienen como objetivo lograr fomentar la participación de más mujeres en Seguridad. Además, establecieron por primera vez el "He for WIS" como reconocimiento a los caballeros que apoyan, promueven e inspiran el trabajo WIS, recibieron este reconocimiento: Jaime P. Owens, CPP, Pablo Colombres, CPP y el Coronel(r) Luis Enrique La Rotta. Se resaltó también el gran apoyo de Enrique Tapia Padilla MA CPP y de José Echeverria, MSc, CPP.

Se tuvieron bloques sobresalientes con las WIS representantes de diferentes países, compartiendo casos de éxito de mujeres en Seguridad. Por Perú se expuso la iniciativa "Patronato Barrio Seguro", trabajo de integración y articulación entre los sectores Público y Privado.

Finalmente, cada representante WIS eligió un valor que la representa. Nuestros principales banderas y los elegidos por WIS Perú fueron Integración y Servicio, valores considerados como columnas que sustentan nuestro trabajo díario Sin duda el II Foro WIS fue una experiencia inolvidable y gratificante.

¡Nos vemos en el III Foro WIS 2020 - México!

CIBERDEFENSA Y CIBERESPACIO

La ciberdefensa es la capacidad militar que permite actuar en el ciberespacio frente a amenazas o ataques y que vulneren a la seguridad nacional.

El ciberespacio es mucho más que la internet. Realmente es el entorno digital que empleamos como los teléfonos IP e celulares, los sensores digitales inalámbricos en las casas o empresas, denominados IoT (*Internet of Things*), nuestras computadoras y tablets, y todo sistema informático que intercambia información física o inalámbricamente, con Internet o sin ella. Podemos definir sus componentes como hardware, con las redes inalámbricas incluidas, el software, y las personas. Sí, nosotros somos parte del ciberespacio ya que somos los responsables de manipular el USB, los CDs, de hacer click con el mouse o de teclear. Y por ende, somos el punto más vulnerable para cualquier ataque por nuestro exceso de confianza.

En este nuevo dominio, el ciberespacio, debido a sus enormes dimensiones, presentan un campo de desarrollo para actividades ilegales que es difícil de rastrear y muchas veces, inclusive, de detectar. Los cibercriminales emplean estos sistemas interconectados para determinar sus vulnerabilidades con la finalidad de emplearlas para robar y vender información o dinero, o simplemente para realizar propaganda ideológica conocida como Hacktivismo.

Como se puede ver, las amenazas existen y se pueden clasificar como penetración de redes, que buscan alterar la confidencialidad, integridad o disponibilidad de la información, y como denegación de servicios, que mediante solicitudes masivas a un mismo servidor lo saturan e impiden que responda al resto de usuarios.

La Marina de Guerra, en su preocupación permanente por defender los intereses nacionales e institucionales, ha implementado la Comandancia de Ciberdefensa que cuenta con capacidades de operaciones de defensa para la protección de las redes propias, operaciones de explotación que se encarga de determinar las amenazas que traten de impedir la libertar del uso del ciberespacio por parte de nuestras fuerzas, y operaciones de respuesta con capacidades ofensivas para restaurar el correcto empleo del ciberespacio y para disuadir a actores poco amigables. Adicionalmente, también tenemos un área de forense informática, ingeniería reversa e investigación y desarrollo que busca analizar el comportamiento y los vectores de ataque del malware y así mejorar nuestras propias capacidades de defensa.

Para finalizar, es importante reaccionar y tomar las medidas de seguridad necesarias para no caer en la estadística de los ataques digitales. Las siguientes son algunas recomendaciones que pueden contribuir a dificultar ser blanco de un ataque:

1. Contar con passwords complejos con más de 8 caracteres y que tenga mayúsculas, minúsculas, números y símbolos, no los comparta, y no los deje en un Post-It en su escritorio o computadora.
2. Emplear los cifradores de documentos que vienen en los programas que empleamos para redactarlos con la finalidad de encriptar los archivos que contengan información confidencial.
3. Emplear un antivirus para proteger su computadora y escanear todos los archivos que descargue desde USBs, emails o desde la misma internet.
4. Mantenga actualizados todos los parches de seguridad que le piden sus dispositivos como PCs, tablets y smartphones.
5. No abra o haga click en emails de procedencia dudosa. Verifique la dirección electrónica del remitente para ver si es original o no.
6. No usar software no autorizado o pirata porque viene con archivos maliciosos.

Si se aplican estas recomendaciones pueden sentirse menos vulnerables, pero lo más importante es compartirlas para que nuestro entorno sea más seguro.

CONTRALMIRANTE ENRIQUE LUIS ARNÁEZ BRASCHI
Comandante de Ciberdefensa de la Marina de Guerra del Perú

Graduado de la Escuela Naval del Perú y Magíster en Ingeniería de Control y Automatización de la Pontificia Universidad Católica del Perú (PUCP). Profesionalmente se ha desempeñado en la Marina de Guerra del Perú y, como docente, en cursos de la Escuela Naval y de la Escuela de Calificación de Oficiales. Asimismo, cuenta con amplia experiencia como catedrático en la Maestría de Ingeniería de Control y Automatización de la PUCP, en la Maestría de Sistemas de la Universidad San Martín de Porres (USMP) y en el área de control y robótica de la Carrera de Ingeniería Electrónica de la Universidad Peruana de Ciencias Aplicadas (UPC).
Ha prestado servicios en la Escuela Naval del Perú, en la Dirección General del Personal de la Marina, en la Comandancia General de Operaciones del Pacífico, en el Estado Mayor General de la Marina y en la Secretaría de la Comandancia General de la Marina como Subsecretario del Comandante General. Del mismo modo, ha prestado servicios como Oficial Enlace ante la Comandancia de las Fuerzas de las Flotas de la Marina de los Estados Unidos, y como Asesor del Presidente del Consejo de Delegados de la Junta Interamericana de Defensa en Washington, DC.
Es portador de las Condecoraciones Cruz Peruana al Mérito Naval, Medalla Naval de Honor al Mérito por haber ocupado el Primer Puesto de su Promoción, Medalla de la Junta Interamericana de Defensa, y Medalla a los Servicios Prestados de la Marina e Infantería de Marina de los Estados Unidos, así como diversas Condecoraciones, Medallas y Distinciones tanto de la Marina de Guerra del Perú como de otros Estados.

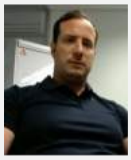
FORO JÓVENES PROFESIONALES

27 DE JUNIO DE 2019

Mensaje a los Jóvenes Profesionales

Matthew Porcelli, CPP
Presidente del Consejo de Jóvenes Profesionales ASIS International

José Barone, PSP
Coordinador Global Outreach de la Región Latinoamericana Comité de Jóvenes Profesionales ASIS Int.



Pablo Colombres, CPP
Vicepresidente Regional Senior Sudamérica. ASIS International

Junta Directiva Global Electa - ASIS International

- Godfried Hendriks (Presidente)
- Radek Havils (Miembro de la J.D.)
- Gail Esen (Miembro de la J.D.)
- Jaime Owens (Member of Board Directors)
- Malcolm Smith (Secretario J.D.)
- Tim McCreigth (Miembro J.D.)
- Jhon Petruzzi (Tesorero)

FORO SEGURIDAD E INNOVACIÓN EN LA 4TA REVOLUCIÓN INDUSTRIAL

El 27 de junio se realizó en Lima el I FORO JOVENES PROFESIONALES: SEGURIDAD E INNOVACIÓN EN LA 4TA REVOLUCIÓN INDUSTRIAL, nos acogió el impresionante auditorio de la Facultad de Derecho de la Pontificia Universidad Católica del Perú..

Nuestro comité de Jóvenes Profesionales asumió el reto de organizar este evento considerando poner en debate los desafíos y compromisos para los Jóvenes Profesionales de Seguridad.

Se desarrolló un diálogo directo con intercambio de conocimientos y experiencias entre líderes de seguridad y especialistas, se consolidó una amplia convocatoria: sectores público, privado, sociedad civil y fuerzas armadas, reunidas en torno a la gestión de seguridad frente a los cambios generacionales, tecnologías emergentes, procesos de transformación digital y el factor humano en el futuro del profesional de Seguridad.

Toda una jornada dedicada a la innovación, tecnología, neuro seguridad y el impacto en la gestión integrada generando valor en los procesos relevantes de la organización.

Destacable participación del señor Moisés Benamor, Jefe de Instituciones Representativas de la OEA.

Nuestro compromiso, seguir fortaleciendo la Cultura de Seguridad.

¿CÓMO LA NEUROSEGURIDAD Y LA SEGURIDAD POR DISEÑO AFECTA A LA SEGURIDAD PRIVADA?

Tanto la NeuroSeguridad como la Seguridad por Diseño son un cambio de paradigma en el enfoque actual para desarrollar estrategias de defensa contra la intrusión y el uso indebido. Ambas inciden en aumentar el nivel de consciencia de las personas para mejorar la efectividad de la tecnología y lo hacen combinando Conocimiento, Diseño y Tecnología.

La NeuroSeguridad marca la línea estratégica. Se centra en la consciencia de las personas y se apoya en el diseño para conseguir la complicidad del usuario y su uso debido. Evidencia que la usabilidad, entendida como la facilidad para el uso de un sistema, (+ las ganas de usarlo adecuadamente), es aún más determinante que las intrínsecas características técnicas del propio sistema. Trabaja desde el conocimiento y las motivaciones humanas.

La Seguridad por Diseño marca la táctica. Se aplica a todo el proceso del proyecto y no solo al desarrollo o diseño del propio sistema de seguridad. Es sin duda un proceso holístico que reduce costes y entropía de los sistemas. Comienza analizando los retos y conexiones que el proyecto deberá afrontar, considera los fundamentos CPTED, avanza con el diseño de soluciones transversales de defensa en profundidad (profundidad y amplitud) y termina diseñando la capacitación de usuarios y gestores de la solución.

NodumLAPS (Logical Security Advanced Process) combina Conocimiento, Diseño y Tecnología de forma Distribuida, Descentralizada y Transversal.

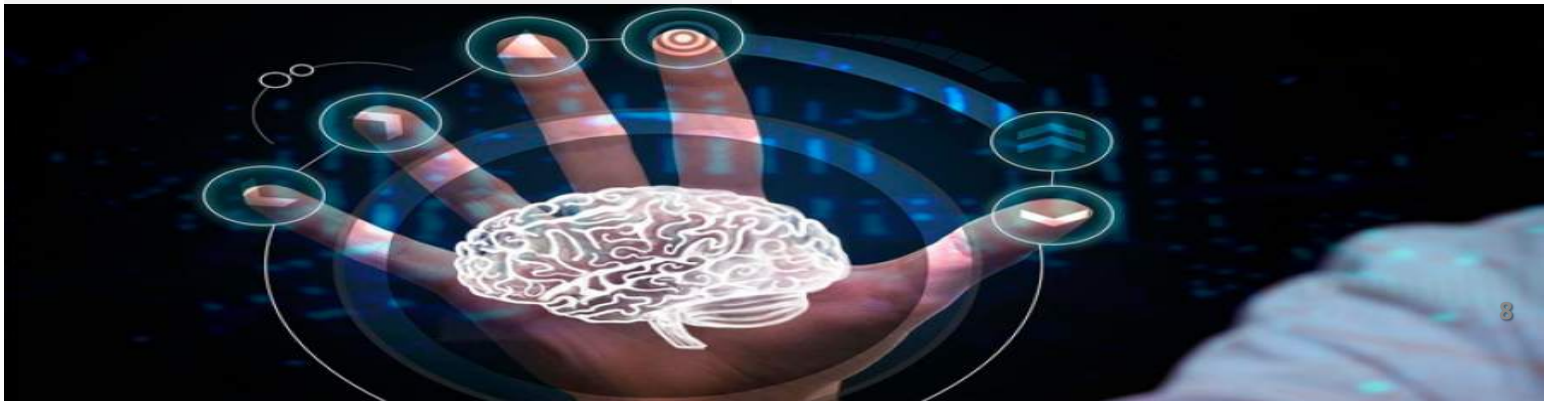
Estas disciplinas comparten fundamentos claramente enfocados a; Personas, Significados y Consecuencias. Diseñan la solución y el proceso, de forma holística y centrados en las personas.

7 claves del nuevo paradigma en seguridad:

- En lugar de trabajar con los sistemas para controlar a las personas, trabaja con las personas para mejorar la efectividad de la tecnología.
- Es un cortafuegos natural contra ciber ataques (negentropía, dosis de descentralización y personas controlando a la tecnología).
- Diseña el proceso del proyecto en lugar de solo el sistema.
- Considera el significado y las consecuencias.
- Protege tanto de la intrusión como del uso indebido.
- Reduce el impacto económico y social del exceso de «cacharros».
- Es vertical (profunda) y transversal (amplia).

La Seguridad por Diseño y la Neuroseguridad se enfocan en Conocimiento y Diseño para aumentar la consciencia y al mismo tiempo, reducir el impacto económico y social que un exceso de tecnología genera sobre las personas.

Ángel Olleros
Security Concept Developer
Consultor de Seguridad en Estrategia e Innovación




Organiza:
asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ
Apoyo Institucional:
ASIS
INTERNATIONAL
LA SEMANA DE LA
GESTIÓN INTEGRAL DE RIESGOS
VI SEMINARIO INTERNACIONAL
PREVENCIÓN
DE FRAUDES
8°Seminario Internacional de
Riesgo Operacional
ROp
01, 02 y 03 de octubre | Hotel Los Delfines


07/08 Noviembre
ASIS 2019
PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS
VIII ENCUENTRO REGIONAL DE SEGURIDAD
HOTEL INTERCONTINENTAL
SANTIAGO DE CHILE


EXPERIENCE
INNOVATION
GSX 2019— an elevated
event experience
Global Security Exchange (GSX), 8-12 September, is the only event that brings together security professionals from all vertical markets throughout the world to network, learn, and re-invest in the industry. It's home for all security practitioners and their partners.

INTELIGENCIA DE AMENAZAS DANDO UN PASO ADELANTE

Las amenazas de ciberseguridad están creciendo y evolucionando rápidamente, es importante para las organizaciones tener mecanismos de alerta temprana para la adecuada protección de sus infraestructuras.

En este contexto surgen la inteligencia de amenazas como un practica imprescindible al momento de definir estrategias de ciberseguridad y de esta forma sustentar operaciones seguras en el ciberespacio.

La inteligencia de amenazas da un valor agregado a las organizaciones dado que les permite reducir notablemente la incertidumbre para la toma de decisiones por ejemplo en los controles a implementar, así como también la identificación de amenazas y oportunidades para enfrentar el riesgo. También es posible producir inteligencia precisa, oportuna y relevante con esta información .

Existen varias plataformas de Inteligencia de amenazas, pero definitivamente no solo se trata de la plataforma sino de una adecuada organización para poder gestionar la información que recibimos de estas plataformas, pero hablemos ahora de las plataformas, si bien hay varias nombraremos algunas de las principales:

ThreatConnect
Es una plataforma que tiene la posibilidad de generar un acceso gratuito en donde podemos recibir alertas e indicadores de compromiso para poder gestionar una adecuada defensa de nuestra infraestructura.

IBM X-Force Exchange
Otra muy robusta plataforma es la de IBM, la conocida X-Force Exchange basada en la nube permite a los usuarios investigar sobre amenazas mas reciente y gestiona la colaboración entre todos sus miembros para el intercambio de información, una característica muy importante aquí es la facilidad de uso de la interfaz de la plataforma.

MISP (Malware Information Sharing Platform)
Quizás el premio a la más cocida y usada actualmente se lo lleva MISP una plataforma de código abierto que permite interconectarse con otras plataformas MISP y lo más interesante es que es permite crear varias organizaciones. De hecho, ahora mismo se está usando en muchos CSIRT a nivel mundial. Una prueba de ello es que los países miembros de alianza del pacifico (Colombia, Chile, México, Perú) y la OEA (Organización de estados americanos) ya se han interconectado a través de esta plataforma logrando un gran avance en materia de colaboración transfronteriza en materia de ciberseguridad.

Otra ventaja que tiene MISP es su fácil integración con otras plataformas como por ejemplo con la plataforma de gestión de incidentes “THEHIVE”, lo que permite rápidamente interconectar la inteligencia de amenazas con la gestión de incidencias, de esta forma colaborativa se puede cerrar el círculo de trabajo de un CISRT o área responsable de gestionar la ciberseguridad.

El reto ahora es organizar el intercambio de información y gestionar taxonomías o clasificaciones estandarizadas en la región para poder llevar un buen registro e estadísticas de las amenazas de ciberseguridad y poder enfrentarlas. Para ello se hace necesario tener consensos regionales y porque no mundiales respecto a la manera de definir y clasificar amenazas, por ello el gran cambio de paradigma será tener por delante la inteligencia de amenazas como herramienta para el diseño de las nuevas estrategias de ciberseguridad.

Ing. Maurice Frayssinet Delgado

Ingeniero de Sistemas e informática con estudios de maestría en ingeniería de sistemas, colegiado con experiencia de 18 años en Auditoria, Seguridad Informática, Seguridad de la Información y gestión de TI, actualmente trabaja en la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros como responsable de la práctica de Gestión de Seguridad de la Información y Continuidad de Negocio.

JUEGOS PANAMERICANOS LIMA 2019

Los Juegos Panamericanos de Lima 2019, oficialmente los XVIII Juegos Panamericanos, se llevaron a cabo entre el 26 de julio y el 11 de agosto de 2019 en Lima. Participaron deportistas de los 41 países de América en 39 deportes.

La ceremonia de inauguración fue un evento que quedará en la memoria de todos los que estuvieron en el Estadio Nacional así como los más de 400 millones de personas que siguieron esta fiesta desde diversas partes del mundo.

Neven Ilic, presidente de Panam Sports, en su discurso por la ceremonia de clausura de Lima 2019 manifestó que los XVIII Juegos Panamericanos son los mejores en la historia.

La delegación peruana se ubicó en un honroso noveno puesto con un total de 39 presea, un récord histórico desde la participación nacional en el evento multideportivo.

JUEGOS PARAPANAMERICANOS LIMA 2019

Los Juegos Parapanamericanos de Lima 2019, oficialmente los VI Juegos Parapanamericanos, son un evento multideportivo internacional que se celebra entre el 23 de agosto y el 1 de septiembre de 2019 en Lima (Perú). Participan deportistas de 33 países de América en 17 deportes. Los juegos sirven de clasificación para los Juegos Paralímpicos de 2020.

El 23 de agosto aplaudimos la determinación de cada Para deportista, en la ceremonia de inauguración de los Juegos Parapanamericanos.

Y este 01 de septiembre será el cierre de los Juegos Parapanamericanos Lima 2019. En medio de un espectáculo liderado por artistas de primer nivel, despediremos la antorcha Parapanamericana de Lima 2019 y agradeceremos por la gran experiencia de vivir los Juegos en la capital peruana.

RESUMEN DE ACTIVIDADES 2019

WEBINAR I

28 DE MAYO DE 2019

WEBINAR II

12 DE JUNIO DE 2019

WEBINAR III

14 DE AGOSTO DE 2019

WEBINAR IV

27 DE AGOSTO DE 2019

WORKSHOP I

23 DE MARZO DE 2019

SEGURIDAD CIUDADANA, CIBERDELINCUENCIA E IDENTIDAD DIGITAL

WORKSHOP II

04 DE MAYO DE 2019

PROTECCIÓN EN GRANDES EVENTOS

WORKSHOP III

17 DE JULIO DE 2019

INTRODUCCIÓN A UN SISTEMA DE GESTIÓN ANTISOBORNO

Consejo Directivo

Percy Quispe Morales
Presidente

Martin Galvez Vizquerra
Vicepresidente

Luis Gonzales Saponara, CPP

Carlos Prado Grados
Tesorero

Consejo Consultivo

Gladys Andrich Muñoz
Past President

Milagros Céspedes Álvarez
Past President & WIS

Aldo Schwarz Cossu, CPP
Past President

Herbert Calderón Alemán, CPP, PCI, PSP
Past President

José Jaramillo Díaz, CPP
Past President

Líderes Voluntarios

Marco Scarpatti del Águila
Líder Voluntario

Nestor Garrido Granda
Líder Voluntario / ARVP región SC

Piero Perales Silva
Líder Voluntario

Andrés Schwarz
Líder Voluntario / Young Professional

Certificaciones ASIS

CPP Certified Protection Professional
Board Certified in Security Management

PCI Professional Certified Investigator
Board Certified, ASIS International

PSP Physical Security Professional
Board Certified, ASIS International

APP Associate Protection Professional
Board Certified In Security Management Fundamentals

ASIS INTERNATIONAL Perú Chapter

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