Newsletter

ASIS INTERNATIONAL Perú Chapter

ASIS Perú

Edición Especial **9/2019**

Editorial

ASIS PERÚ, fue elegido por ASIS International como el ganador a nivel Global del 2019 IB Hale Chapter of the Year Award. La ceremonia de premiación se realizó el 10 de setiembre en el marco del GSX 2019 en Chicago.

También en esta edición resaltamos lo más relevante del GSX y en especial un evento muy significativo para nosotros "La noche Latina". Oficialmente la primera reunión de la Región 7 y 8 de ASIS.

Asimismo, durante este mes continuamos con las actividades de beneficio de nuestros miembros y la comunidad de seguridad. Saludamos la formación de nuevos capítulos de ASIS durante el 2019 y compartimos artículos que abordan temas ciberseguridad, continuidad de negocio, geo prevención e interoperabilidad biométrica.

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

2019 I.B. Hale
Chapter of the Year Award

ASIS Lima, Perú Chapter

ASIS Capítulo 222, Lima - Perú fue elegido por ASIS International como el ganador del 2019 I.B. Hale Chapter of the Year Award. 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.

El premio lo recibimos en una ceremonia en el marco del GSX 2019 desarrolado del 8 al 12 de setiembre en Chicago-IL.

Estamos muy felices y orgullosos, asimismo consideramos que es muy significativo para nuestra región ya que es el primer IB Hale Chapter of the Year Award de Sudamérica.

Este reconocimiento sólo fue posible con planificación, trabajo en equipo y decidido compromiso de nuestros miembros, comités, consejo consultivo, directiva y la comunidad de seguridad en general que siempre nos acompaña.

Nuestro capítulo actualmente tiene activos los comités de Mujeres en Seguridad, Jóvenes Profesionales, Investigaciones, Seguridad Hospitalaria y Ciberseguridad. Asimismo, realizamos diferentes actividades como reuniones, Workshops, Foros, Seminarios, Webinars y disponemos también de diferentes medios de comunicación como correo electrónico institucional, Línea telefónica y WhatsApp, Página web, Facebook, LinkedIn, Blog, Newsletter y un canal de YouTube.

En nuestros eventos se presentan líderes y reconocidos especialistas de la Seguridad. Siendo las actividades más destacadas el último año el I Foro Latinoamericano de Mujeres en Seguridad y el Foro de Jóvenes Profesionales.

Parte importante de nuestro trabajo es la articulación con organizaciones públicas y privadas lo cual nos permite compartir conocimientos, experiencias, buenas prácticas, promover eventos de seguridad y difundir publicaciones.

Nuestro compromiso es continuar trabajando para promover el desarrollo, la profesionalización y el mejoramiento continuo de la seguridad en el Perú.

MARCO NIST DE CIBERSEGURIDAD: UN ABORDAJE INTEGRAL DE LA CIBERSEGURIDAD

Dado un aumento sostenido de la cantidad de incidentes de ciberseguridad en los EEUU, el presidente Barack Obama, el 12 de febrero de 2013, emite la orden ejecutiva 13636 en donde se encarga al Instituto de Nacional de Estándares y Tecnologías (NIST, por sus siglas en inglés) el desarrollo del Marco de ciberseguridad para la protección de infraestructuras críticas, lo que hoy se conoce como el Cybersecurity Framework (CSF). EEUU identifica 16 sectores de infraestructuras críticas, estos son: químico; instalaciones comerciales; comunicaciones; fabricación crítica; presas/represas; base industrial de defensa; servicios de emergencia; energía; servicios financieros; comida y agricultura; instalaciones gubernamentales; salud y salud pública; tecnología de información; reactores nucleares, materiales y residuos; sistemas de transporte; sistemas de agua y aguas residuales.

El Marco fue concebido bajo las premisas de identificar las normas y directrices de seguridad aplicables en todos los sectores de infraestructura crítica, proporcionando un enfoque flexible y repetible, que permite la priorización de actividades y apunta a obtener un buen rendimiento de las infraestructuras, manteniéndose rentable para el negocio.

Es sin dudas una herramienta para la gestión de riesgos de ciberseguridad, que habilita la innovación tecnológica y se ajusta a cualquier tipo de organización (sin importar rubro o tamaño). El Marco tomó como estrategia basarse en estándares de la industria ya aceptados por el ecosistema de ciberseguridad (NIST SP 800-53 Rev.4, ISO/IEC 27001:2013, COBIT 5, CIS CSC, entre otros).

Se presentan como una estrategia de abordaje simple de la gobernanza de la ciberseguridad, permitiendo trasladar fácilmente conceptos técnicos a los objetivos y necesidades del negocio. Su desarrollo fue bajo una metodología participativa, donde todas las partes interesadas (gobierno, industria, academia) pudieron participar y brindar mejoras.

La principal innovación del CSF está dada por dejar de lado estándares rígidos, que era la norma en ese momento; pero no fue el primero en desarrollar una iniciativa para la protección de las infraestructuras críticas. La OTAN ya había desarrollado una serie de manuales orientados hacia la protección de infraestructuras críticas para la defensa nacional, como es el caso del "Manual del Marco de Trabajo de Ciberseguridad Nacional" (National Cyber Security Framework Manual). Esto no quiere decir que el CSF de NIST excluya estos documentos, al contrario, los complementa y mejora.

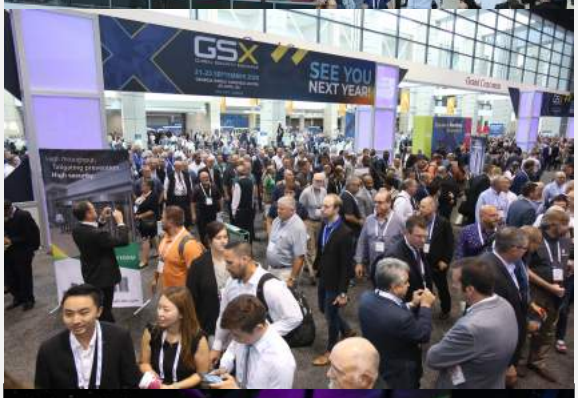
El gran diferencial que ha presentado el CSF respecto a sus antecesores es su simplicidad y flexibilidad; simplicidad para poder transmitir una estrategia técnica en términos que el negocio comprenda y flexibilidad para adecuarse a cualquier organización. Esta diferencia es lo que ha hecho que, a la fecha, la industria y comunidad técnica de todo el mundo haya visto con muy buenos ojos este marco. Empresas, academia y gobiernos han adoptado de manera voluntaria el CSF como parte de su estrategia de ciberseguridad. Incluso organizaciones líderes en la generación de normas y estándares han incorporado el CSF, como por ejemplo ISACA e ISO. En particular, ISO generó la ISO/IEC TR 27103:2018 que proporciona orientación sobre cómo aprovechar los estándares existentes en un marco de ciberseguridad, en otras palabras, cómo utilizar el CSF.

"White Paper desarrollado por la OEA y AWS"
(Texto tomado de la Introducción del White Paper)
https://www.oas.org/MarcoNIST

BELISARIO CONTRERAS

Gerente de Programa de Ciberseguridad
Organización de los Estados Americanos (OEA)
Washington, EEUU

OEA
Más derechos para más gente



GSX establece el estándar para la innovación en seguridad, atrayendo a 20,000 asistentes de todo el mundo

Las puertas se han cerrado en el Global Security Exchange (GSX) de este año, celebrado en el McCormick Place de Chicago. Presentado por ASIS International, la asociación más grande del mundo para profesionales de gestión de seguridad, el evento ofreció seis días llenos de educación y redes para la comunidad de seguridad global. La asistencia fue fuerte con 20,000 inscriptos de más de 125 países y más de 550 expositores llenando el centro de convenciones. Los profesionales de seguridad también participaron en sesiones en todo el mundo a través de Global Access LIVE! streaming: con participantes en más de 15 países.

"GSX sirve como un poderoso foro para convocar a líderes de seguridad en todo el mundo para aprender, compartir información y redes", dijo Christina Duffey, CPP, Presidenta de ASIS 2019. "Dejo el GSX de este año con más energía sobre nuestra asociación, nuestra profesión y nuestra industria. Estoy eternamente agradecida con nuestro Capítulo de Chicago y el comité anfitrión por su fuerte apoyo y espero con ansias el GSX 2020, que tendrá lugar en Atlanta ".

GSX 2019 se lanzó el sábado 7 de septiembre, con revisiones de certificación y talleres de educación continua. El domingo 8 los asistentes pudieron participar de un foro de discusión abierto, en el cual participaron líderes voluntarios de ASIS. El lunes 9 de septiembre, el discurso de apertura fue pronunciado por el experto en geopolítica y autor Ian Bremmer, Ph.D., cubriendo los riesgos, tendencias y economía más apremiantes en todo el mundo. El GSX Exhibit Hall abrió el martes 10 de septiembre con más de 550 expositores y áreas de funciones innovadoras que incluyen el GSX Disruption District, las etapas de X-Learning y el D3 (Drones, Droids, Defense) Learning Theater, y nuevo este año, el Startup Sector pabellón, destacando nuevas innovaciones en la profesión de seguridad. El orador de la sesión general del martes, Steve Demetriou, presidente y director ejecutivo, Jacobs, habló sobre los tiempos cambiantes. John F.Kelly, general retirado de cuatro estrellas, exsecretario de Seguridad Nacional de Estados Unidos y jefe de gabinete de la Casa Blanca, inició el Día de Apreciación Militar y de las Fuerzas del Orden el miércoles 11 de septiembre. El general Kelly también se refirió a los cambios en las estructuras y políticas de las agencias del Departamento de Seguridad Nacional (DHS) desde el 11 de septiembre y describió cómo el aumento dramático de la colaboración entre las agencias de inteligencia y cumplimiento en los últimos años ha hecho que el país sea mucho más seguro.

Nuevo en GSX este año y el primero en la industria de la seguridad, 12 compañías fueron seleccionadas para competir en la primera competencia GSX Pitch.

La sesión general de clausura contó con Tarah Wheeler, investigadora de políticas de seguridad cibernética en New America.

Tomado de www.asisonline.org

GSX punto de encuentro de Latinos

La Noche Latina, fraternal reunión, muy significativa y que oficialmente por primera vez convocó a los Capítulos de ASIS Latinos de la Región 7 y 8 y a socios afiliados de ASIS International, se realizó el 9 de setiembre en el Punch Bowl Social Chicago.

El 10 de setiembre ASIS PERÚ fue galardonado con el 2019 IB Hale Chapter of the Year Award. Cabe resaltar también el premio IB Hale para ASIS Capítulo 217 - México y los premios por Newsletter y Página Web de ASIS Capítulo 215 – Buenos Aires. Demostración clara del aporte de los Latinoamericanos a la Seguridad Global.

Destacamos también la nominación de los 14 nuevos miembros para el Global Board de ASIS INTERNATIONAL. Los latinos estamos muy felices porque ya contábamos con un destacado profesional de la Seguridad Latino, Jaime Owens, CPP de Panamá actual Board Director. Ahora se suma al equipo de Directores Globales nuestro actual Vicepresidente Regional Senior (Región 8), Pablo Colombres, CPP, quien a su vez se convierte en el profesional más joven en la historia de ASIS International en formar parte de este selecto grupo de profesionales. Felicitaciones Pablo!!

LA TÉCNICA REID DE ENTREVISTA E INTERROGATORIO

18 DE SETIEMBRE DE 2019
HORA: 16:00 pm

Expositor
Sr. Rodrigo Velarde Santos, CPP CRT DSE

WEBINAR V

Detección de la mentira y la obtención de la verdad.
¿POR QUÉ MIENTE LA GENTE?

Para evitar una consecuencia: castigo, regaño, perder trabajo, ir a la cárcel, pérdida de imagen personal.
¿POR QUÉ CONFIESA LA GENTE?

Porque se les convence de que las cosas van a mejorar si lo hacen.

LA SEGURIDAD EN EL RETAIL

Comité de Investigaciones

WEBINAR VI

25 DE SETIEMBRE DE 2019
HORA: 16:00 pm

Expositor
Ing. José Jaramillo, CPP

GEO PREVENCIÓN

Desarrollar ciudades seguras, conlleva el aplicar diversas estrategias y llevar a cabo acciones de fondo y forma. Dentro de ellas, el diseño urbano representa un aspecto fundamental que merece un estudio profundo para evaluar sus condiciones y proponer, con un enfoque de "geo prevención", ofrecerle a las comunidades una mejor calidad de vida.

Una estrategia útil y efectiva para prevenir el crimen y la sensación de inseguridad, la constituye la "prevención del crimen a través del diseño ambiental", conocida por sus siglas en inglés como CPTED, (Crime Prevention Through Environmental Design), la cual plantea la modificación de elementos del contexto municipal para inhibir la comisión de actos delictivos, a través de prácticas disuasivas y de rediseño de espacios públicos.

La CPTED se basa en vulnerabilidades y se fundamenta en el principio de oportunidad a cometer un delito. Propone 5 conceptos, interrelacionados, destinados a reducir las oportunidades para la comisión de delitos, así como el miedo ante la inseguridad:

- **Control natural de accesos.**
  Al apropiarse los miembros de la comunidad, de los accesos del espacio, ya sea por su uso o señalización.

- **Vigilancia natural.**
  Basada en la visibilidad de un espacio, es decir, que una persona sienta confianza, que pueda ver y ser vista. Este tipo de vigilancia permite observar y modificar comportamientos inadecuados, reportándolos a la policía o a los vecinos de la comunidad. Ello conforma, asimismo, un factor disuasivo para cualquier delincuente de operar en el lugar.

- **Refuerzo del territorio.**
  Al darse una relación afectiva entre las personas y su entorno inmediato, generándole un sentido de identidad y pertenencia al mismo, provocando que cuide dicho espacio. En áreas inseguras, se logra promoviendo y realizando actividades seguras en el lugar de carácter recreativo o deportivo, reduciendo así la oportunidad de consumo de alcohol y drogas.

- **Mantenimiento de los espacios públicos.**
  Al ocuparse de mantener el espacio en condiciones apropiadas para el uso y disfrute de los vecinos, ya que de prevalecer el descuido y deterioro, existe una mayor oportunidad para los delincuentes de actuar en el lugar.

- **Participación comunitaria.**
  Se debe lograr el involucramiento de los miembros de la comunidad en todas las etapas de la estrategia, con el fin de reducir o erradicar la comisión de delitos y revertir la percepción de inseguridad en el lugar.

Si bien para la realización de esta estrategia se debe contar idealmente con el apoyo de las autoridades, la ciudadanía juega un papel determinante al ser el protagonista principal de las acciones a realizarse en la comunidad.

Al recuperar y ocupar los espacios perdidos, estaremos recuperando nuestra seguridad y generando los espacios para el correcto desarrollo de nuestros hijos.

Para que profundices en el tema y pongas en práctica las recomendaciones de la CPTED, ponemos a tu disposición el documento: Espacios urbanos seguros, recomendaciones de diseño y gestión comunitaria para la obtención de espacios urbanos seguros, que muestra un modelo aplicado exitosamente en Chile, país que ha logrado implementar con eficacia ésta estrategia

DAVID LEE
Presidente en GRUPO PALADIN
Naucalpan de Juárez y alrededores, México
Recaudación de fondos.

Autor del Manual para la Prevención de Delitos y Director Nacional de la Campaña de Seguridad "Por un Futuro más Seguro". Imparte la Conferencia Magistral "Aprendiendo a Vivir Seguros".


XIV
Congreso anual
ASIS International
Capítulo México Occidental 247
ASIS
INTERNATIONAL
CAPITULO MÉXICO OCCIDENTE 247
Del 2 al 4 de Octubre 2019
Hotel Riu Plaza
Gadalajara
contacto@asisoccidente.com.mx
informacion@asisoccidente.com.mx
presidencia@asisoccidente.com.mx


SECURITY WEEK
LATAM ASIS 2019
ASIS
INTERNATIONAL
CAPÍTULO MÉXICO 217
Security Week LATAM ASIS 2019
Del 13 al 17 de Octubre 2019
HORA: 08:00 am
LUGAR: Centro Citibanamex
Ciudad de México
SECURITY WE


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

PORQUÉ SE DEBE IMPLEMENTAR EL PLAN DE CONTINUIDAD DE NEGOCIO (PCN) EN SU INSTITUCIÓN.

Las empresas desarrollan e implementan soluciones que involucran procesos operativos asociados con la fabricación de productos o prestación de servicios, a fin de reducir la probabilidad de ocurrencia de incidentes que afecten sus procesos o que interrumpan el normal desarrollo de sus actividades; también sabemos que existe un número limitado de situaciones que no pueden ser evitadas por lo que un incidente de seguridad podría ocurrir. Por esta razón, las empresas establecen medidas para que se continúen prestando sus servicios a pesar de que se registre un incidente y lo más importante, que la recuperación al estado normal de operación, se realice en el menor tiempo posible.

El riesgo por fallas eléctricas en una empresa resulta ser un factor común de incendios debido a cortos circuitos, esto debido a una deficiente instalación de técnicos inexpertos o no calificados, un cálculo errado de las cargas eléctricas, un error en la segmentación eléctrica por zonas, por no acatar las normas de seguridad establecidas, o el uso de materiales de baja calidad, empleados casi siempre tomando como referencia un mal entendido “ahorro en los costos” o también referenciado como “un logro de la eficiencia en los costes”.

Algunas cifras estadísticas nos indican que las fallas eléctricas causan el 90% de los incendios, que el 43% de las empresas que no cuenta con un Plan de continuidad de negocio no se recuperan luego de ocurrido un incidente de seguridad, el 51% logra sobrevivir pero tarda 2 años en reinsertarse en el mercado y el 6% mantiene su negocio a largo plazo. Otros datos de interés nos indican que el 30% de las copias de seguridad y el 50% de las restauraciones fallan cuando se requiere su restablecimiento; muchos responsables de los departamentos de seguridad de información no se encuentran convencidos de ser capaces de recuperar los datos luego de un incidente.

Para atender situaciones como la comentada debemos disponer de un PCN, como respuesta a las condiciones de riesgo que se pueden presentar, no importa el tamaño de la empresa o el costo de las medidas de seguridad implementadas ya que tarde o temprano nos tendremos que enfrentar a un incidente de seguridad. En líneas generales podemos decir que el objetivo de un PCN es el de impedir que se interrumpan las actividades de una empresa y si no puede evitarse, lograr que el tiempo de recuperación sea el menor posible.

Un aspecto importante en la elaboración del PCN es la definición de situaciones críticas y la conformación de un Comité interno de continuidad de negocio, donde se defina claramente los roles y escalamiento necesarios para atender la crisis. También es importante priorizar los procesos y procedimientos asociados a los servicios que necesitamos restablecer, teniendo en cuenta que se registren todos los eventos e incidentes, para formar la base de conocimiento e indicadores de Gestión.

El PCN debe encontrarse actualizado y conocido por el personal involucrado en los procesos necesarios para reactivar un servicio (en especial aquellos que resultan críticos); todo ello debe ser realizado con la oportunidad debida y antes de que ocurra un incidente, siendo el objetivo principal, el de mantener el nivel de servicio acordado con los clientes. Recordemos que no es necesario que todos los procesos se activen en forma simultánea, por ello es importante conocer el flujo de procesos, la secuencia de reinicio, y las lecciones aprendidas.

En líneas generales, el PCN debe considerar: La definición o alcance priorizando los procesos que resulten críticos para el negocio, el análisis del impacto y los riesgos identificados, con indicaciones claras de cómo accionar para alcanzar el pronto restablecimiento de los servicios, la selección de la estrategia nos ayudará a tomar decisiones al momento de resolver la crisis ya que estaremos tan ocupados en atenderla, que será de mucha ayuda contar con los procesos previamente definidos, el desarrollo de los planes a desplegar y los procedimientos a utilizar, incluyendo pruebas de continuidad para garantizar que funcione cuando sea requerido.

Como vemos, el PCN requiere de un conocimiento profundo de los procesos involucrados en el desarrollo de los productos o servicios; igualmente requiere del compromiso de los funcionarios que participan en él, pero, sobre todo, se requiere de la participación y apoyo de la alta dirección de la empresa, ya que sin este entendimiento no se podrán implementar las medidas de control o mitigación, los sistemas y la seguridad necesaria para que, cuando se presente un incidente, se pueda activar el PCN y se pueda resolver la crisis con prontitud.

Iniciamos esta nota comparando el PCN como documento y continuamos analizando el PCN como una cultura de continuidad organizacional; concluimos ahora señalando que una empresa que motiva a su personal a practicar el PCN y que incorpora dichas actividades como un elemento natural en el desarrollo de sus procesos, alcanzó su estado de madurez, este estado le da mayores probabilidades de continuar operando con normalidad, luego de un incidente de crisis, especialmente a aquellas que hacen un uso intensivo de la tecnologías de información. No es necesario que tengamos que desarrollar un PCN para cumplir con alguna norma de carácter obligatorio o exigencia de parte de nuestros clientes, debemos hacerlo por propia convicción.

Finalmente concluyo estas líneas resaltando que ningún PCN resultará exitoso si es que no cuenta con: el compromiso de la alta dirección, el involucramiento del personal y los recursos necesarios para atender un incidente.

Giovanni Bautista Pichling Zolezzi

Gerente de Operaciones en ASBANC
Asociación de Bancos del Perú

LA SEMANA DE LA GESTIÓN INTEGRAL DE RIESGOS

1, 2 Y 3 DE OCTUBRE 2019

VI SEMINARIO INTERNACIONAL
PREVENCIÓN DE FRAUDES
01 Y 02 DE OCTUBRE | HOTEL LOS DELFINES

ROp Perú 2019
8°Seminario Internacional de Riesgo Operacional
02 y 03 de octubre I Hotel Los Delfines

Temas a tartar:

- Situación actual del fraude y el cibercrimen.
- Análisis del fraudador en nuestra Sociedad.
- Fraudes en operaciones creditcicias.
- Regulación de Ciberseguridad.
- Ciberseguridad y Reputación financiera.
- Riesgo Operacional en la nuevas iniciativas y cambios significativos.
- Modelo integrado de control interno.
- Gestión integral de riesgos en las Cooperativas.

Organiza:

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Apoyo Institucional:

ASIS INTERNATIONAL
Perú Chapter

Lugar:

DELFINES HOTEL & CONVENTION CENTER

Los Eucaliptos 555
San Isidro - Lima – Perú

Algunos expositores:


Carlos Ramires


Orlando Gracés


Adriana Umeda


Raúl Rivera


Oscar Basso

Para mas Información:

Inscripciones:
eventos@asbanc.com.pe
612-3333

Auspicios:
drojo@asbanc.com.pe
612-3333 anexo 3585

INTEROPERABILIDAD BIOMÉTRICA, UNA ESTRATEGIA TECNOLÓGICA PARA EL DESARROLLO SOSTENIBLE

Es importante tener presente las consideraciones al momento de construir plataformas de interoperabilidad tecnológica el cual permiten la validación en procesos digitales realizadas por diferentes organizaciones que mantienen relación afín. La construcción de plataformas en diferentes entornos genera dificultad al poder integrarlos con soluciones de cada organización; en el caso particular corresponde mencionar el uso de la biometría en procesos de validación e identificación de la identidad de las personas considerando que existen alcances definidos al momento de realizar consultas; existen parámetros estandarizados para una consulta y que estos estén debidamente optimizados permiten tener un adecuado nivel en tiempos de respuesta que garanticen en el lado del usuario final una oportuna atención.

La necesidad de establecer lineamientos y alcances en torno a servicios web, criterios de aceptación y rechazo, tiempos de respuesta, conectividad redundante en caso de enlaces físicos, así como infraestructura redundante en el lado del proveedor son de necesidad si estas plataformas atienden a nivel nacional y son críticos para la atención directa en los ciudadanos y su no operatividad genera serios problemas a usuarios finales. ¿Cómo establecer criterios de medición del nivel de la interoperabilidad?, ¿cómo garantizamos la atención oportuna a los usuarios respecto de una petición biométrica? La existencia de normas y estándares permiten una valida petición biométrica de tal forma se gestione en forma debida las consultas a la plataforma biométrica. La construcción de arquitecturas que soporten peticiones biométricas a nivel nacional demanda capacidades de las organizaciones en tecnología biométrica, así como infraestructuras redundantes en todos los niveles de la plataforma. Es necesario entonces la existencia de protocolos para atender la gestión de la plataforma de interoperabilidad de tal forma garantizar su adecuado uso.

Es claro entonces que tener una plataforma biométrica debidamente implementada permite a las organizaciones tener una interacción mucho más confiable y dinámica facilitando que las otras tecnologías complementarias puedan interactuar y atender los procesos digitales que existe en cada organización. Si las sumas de estas relaciones digitales mantienen continuidad en el tiempo podemos tener entonces dinámicas que interactúan entre sí.

Considerando que en un proceso de consulta las peticiones son de huellas dactilares, imágenes faciales, archivos de voz y otras biometrías complementarias podemos entender entonces que las diferentes soluciones existentes pueden validar la identidad de una persona. Sumando a ello otras características relacionadas de la persona podemos entonces establecer una información completa de todo ciudadano en su quehacer diario con respecto a los diferentes servicios digitales en el cual es atendido.

Las plataformas digitales de interoperabilidad permiten que exista una relación sostenible de información, permitiendo que unos conjuntos de indicadores sean de educación, seguridad, salud, licencia de conducir, sistema financiero, información legal, penal, policial y otros puedan estar disponibles para la toma decisiones oportuna en el momento adecuado.

El estado con dicha información puede elaborar políticas de alcance nacional y orientar debidamente su accionar en las necesidades reales de una región determinada o de un grupo etario correspondiente. Es evidente que plataformas tecnológicas como la presente agilizan las soluciones digitales que interactúan con ella, ordenando de esta manera a la sociedad en su conjunto y permitiendo que diferentes soluciones digitales brinden un adecuado servicio al ciudadano.

La integración de diferentes factores en torno a plataformas como la presente proteja en los derechos a cada persona desde que nace permitiendo tener una sola identidad en diferentes escenarios en el cual se desenvuelve. La identidad digital garantizada a través de diferentes plataformas permite a cada persona autenticarse en medios digitales con una identidad propia a través de la infraestructura de PKI que se dispone dentro de la organización.

RENIEC como organización cumple con el encargo que el Estado le brinda en otorgar confianza y seguridad de la identidad de una persona para que se pueda desenvolver en todos los escenarios sean virtuales o no facilitándole un conjunto de servicios que se encuentra su disposición.

Felix Eloy Jiménez Chuque

Sub Gerente de Operaciones Telemáticas
Registro Nacional de Identificación y Estado Civil (RENIEC)

NUEVOS CAPÍTULOS ASIS 2019

El 29 de marzo de 2019 se realizó en La Paz la ceremonia de inauguración oficial de ASIS Capítulo 306 en Bolivia, en el marco de la Jornada Internacional de ASIS Bolivia 2019

Representación de ASIS International

- **Pablo Colombres, CPP**
- SRVP (Senior Regional Vice President) del Grupo 8 en Sud America que incluye: Argentina, Bolivia, Brazil, Chile, Colombia, Ecuador, Paraguay, Peru, Uruguay and Venezuela.
- **Carlos R. Flores, CPP (Uruguay)**
  RVP (Regional Vice President) Grupo 8C – ASIS International
- **Juan Carlos Medina (Bolivia)**
  Presidente ASIS BOLIVIA
- **Herbert CALDERON, CPP, PCI, PSP, CSMP®M.ISMI,CFE (Perú)**
  Past President ASIS PERÚ
- **Percy Quispe, MBA, CIP (Perú)**
  Presidente ASIS PERÚ
- **Osmar Florenciañez (Paraguay)**
  ARVP – Grupo 8C – ASIS International
- **Humberto Santibañez, CPP (Chile)**
  PCB (Professional Certification Board) – ASIS International

AGOSTO 2019

Capítulo 310 GUAYAQUIL, ECUADOR
Presidente:
Sra. Jhenny M Andrade, CPP

Guayaquil, ciudad portuaria de Ecuador, es una puerta de entrada a las playas del Pacífico y a las Islas Galápagos

SETIEMBRE 2019

Capítulo 311 PENÍNSULA YUCATÁN, MÉXICO
Presidente:
Sr. Carlos Contrera

Yucatán es una de las treinta y dos entidades federativas que integran los Estados Unidos Mexicanos. Su capital y ciudad más poblada es Mérida

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 / ASVP 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