

Perú Edición 02/2023

Editorial

La continuidad de negocio es esencial para garantizar la resiliencia y supervivencia de las corporaciones en tiempos de adversidad. Ante desafíos como desastres naturales, ciberataques y crisis económicas, contar con estrategias bien definidas y planes de contingencia permite minimizar interrupciones, mitigar riesgos y mantener la competitividad. La anticipación, la respuesta efectiva y la capacidad de adaptación son fundamentales para superar obstáculos y garantizar la sostenibilidad a largo plazo. La continuidad de negocio debe ser una prioridad en todas las organizaciones para enfrentar los desafíos cambiantes del entorno empresarial.

Maurice Frayssinet Delgado
Presidente ASIS Perú



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 públicos 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"

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.

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

"Juntos somos más fuertes"

COMUNIDAD WIS (WOMEN IN SECURITY)

Fortaleciendo la Primera Línea de Defensa en ciberseguridad con la Capacitación y Concientización

QR



Anita Guerra Tasaico

Ingeniera en Administración de Empresas, Especialista en Gestión de Talento Humano y Comunicación, MBA en Administración de Negocios, Master europeo en Dirección de Empresas. Especialización: Calidad total en la Gestión Administrativa; Administración y Gestión Pública. Miembro del Colegio de Ingenieros del Perú; Miembro de ASIS International Comunidad Global de Profesionales de la Seguridad. Actualmente responsable del Centro de Comunicaciones y Educación Digital del Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros.

En el panorama actual de amenazas cibernéticas en constante evolución, la capacitación y la concientización en ciberseguridad se han convertido en elementos fundamentales para proteger a las organizaciones de ataques maliciosos. En este artículo, exploraremos la importancia de la capacitación y la concientización en ciberseguridad, analizaremos los beneficios que aportan a las empresas y brindaremos consejos prácticos sobre cómo implementar programas efectivos de capacitación y concientización en la era digital.

La capacitación en ciberseguridad es esencial para dotar a los empleados de los conocimientos y habilidades necesarios para reconocer y responder a las amenazas cibernéticas. Una fuerza laboral capacitada es la primera línea de defensa de una organización contra los ataques. La capacitación adecuada no solo ayuda a prevenir incidentes de seguridad, sino que también permite una respuesta rápida y eficiente en caso de que ocurra un incidente. Además, la capacitación en ciberseguridad promueve una cultura de seguridad en toda la organización, fomentando prácticas seguras en línea y conciencia de los riesgos asociados con la manipulación de datos, el phishing, la ingeniería social y otras tácticas utilizadas por los ciberdelincuentes.



COMUNIDAD WIS (WOMEN IN SECURITY)

Fortaleciendo la Primera Línea de Defensa en ciberseguridad con la Capacitación y Concientización

De otro lado la concientización en ciberseguridad implica educar a los empleados sobre los riesgos cibernéticos, las mejores prácticas de seguridad y las políticas y procedimientos internos de la organización. Algunos de los beneficios clave de la concientización en ciberseguridad incluyen:

- **Identificación temprana de amenazas:** La concientización ayuda a los empleados a reconocer las señales de advertencia de ataques cibernéticos, como correos electrónicos de phishing o sitios web fraudulentos. Esto permite una detección temprana y una respuesta rápida para evitar incidentes mayores.
- **Reducción de errores humanos:** Los errores humanos son una de las principales causas de brechas de seguridad. La concientización en ciberseguridad ayuda a los empleados a comprender los riesgos asociados con ciertas acciones en línea y a adoptar prácticas seguras para reducir la posibilidad de cometer errores que puedan comprometer la seguridad de la organización.
- **Protección de la reputación y la confianza:** Una brecha de seguridad puede tener un impacto significativo en la reputación y la confianza de una organización. La concientización en ciberseguridad ayuda a mitigar este riesgo al promover una cultura de seguridad sólida y demostrar el compromiso de la organización para proteger la información confidencial de sus clientes y socios comerciales.

Diseño de un programa de capacitación y concientización en ciberseguridad

Para implementar un programa efectivo de capacitación y concientización en ciberseguridad, se deben seguir algunos pasos clave:

- **Evaluación de necesidades:** Realizar una evaluación exhaustiva de las necesidades de capacitación y concientización en ciberseguridad de la organización. Esto puede incluir identificar áreas de riesgo, evaluar el nivel de conocimiento actual de los empleados y determinar las metas y objetivos del programa.
- **Desarrollo de contenido:** Crear contenido de capacitación y concientización relevante y personalizado es fundamental. Esto puede incluir módulos de aprendizaje en línea, tutoriales interactivos, estudios de casos y simulaciones de ataques. Es importante adaptar el contenido a diferentes roles y niveles de experiencia dentro de la organización.
- **Comunicación efectiva:** Establecer una comunicación clara y constante sobre la importancia de la ciberseguridad es esencial. Esto puede incluir correos electrónicos, boletines informativos, carteles y reuniones regulares para discutir temas de seguridad. Es fundamental que los empleados entiendan la relevancia de la capacitación y la concientización en su trabajo diario.
- **Participación activa:** Fomentar la participación activa de los empleados en el programa es crucial. Esto puede lograrse a través de actividades interactivas, como cuestionarios, juegos de roles y ejercicios prácticos. También es importante proporcionar retroalimentación y recompensas para fomentar la participación y el compromiso.

COMUNIDAD WIS (WOMEN IN SECURITY)

Fortaleciendo la Primera Línea de Defensa en ciberseguridad con la Capacitación y Concientización



- **Evaluación y seguimiento:** Realizar evaluaciones periódicas para medir el impacto del programa de capacitación y concientización es esencial. Esto puede incluir pruebas de conocimientos, encuestas de satisfacción y análisis de métricas de seguridad, como la disminución de incidentes de phishing o la mejora en la identificación de amenazas.
- **Actualización continua:** La ciberseguridad es un campo en constante evolución, por lo que es importante mantener el programa actualizado. Revisar y actualizar el contenido regularmente para abordar nuevas amenazas y tendencias de seguridad asegurará la relevancia y la eficacia del programa a largo plazo.

Conclusiones

La capacitación y la concientización en ciberseguridad son elementos fundamentales para fortalecer la seguridad de una organización. Al implementar programas efectivos, las empresas pueden empoderar a sus empleados para ser conscientes de los riesgos y tomar medidas proactivas para proteger la información confidencial y preservar la seguridad en la era digital.

COMUNIDAD WIS (WOMEN IN SECURITY)

Seguridad en dispositivos IoT, explorando los posibles riesgos y soluciones

QR



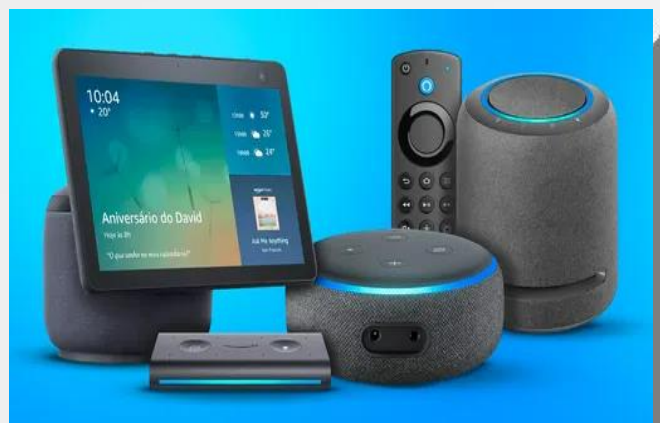
Flor Meza Silvestre

Ingeniera de Sistemas e informática, con estudios de Maestría en Administración Estratégica, cursando la maestría en Inteligencia Artificial. Con especialización en Ciberseguridad y Ciberdefensa, Ethical Hacking, Linux, Cloud Computing, Gestión de incidentes de ciberseguridad. Miembro del Colegio de Ingenieros del Perú; Miembro de ASIS Internacional Comunidad Global de Profesionales de la Seguridad. Experiencia en Infraestructura de Security Operations Center. Actualmente se encuentra en el área de Equipo de Respuestas ante Incidentes de Seguridad Digital (CSIRT) del Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros.

La creciente popularidad de los dispositivos de Internet de las cosas (IoT, por sus siglas en inglés) ha llevado a un mundo cada vez más interconectado. Estos dispositivos, que abarcan desde electrodomésticos inteligentes hasta sistemas industriales avanzados, ofrecen comodidad y eficiencia en nuestras vidas diarias. Sin embargo, también plantean importantes desafíos en términos de seguridad. En este artículo, exploraremos los posibles riesgos asociados con los dispositivos IoT y analizaremos algunas soluciones para garantizar una mayor seguridad en este entorno.

Los dispositivos IoT suelen utilizar software y firmware personalizado para su funcionamiento, estos componentes pueden contener vulnerabilidades que los hackers pueden aprovechar para acceder a los dispositivos y comprometer su seguridad. La falta de actualizaciones regulares del software y la falta de enfoque en la seguridad por parte de los fabricantes pueden exponer a los dispositivos a ataques. Muchos dispositivos IoT tienen contraseñas predeterminadas débiles o incluso carecen de autenticación adecuada. Esto facilita a los hackers el acceso no autorizado a los dispositivos y les permite controlarlos o utilizarlos como puerta de entrada a la red más amplia.

Algunos dispositivos IoT carecen de mecanismos adecuados para proteger la comunicación entre ellos y otros dispositivos o redes. Esto puede permitir a los atacantes interceptar y manipular los datos transmitidos, lo que puede tener implicaciones graves, especialmente en aplicaciones críticas como la atención médica o la infraestructura inteligente. También encontramos que a menudo los dispositivos IoT recopilan y transmiten una gran cantidad de datos sensibles. Si estos datos no se protegen de manera adecuada, pueden ser accesibles para personas no autorizadas, lo que puede resultar en violaciones de la privacidad y el robo de información confidencial.



COMUNIDAD WIS (WOMEN IN SECURITY)

Seguridad en dispositivos IoT, explorando los posibles riesgos y soluciones

Soluciones para mejorar la seguridad en dispositivos IoT

Los fabricantes deben proporcionar actualizaciones periódicas de software y firmware para abordar las vulnerabilidades conocidas y garantizar la seguridad continua de los dispositivos IoT. Esto debe incluir mecanismos sencillos de actualización para los usuarios. Es esencial que los dispositivos IoT implementen métodos sólidos de autenticación, como el uso de contraseñas robustas y únicas, así como la autenticación de dos factores. Además, las contraseñas predeterminadas deben eliminarse o requerir un cambio obligatorio durante la configuración inicial.

Los dispositivos IoT deben utilizar protocolos de comunicación seguros, como el cifrado de extremo a extremo, para garantizar la integridad y la confidencialidad de los datos transmitidos, esto evita que los atacantes intercepten y manipulen la información sensible, también se deben implementar medidas de protección de datos sólidas, como el almacenamiento seguro y el cifrado de los datos recopilados por los dispositivos IoT. Esto incluye garantizar que los datos se almacenen de manera segura y que solo se compartan con los servicios y aplicaciones autorizados.

Por otro lado, se deben realizar pruebas de seguridad exhaustivas en sus dispositivos IoT para identificar posibles vulnerabilidades y riesgos. Esto puede incluir pruebas de penetración, análisis de código y auditorías de seguridad. Además, es importante realizar evaluaciones de riesgos periódicas para adaptarse a las nuevas amenazas y asegurar la protección continua de los dispositivos.

Por último, los usuarios de dispositivos IoT también desempeñan un papel crucial en la seguridad, por esta razón es esencial proporcionar una educación adecuada sobre las mejores prácticas de seguridad, como la configuración de contraseñas fuertes, la actualización regular de software y la identificación de posibles amenazas. Los usuarios deben ser conscientes de los riesgos asociados con los dispositivos IoT y estar informados sobre cómo proteger su privacidad y seguridad.



Conclusiones

A medida que la adopción de dispositivos IoT continúa creciendo, es fundamental abordar los desafíos de seguridad que plantean. Los riesgos asociados con los dispositivos IoT pueden tener graves implicaciones en términos de privacidad, seguridad personal y seguridad de la infraestructura. Sin embargo, mediante la implementación de soluciones como actualizaciones de software regulares, autenticación segura, comunicación cifrada y protección de datos, podemos mitigar estos riesgos y garantizar un entorno de IoT más seguro. Además, la educación y concientización de los usuarios son fundamentales para promover prácticas seguras y una mayor seguridad en el mundo de los dispositivos IoT.

ARTÍCULO DE COLABORACIÓN

Gestión de Continuidad de Negocio: Garantizando la Resiliencia Empresarial con la Norma ISO 22301

QR



Shirley Castillo Boulanger

Ingeniera de Sistemas, con estudios culminados de Maestría en Gestión Pública, con más de 20 años de experiencia, de los cuales 14 años en Auditoría Informática & de Sistemas, Seguridad de la Información, Gestión de la Información, con estudios en Directrices de Ciberseguridad ISO 27032, Big Data y Business Analytics, Transformation Digital, Certified Ethical Hacker V10, Implementador Líder ISO 27001 Seguridad de la Información, Auditoría basada en Riesgos, Diseño de Data Centers, CISSP: Certified Information Systems Security Professional, con Certificación en SAP-FI entre otros. Ha laborado en la SUNARP y en la SUNAT en el Órgano de Control Institucional. Actualmente Coordinadora Nacional de Seguridad de la Información del Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros.

En un mundo cada vez más volátil y lleno de incertidumbre, la capacidad de una organización para mantener la continuidad de sus operaciones es vital. La norma ISO 22301 se ha convertido en un referente global para la gestión de la continuidad de negocio, proporcionando un marco sólido para ayudar a las organizaciones a prepararse, responder y recuperarse de eventos disruptivos. En este artículo, exploraremos los fundamentos de la gestión de la continuidad de negocio basada en la norma ISO 22301, analizaremos sus beneficios y ofreceremos consejos prácticos para su implementación efectiva.

¿Qué es la norma ISO 22301?

La norma ISO 22301, titulada "Sistemas de Gestión de la Continuidad de Negocio: Requisitos", establece los criterios para desarrollar, implementar, mantener y mejorar un sistema de gestión de la continuidad de negocio. Proporciona una estructura para ayudar a las organizaciones a identificar y gestionar las amenazas, mantener las operaciones durante situaciones de crisis y garantizar una rápida recuperación y retorno a la normalidad después de un incidente. La norma ISO 22301 se basa en un enfoque de ciclo de vida, que abarca desde la planificación y el establecimiento de políticas hasta la implementación, el monitoreo y la mejora continua.



ARTÍCULO DE COLABORACIÓN

Gestión de Continuidad de Negocio: Garantizando la Resiliencia Empresarial con la Norma ISO 22301

Beneficios de la gestión de continuidad de negocio basada en la ISO 22301

Resiliencia empresarial: La norma ISO 22301 ayuda a las organizaciones a fortalecer su capacidad para resistir y recuperarse de interrupciones significativas, minimizando así el impacto en las operaciones y la reputación.

Cumplimiento regulatorio: Al cumplir con los requisitos de la norma ISO 22301, las organizaciones pueden demostrar su cumplimiento con las regulaciones y normativas relacionadas con la continuidad de negocio.

Gestión de riesgos mejorada: La norma ISO 22301 ayuda a las organizaciones a identificar y evaluar los riesgos potenciales para la continuidad de negocio, lo que permite una gestión más efectiva de dichos riesgos y una toma de decisiones informada.

Confianza de los stakeholders: La implementación de un sistema de gestión de la continuidad de negocio muestra el compromiso de la organización con la protección de sus activos, clientes y socios comerciales, generando confianza y credibilidad.

Integración con otros estándares: La continuidad de negocio se integra y relaciona con las tecnologías de la información, ciberseguridad, seguridad de la información y gestión del riesgo.

Principios clave de la norma ISO 22301

- **Enfoque basado en riesgos:** La norma ISO 22301 adopta un enfoque basado en riesgos para identificar y tratar los posibles impactos en la continuidad del negocio. Esto implica que las organizaciones deben identificar y evaluar los riesgos que podrían afectar su capacidad para mantener sus operaciones y tomar medidas para mitigarlos o gestionarlos adecuadamente.
- **Orientación a la dirección:** La norma enfatiza la importancia de la participación y el liderazgo de la alta dirección en el establecimiento de la continuidad del negocio. Los líderes de la organización deben demostrar su compromiso con la continuidad del negocio, establecer políticas claras y objetivos medibles, y proporcionar los recursos necesarios para implementar y mantener el SGCN.
- **Enfoque holístico:** La norma ISO 22301 promueve un enfoque holístico de la continuidad del negocio, considerando todas las partes interesadas relevantes y los aspectos internos y externos que podrían afectar la continuidad de las operaciones. Esto incluye la identificación de los productos y servicios críticos, los procesos y recursos necesarios, así como las interacciones con proveedores, clientes y otras partes involucradas.



ARTÍCULO DE COLABORACIÓN

Gestión de Continuidad de Negocio: Garantizando la Resiliencia Empresarial con la Norma ISO 22301

- **Enfoque holístico:** La norma ISO 22301 promueve un enfoque holístico de la continuidad del negocio, considerando todas las partes interesadas relevantes y los aspectos internos y externos que podrían afectar la continuidad de las operaciones. Esto incluye la identificación de los productos y servicios críticos, los procesos y recursos necesarios, así como las interacciones con proveedores, clientes y otras partes involucradas.
- **Ciclo de mejora continua:** La norma ISO 22301 adopta el enfoque del ciclo de mejora continua, basado en el ciclo PDCA (Planificar, Hacer, Verificar, Actuar). Esto implica que las organizaciones deben planificar y establecer objetivos, implementar y operar el sistema de gestión, realizar evaluaciones y revisiones periódicas para verificar su eficacia y realizar acciones correctivas y preventivas para mejorar continuamente la capacidad de continuidad del negocio.
- **Participación de los empleados:** La norma fomenta la participación activa de los empleados en la gestión de la continuidad del negocio. Esto incluye la identificación de roles y responsabilidades claras, la capacitación adecuada, la conciencia sobre la continuidad del negocio y la promoción de una cultura de preparación y respuesta frente a incidentes.

La norma ISO 22301 proporciona un marco efectivo para garantizar la resiliencia empresarial y la continuidad del negocio en un entorno cada vez más complejo y volátil. Al adoptar un enfoque basado en riesgos, orientación a la dirección, enfoque holístico, ciclo de mejora continua y participación de los empleados, las organizaciones pueden fortalecer su capacidad para enfrentar interrupciones y crisis, proteger su reputación y mantener la confianza de las partes.



SAVE THE DATE

II CONGRESO ASIS LATAM

SEGURIDAD SIN LÍMITES

"Juntos somos más fuertes"

26 y 27 de octubre 2023, Lima - Perú

swissotel LIMA



¡Apoyar, promover e inspirar!



Día Internacional de la Mujer Comunidad WIS (Women In Security) contribución a la Profesión de la Seguridad

El 08 de marzo del 2023, en homenaje a la mujer por su día, se realizó un video con palabras de motivación y experiencias profesionales de las integrantes de la Comunidad WIS Perú (Women In Security). Incentivando a las mujeres al empoderamiento y a unirse a la Comunidad WIS Perú.

El video se puede encontrar en la siguiente URL:

LinkedIn: <https://www.linkedin.com/feed/update/urn:li:activity:7039200371138818048>

YouTube: <https://www.youtube.com/watch?v=UCvykw-h7c>


PUBLICACIONES EN REDES

ASIS
INTERNATIONAL




Lima, Perú
Chapter

WEBINAR

Antes, durante y después de un ataque de Ransomware


Ing. Maurice Frayssinet
PRESIDENTE ASIS PERÚ

14 DE MARZO
8:00 PM (GMT-5)
ACCESO LIBRE

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

El webinar abordó la importancia del ciclo completo de un ataque de ransomware, proporcionando una visión integral de cómo prepararse, responder y recuperarse de un ataque de ransomware, brindando a los participantes herramientas necesarias para proteger sus organizaciones y minimizar los impactos negativos. El evento virtual tuvo una asistencia de 100 participantes conformado por miembros de ASIS de diferentes capítulos y público en general.

ASIS
INTERNATIONAL

Lima, Perú
Chapter

CONVERSATORIO
Comunidad Ciberseguridad

Estado de la Ciberseguridad en el Perú y herramientas de protección


Moderador: Ing. Shirley López


Ing. Sara Mostajo


Ing. Jenny Castañeda

23 DE MARZO
8:00 PM (GMT-5)
ACCESO LIBRE

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

El conversatorio trató sobre la evolución de la ciberseguridad con el pasar de los años. El incremento significativo que hubo de incidentes de ciberseguridad en el Perú, teniendo como víctimas de ataques a las organizaciones tanto públicas como privadas. Asimismo, se hizo mención de las herramientas y medidas que pueden ayudar a protegerse contra las amenazas cibernéticas. El evento virtual tuvo una asistencia de 98 participantes conformado por miembros de ASIS de diferentes capítulos y público en general.

PUBLICACIONES EN REDES



Lima, Perú
Chapter



WEBINAR

Como implementar un laboratorio forense digital



Ing. Raul Chávez

28 DE MARZO
8:00 PM (GMT-5)

ACCESO LIBRE

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

Webinar enfocado a la implementación de un laboratorio forense digital, donde se trató sobre las capacidades de un laboratorio forense digital, es decir, los requisitos mínimos de infraestructura (almacén de evidencia física, almacén de evidencia lógica, área de laboratorio forense digital), recurso de hardware y software (open source y licenciados), recurso humano calificado (perfil de un perito informático forense), la evidencia digital, normas nacionales, internacionales y/o buenas prácticas, casos analizados y resueltos. El evento virtual tuvo una asistencia de 100 participantes conformado por miembros de ASIS de diferentes capítulos y público en general.



Lima, Perú
Chapter



CONVERSATORIO

Comunidad Ciberdefensa

Estrategia Nacional de Ciberseguridad U.S. 2023



Moderador: General (r) Ing. Augusto García Calderón



Coronel FAP Martín Pacherez



Coronel EP Octavio Freitas

31 DE MARZO
7:00 PM (GMT-5)

ACCESO LIBRE

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

El conversatorio llevado a cabo por un panel de expertos, trató sobre la Estrategia Nacional de Ciberseguridad de los Estados Unidos, lanzada el 02 de marzo, con el fin de garantizar los beneficios de un ecosistema digital seguro y protegido para todos los ciudadanos de los EE.UU., este modelo busca que el ecosistema Estadounidense sea defendible, resiliente y se encuentre alineado con valores. El evento virtual tuvo una asistencia de 80 participantes conformado por miembros de ASIS de diferentes capítulos y público en general.

NEWSLETTER



Lima, Peru
Chapter

Perú Edición 02/2023

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



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.



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.



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.



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:

