NEWS LETTER

Perú Edición 04/2023

ASIS INTERNATIONAL® Lima, Peru Chapter

Editorial

La protección ante eventos de ransomware es de vital importancia en la actualidad debido a la creciente sofisticación y frecuencia de estos ataques cibernéticos. El ransomware puede paralizar por completo las operaciones de una empresa y causar graves pérdidas financieras y de reputación. La implementación de medidas de seguridad robustas, como sistemas de respaldo y recuperación de datos, firewalls actualizados y concientización del personal sobre prácticas seguras en línea, es crucial para evitar estos ataques y garantizar la continuidad del negocio. La protección ante ransomware es esencial para salvaguardar los activos y la reputación de una empresa.

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"

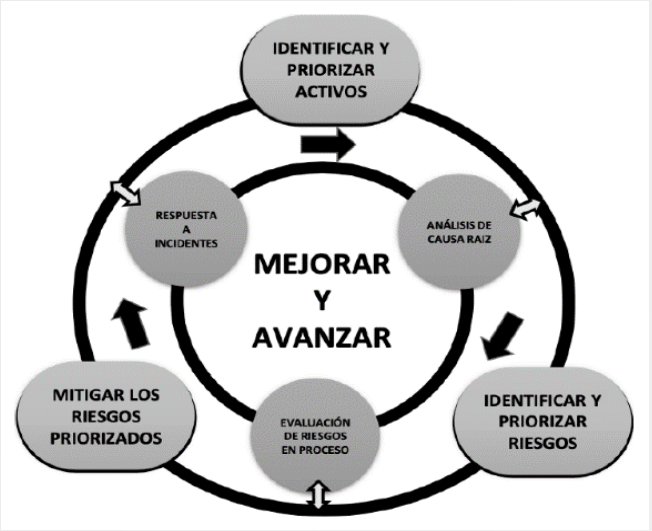
ARTÍCULO DE COLABORACIÓN

Protegiendo los Activos y Preservando la Confianza en la Era Digital

Maurice Frayssinet Delgado

Ingeniero de Sistemas e Informática, Maestría en Tecnologías de la Información, Maestría en ciberseguridad, Maestría en seguridad informática, actualmente cursando la Maestría en Inteligencia Artificial, Doctorado en Ingeniería de Sistemas, miembro del Colegio de Ingenieros del Perú. Con experiencia de más de 20 años en Auditoria de Sistemas , Ciberseguridad, Ciberdefensa, Ciberinteligencia, Seguridad de la Información, Gestión de continuidad de negocio, Gobierno Digital, Inteligencia Artificial, Educación Virtual, Transformación Digital y gestión de Tecnologías de la información y comunicaciones. Cuenta con las certificaciones internacionales ISO 27001 Lead Implementer, ISO 27001 Lead Auditor, ITIL, ISFS 27002, LPIC-1 entre otras. **Actualmente Presidente de ASIS Perú.**

En el entorno empresarial actual, la seguridad corporativa se ha convertido en una preocupación fundamental para las organizaciones de todo el mundo. Con el avance de la tecnología y la creciente sofisticación de los ciberataques, las empresas se enfrentan a una amplia gama de amenazas que pueden comprometer la confidencialidad, integridad y disponibilidad de la información empresarial. En este artículo, exploraremos la importancia de la seguridad corporativa, sus desafíos y proporcionaremos consejos prácticos para proteger los activos y preservar la confianza en la era digital.



Comprender los riesgos y desafíos actuales

La seguridad corporativa implica la protección de los activos de información, incluyendo datos confidenciales, propiedad intelectual, sistemas y redes empresariales. Sin embargo, en la era digital, las empresas se enfrentan a una amplia gama de riesgos y desafíos en materia de seguridad. Los ciberataques, el robo de datos, el ransomware, la ingeniería social y las amenazas internas son solo algunos ejemplos. Es fundamental que las organizaciones comprendan estos riesgos y evalúen su exposición a ellos. Realizar una evaluación de riesgos y un análisis de vulnerabilidades ayudará a identificar las posibles brechas en la seguridad y las áreas que requieren una mayor atención.

Implementar un enfoque integral de seguridad

La seguridad corporativa no es un tema que pueda abordarse de manera aislada o mediante la implementación de soluciones fragmentadas. Es esencial adoptar un enfoque integral que abarque políticas, procesos y tecnologías. Esto incluye establecer políticas claras de seguridad, normas de uso aceptable y una cultura organizacional que promueva la seguridad en todos los niveles. Además, es crucial implementar medidas técnicas como firewalls, sistemas de detección y prevención de intrusiones, cifrado de datos y protección contra malware.

ARTÍCULO DE COLABORACIÓN

Protegiendo los Activos y Preservando la Confianza en la Era Digital

La seguridad física también juega un papel importante, especialmente en el control de acceso a instalaciones y la protección de equipos críticos.

Concientización y capacitación de empleados

Los empleados son una parte fundamental de la estrategia de seguridad corporativa. La concientización y la capacitación en seguridad deben ser una prioridad en toda la organización. Los empleados deben comprender los riesgos asociados con la manipulación de datos, el uso de contraseñas débiles, el phishing y otras tácticas de ingeniería social.

Mediante la capacitación regular, los empleados pueden aprender a identificar y reportar posibles amenazas de seguridad, así como a utilizar las mejores prácticas de seguridad en su trabajo diario. La concientización también implica fomentar una cultura de seguridad, donde se aliente a los empleados a informar cualquier incidente o actividad sospechosa.

Protección de datos y privacidad

La protección de datos y la privacidad son aspectos críticos de la seguridad corporativa. Las empresas deben implementar políticas y medidas para garantizar que los datos de los clientes, socios comerciales y empleados estén protegidos y se utilicen de manera ética y legal. Esto implica cumplir con las leyes y regulaciones de privacidad, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea. Las empresas deben establecer políticas claras de manejo y almacenamiento de datos, así como procedimientos de consentimiento informado para recopilar y utilizar información personal. Además, es fundamental contar con medidas de seguridad sólidas, como el cifrado de datos, el acceso restringido y la realización de auditorías periódicas para garantizar el cumplimiento y la protección de los datos confidenciales.

ARTÍCULO DE COLABORACIÓN

Protegiendo los Activos y Preservando la Confianza en la Era Digital

Gestión de incidentes y respuesta a emergencias

Incluso con las mejores medidas de seguridad, es posible que una empresa experimente un incidente de seguridad en algún momento. Es esencial contar con un plan de gestión de incidentes y una respuesta eficiente a emergencias. Esto incluye establecer un equipo de respuesta capacitado, asignar roles y responsabilidades claras, y tener procedimientos documentados para contener, investigar y mitigar los incidentes. Además, es importante establecer comunicaciones claras y transparentes con las partes interesadas internas y externas durante un incidente, preservando la confianza y la reputación de la empresa.

Mantenerse actualizado y estar preparado

La seguridad corporativa es un campo en constante evolución, y las amenazas cibernéticas están en constante cambio. Es fundamental que las empresas se mantengan actualizadas con las últimas tendencias y desarrollos en seguridad. Esto implica estar informado sobre las nuevas técnicas utilizadas por los ciberdelincuentes, las vulnerabilidades emergentes y las mejores prácticas de seguridad. Las organizaciones deben invertir en la formación continua de su personal de seguridad y en la participación en comunidades de seguridad y conferencias relevantes. Además, es importante realizar pruebas de penetración y evaluaciones de seguridad periódicas para identificar posibles vulnerabilidades y corregirlas de manera proactiva.

Conclusiones

La seguridad corporativa es una preocupación crítica en la era digital. Al implementar un enfoque integral de seguridad, concienciar y capacitar a los empleados, proteger los datos y estar preparados para emergencias, las empresas pueden proteger sus activos y preservar la confianza de sus clientes y socios comerciales.

ARTÍCULO DE COLABORACIÓN

La Gestión de Seguridad en escenarios volátiles

Mikel Rufián Albarrán

Director Global de Cybersecurity & Intelligence de BIDAIDEA, la Firma multinacional de Ciberseguridad, Inteligencia y Seguridad Integral. Socio de referencia de la OCC – Oficina de Coordinación de Ciberseguridad y el CNPIC - El Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) del Ministerio del Interior.

Cuenta con más de 16 años de experiencia, su carrera profesional ha estado orientada principalmente en el ámbito de la seguridad, gestión de riesgos integrales, investigación e Inteligencia-Contrainteligencia en diversos sectores (Energía, Industria, Servicios, Telecomunicaciones, Banca y Seguros, Tecnología y software, Auditoría y Consultoría, Construcción, inmobiliaria y Sector Público).

La importancia del ciberespacio y del avance tecnológico ha supuesto un cambio sustancial en las relaciones entre ciudadanos, empresas, administraciones públicas, infraestructuras críticas y servicios esenciales, así como un impulso al desarrollo de las sociedades actuales. Y es que en el ciberespacio no existen fronteras: las amenazas, los riesgos, las oportunidades y los ataques pueden provenir de cualquier lugar, en cualquier momento y de actores no convencionales (ciberguerra híbrida).

Exposición digital y resiliencia

Garantizar la seguridad en el ciberespacio se ha convertido en un objetivo prioritario en las agendas de la mayoría de los gobiernos, ya que en ocasiones puede llegar a afectar a la seguridad nacional. Sin embargo, no solo este punto hace que el reto sea mayor.

Con el uso de las nuevas tecnologías (IT-OT-IoT) para cometer ciberataques contra gobiernos, empresas e individuos, palabras y frases que hace una década apenas existían, forman ahora parte de nuestro vocabulario diario. La capacidad de absorción de dicho impacto y los mecanismos de protección válidos para la mayoría de las organizaciones pueden no ser suficientes en los entornos críticos y esenciales e incluso en sistemas IT-OT-IoT, no de por sí establecidos como críticos, pero que indirectamente afectan a estos.

Los tiempos cambian, y estamos en plena transformación digital de la seguridad. Por ello, las infraestructuras críticas y los servicios esenciales se han adaptado a un modelo digital para acercar sus servicios. Y esta migración conlleva una gran exposición de todas las organizaciones. Al igual que las empresas contratan seguridad física, electrónica o protección contra incendios para sus oficinas, ahora deben contratar inteligencia y ciberseguridad. El ecosistema IoT incluye dispositivos, redes, plataformas y aplicaciones que requieren múltiples medidas de protección de la seguridad en cada capa, presentando vulnerabilidades técnicas relacionadas en sus mecanismos de autenticación o en el cifrado de la información que transmiten; por ejemplo, una gran cantidad de datos que, sin el cifrado apropiado, se difunden a través de redes inalámbricas de manera pública y sin seguridad. Te interesa: Ciberdefensa nacional, responsabilidad público-privada compartida.

ARTÍCULO DE COLABORACIÓN

La Gestión de Seguridad en escenarios volátiles

La base de cualquier organización pública o privada es entender su capacidad adaptativa y cómo incrementarla para acometer con éxito esta crisis. Y con capacidad adaptativa nos referimos a la posibilidad que tiene la organización de mantener su desempeño ante diferentes situaciones, modificando si es necesario los planes, estructuras o procesos inicialmente establecidos con acciones rápidas y flexibles.

En este sentido, y para fortalecer la organización, la resiliencia debe formar parte de su cultura. Se trata de medir y de llevar a cabo prácticas para prevenir, simular eventos, proteger, adaptarse y recuperarse valiéndose del aprendizaje sobre las experiencias vividas y la colaboración entre sus diferentes unidades. En definitiva, el ciberespacio constituye un escenario táctico, estratégico y operativo diferente a los espacios terrestre, marítimo, aéreo y exterior, y ha sido calificado en la doctrina como uno de los global commons. Es un entorno complejo resultante de la interacción entre las personas, el software y los servicios en Internet por medio de dispositivos tecnológicos (TIC) conectados a redes, las cuales no existen en ningún tipo de forma física. Servicios esenciales y de aplicación Los servicios de aplicación en el ciberespacio han adquirido un papel y lugar muy importante en la vida cotidiana. De hecho, se están expandiendo más allá de los modelos de empresa y organización a consumidores y de consumidores a consumidores a una forma de interacciones y transacciones de muchos a muchos. Esta situación ha provocado también el aumento de amenazas, riesgos y vulnerabilidades sobre las aplicaciones del ciberespacio, por lo que este último se está convirtiendo en el objetivo de los grupos dedicados a la ciberdelincuencia, cibervandalismo, ciberterrorismo y hacktivismo, así como de actores internos (insiders) y estados y grupos patrocinados por ellos.

La ciberseguridad implica un nuevo paradigma de seguridad global, inclusiva y comprehensiva de la totalidad de los escenarios que se van a ver afectados por la impronta que introducen la existencia y la utilización del ciberespacio. La ciberseguridad se esfuerza, además, por asegurar el logro y el mantenimiento de las propiedades de seguridad de la organización y los activos del usuario contra los riesgos relevantes en el entorno cibernético.

Los objetivos generales de la seguridad comprenden, en definitiva, la preservación de la confidencialidad, la integridad y la disponibilidad de la información en el ciberespacio. Aunque también pueden participar otras propiedades, como la autenticidad, la responsabilidad, el no-repudio y la fiabilidad.

Los activos de la organización y de los usuarios incluyen dispositivos informáticos conectados, personal, infraestructura, aplicaciones, servicios y sistemas de telecomunicaciones, así como la totalidad de la información transmitida y/o almacenada en los sistemas y en el entorno cibernético.

COMUNIDAD DE CIBERSEGURIDAD

Wazuh: Potenciando la Seguridad Empresarial con una Herramienta SIEM de Código Abierto

Jacqueline López Reyes

Ingeniera de Computación y Sistemas, con más de 10 años de experiencia en la administración de Centros de Datos en diferentes plataformas tecnológicas, Gestión de Proyectos y Seguridad de la Información, cursando estudios de Maestría en Inteligencia Artificial, con certificación en ITIL v4 e ISO 27001 Auditor Interno y otros estudios en Gerencia de Proyectos y Calidad con enfoque PMI, Implementador Líder ISO 27001 Seguridad de la Información, Interpretación de la Norma ISO/IEC 27001:2013 Seguridad de la Información, Seguridad Informática, CISSP: Certified Information Systems Security Professional, Administración de redes CCNA I, II y III, Administración y configuración de virtualización con VMware, Administración y manejo de Plataformas de Servidores y Almacenamiento (Storage), entre otros. A**ctualmente Líder de la Comunidad de Ciberseguridad.**

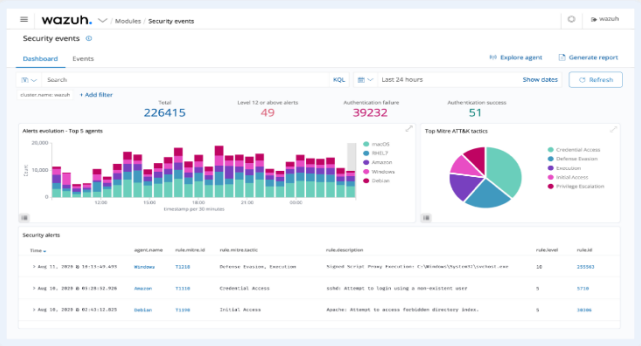
En el entorno empresarial actual, donde las amenazas cibernéticas son cada vez más sofisticadas y frecuentes, contar con una solución eficiente de Gestión de Información y Eventos de Seguridad (SIEM, por sus siglas en inglés) se ha vuelto fundamental para proteger los activos y la integridad de las organizaciones. En este artículo, exploraremos el uso de Wazuh como una herramienta SIEM de código abierto, que permite a las empresas detectar, analizar y responder a incidentes de seguridad en tiempo real. Desarrollaremos las características clave de Wazuh y analizaremos cómo puede potenciar la seguridad empresarial.

¿Qué es Wazuh?

Wazuh es una plataforma de seguridad de código abierto que combina la funcionalidad de un Sistema de Detección de Intrusiones (IDS, por sus siglas en inglés) y una solución SIEM. Su objetivo principal es proporcionar a las organizaciones una visibilidad completa de su entorno de TI y ayudarles a detectar y responder de manera proactiva a las amenazas de seguridad. Wazuh está basado en el proyecto OSSEC, una solución de seguridad ampliamente utilizada y respetada en la comunidad de código abierto.

Funcionalidades clave de Wazuh

Wazuh ofrece una amplia gama de funcionalidades que lo convierten en una herramienta SIEM potente y versátil para las empresas.



Algunas de las características clave incluyen:

Detección de intrusiones: Wazuh utiliza reglas y políticas predefinidas para analizar el tráfico de red y los eventos del sistema en busca de posibles amenazas y actividades maliciosas.

Análisis de registros: La plataforma recopila y analiza registros de eventos de múltiples fuentes, como sistemas operativos, aplicaciones y dispositivos de red, para identificar patrones anormales o sospechosos.

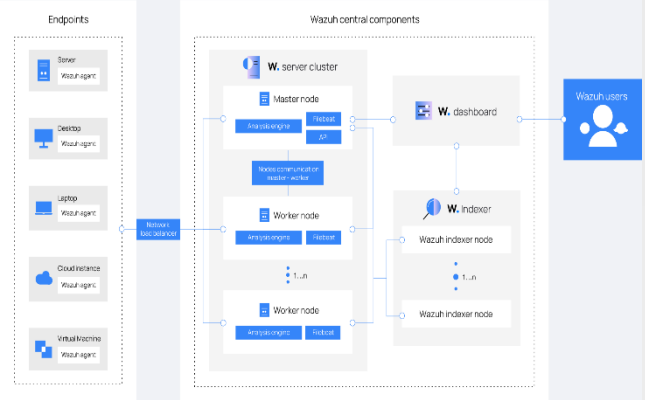
Gestión de activos: Wazuh ayuda a las organizaciones a mantener un inventario actualizado de sus activos de TI, lo que facilita la detección de dispositivos no autorizados o no conformes en la red.

Monitorización de integridad: La herramienta verifica la integridad de los archivos del sistema en busca de cambios no autorizados, lo que puede indicar la presencia de malware o actividades maliciosas.

COMUNIDAD DE CIBERSEGURIDAD

Wazuh: Potenciando la Seguridad Empresarial con una Herramienta SIEM de Código Abierto

Gestión de amenazas y respuestas: Wazuh permite a las organizaciones tomar medidas proactivas para abordar las amenazas de seguridad, como bloquear direcciones IP sospechosas o ejecutar scripts automatizados en respuesta a eventos específicos.



Ventajas del uso de Wazuh

El uso de Wazuh como herramienta SIEM ofrece varias ventajas significativas para las organizaciones:

Costo: Al ser una solución de código abierto, Wazuh no requiere licencias costosas y ofrece una alternativa más económica en comparación con las soluciones comerciales. Esto permite a las empresas aprovechar las capacidades de un SIEM sin incurrir en grandes gastos.

Flexibilidad: Wazuh es altamente personalizable y escalable, lo que permite adaptarlo a las necesidades específicas de cada organización. Los usuarios pueden agregar o modificar reglas, políticas y alertas según sus requisitos de seguridad particulares.

Comunidad activa: Wazuh cuenta con una comunidad de usuarios y desarrolladores activos que colaboran en la mejora continua de la plataforma. Esto significa que hay un soporte sólido y constantes actualizaciones de seguridad y características.

Integración con otras herramientas de seguridad: Wazuh puede integrarse con otras soluciones y herramientas de seguridad, como firewalls, sistemas de detección de intrusiones y sistemas de gestión de incidentes, lo que permite una visibilidad y respuesta más completas frente a las amenazas.

Interfaz intuitiva y amigable: La interfaz de usuario de Wazuh es fácil de usar y proporciona paneles de control intuitivos y visualizaciones claras de los eventos de seguridad. Esto facilita la supervisión y el análisis de la información relevante.

Conclusiones

Wazuh ofrece a las organizaciones una solución SIEM de código abierto y eficiente para mejorar su postura de seguridad. Con sus funcionalidades clave, ventajas económicas y flexibilidad, Wazuh se ha convertido en una opción popular para potenciar la seguridad empresarial y responder de manera efectiva a las amenazas cibernéticas en la era digital.

ARTÍCULO DE COLABORACIÓN

Seguridad en la Nube: Protegiendo los Datos en un Entorno Digital

Jeler Vásquez Cobos

Ingeniero Electrónico, con más de 10 años de experiencia en Tecnológicas de la Información y Comunicación, Gestión de Proyectos y Seguridad de la Información, con Maestría en Seguridad Informática, diplomado en la Interpretación de la Norma ISO 27001 Seguridad de la Información, Seguridad Informática, Administración de redes, Administración y configuración de virtualización con VMware, entre otros.

Especialista en Seguridad de la Información

En la actualidad, la tecnología de la nube ha revolucionado la forma en que almacenamos, compartimos y accedemos a nuestros datos. Sin embargo, este avance tecnológico también ha planteado preocupaciones sobre la seguridad en la nube. A medida que más y más empresas y usuarios individuales confían en servicios de almacenamiento en la nube, es crucial comprender los desafíos de seguridad que se presentan y cómo abordarlos de manera efectiva.

La seguridad en la nube se refiere a las prácticas y medidas implementadas para proteger los datos y las aplicaciones almacenadas en la nube. Uno de los principales desafíos es la protección de la confidencialidad de los datos. Al transferir datos a través de redes públicas, existe el riesgo de que terceros no autorizados puedan acceder a ellos. Para abordar esta preocupación, se utilizan técnicas de cifrado para proteger la confidencialidad de los datos en tránsito y en reposo.

Además del cifrado, la autenticación y la autorización son elementos esenciales en la seguridad en la nube. La autenticación garantiza que solo los usuarios autorizados tengan acceso a los datos, mientras que la autorización establece los permisos y los niveles de acceso para cada usuario. Esto se logra mediante la implementación de controles de acceso adecuados y la gestión de identidades. Otro aspecto crítico de la seguridad en la nube es la protección contra ataques cibernéticos. Los proveedores de servicios en la nube implementan medidas de seguridad, como firewalls y sistemas de detección de intrusiones, para proteger sus infraestructuras.

Sin embargo, los usuarios también tienen la responsabilidad de garantizar que sus propias aplicaciones y datos estén seguros. Esto implica mantener actualizados los sistemas operativos y las aplicaciones, utilizar contraseñas robustas y cambiarlas periódicamente, así como concientizar a los empleados sobre las mejores prácticas de seguridad. Además de las amenazas cibernéticas, existe la preocupación de la pérdida de datos en la nube debido a errores humanos o fallas técnicas. Es importante que los usuarios tengan copias de seguridad y planes de recuperación ante desastres adecuados para garantizar la disponibilidad y la integridad de sus datos en caso de incidentes.

El usuario y el proveedor de servicios en la nube tienen responsabilidades compartidas en términos de seguridad y protección de los datos. A continuación, se detallan las responsabilidades de cada uno:

Responsabilidades del usuario:

1. Gestión de acceso y autenticación: El usuario es responsable de administrar adecuadamente los permisos y la autenticación de los usuarios que acceden a los recursos en la nube. Esto implica asignar roles y permisos adecuados, así como utilizar autenticación de dos factores cuando esté disponible para aumentar la seguridad.
2. Configuración y seguridad de las aplicaciones y sistemas: El usuario es responsable de configurar y asegurar las aplicaciones y sistemas utilizados en la nube. Esto incluye mantener actualizados los sistemas operativos, aplicar parches de seguridad, configurar firewalls y utilizar herramientas de seguridad adecuadas.

ARTÍCULO DE COLABORACIÓN

Seguridad en la Nube: Protegiendo los Datos en un Entorno Digital

3. Gestión de datos: El usuario debe asegurarse de que los datos almacenados en la nube estén adecuadamente protegidos. Esto puede incluir el cifrado de datos sensibles, la implementación de políticas de retención de datos y la realización de copias de seguridad regulares.
4. Cumplimiento de normativas y regulaciones: El usuario es responsable de cumplir con las leyes y regulaciones aplicables en relación con los datos almacenados en la nube. Esto puede incluir normativas como la Ley N° 29733, Ley de Protección de Datos Personales u otras leyes de privacidad y protección de datos en diferentes jurisdicciones.

Responsabilidades del proveedor de servicios en la nube:

1. Seguridad de la infraestructura: El proveedor de servicios en la nube es responsable de garantizar la seguridad de su infraestructura, incluyendo los centros de datos, redes y sistemas. Esto implica implementar medidas de seguridad física, como controles de acceso y monitoreo, así como medidas de seguridad lógica, como firewalls y sistemas de detección de intrusiones.
2. Protección de datos en tránsito y en reposo: El proveedor de servicios en la nube debe implementar medidas de seguridad para proteger los datos en tránsito y en reposo. Esto puede incluir el cifrado de datos durante la transmisión y el almacenamiento, así como el cumplimiento de estándares de seguridad reconocidos.
3. Continuidad del servicio y recuperación de desastres: El proveedor de servicios en la nube debe tener planes y medidas en su lugar para garantizar la continuidad del servicio y la recuperación de desastres en caso de interrupciones o fallas. Esto puede incluir copias de seguridad regulares, redundancia de sistemas y planes de contingencia.
4. Cumplimiento normativo y certificaciones de seguridad: El proveedor de servicios en la nube debe cumplir con las normativas y regulaciones aplicables y, cuando corresponda, obtener certificaciones de seguridad reconocidas para demostrar su compromiso con la seguridad de los datos.

Es importante tener en cuenta que las responsabilidades pueden variar según el modelo de servicio en la nube utilizado (como infraestructura como servicio, plataforma como servicio o software como servicio) y los acuerdos específicos entre el usuario y el proveedor de servicios en la nube. Es recomendable revisar cuidadosamente los términos y condiciones del proveedor de servicios en la nube y establecer acuerdos claros en cuanto a las responsabilidades de seguridad.

La seguridad en la nube es un tema crucial en el mundo digital actual. Si bien ofrece numerosos beneficios, como la accesibilidad y la escalabilidad, también plantea desafíos significativos en términos de protección de datos y aplicaciones. Al implementar medidas de seguridad adecuadas, como el cifrado, la autenticación y la autorización, y la protección contra ataques cibernéticos, los usuarios pueden disfrutar de los beneficios de la nube sin comprometer la seguridad de sus datos. La seguridad en la nube debe ser una prioridad para empresas y usuarios individuales por igual.

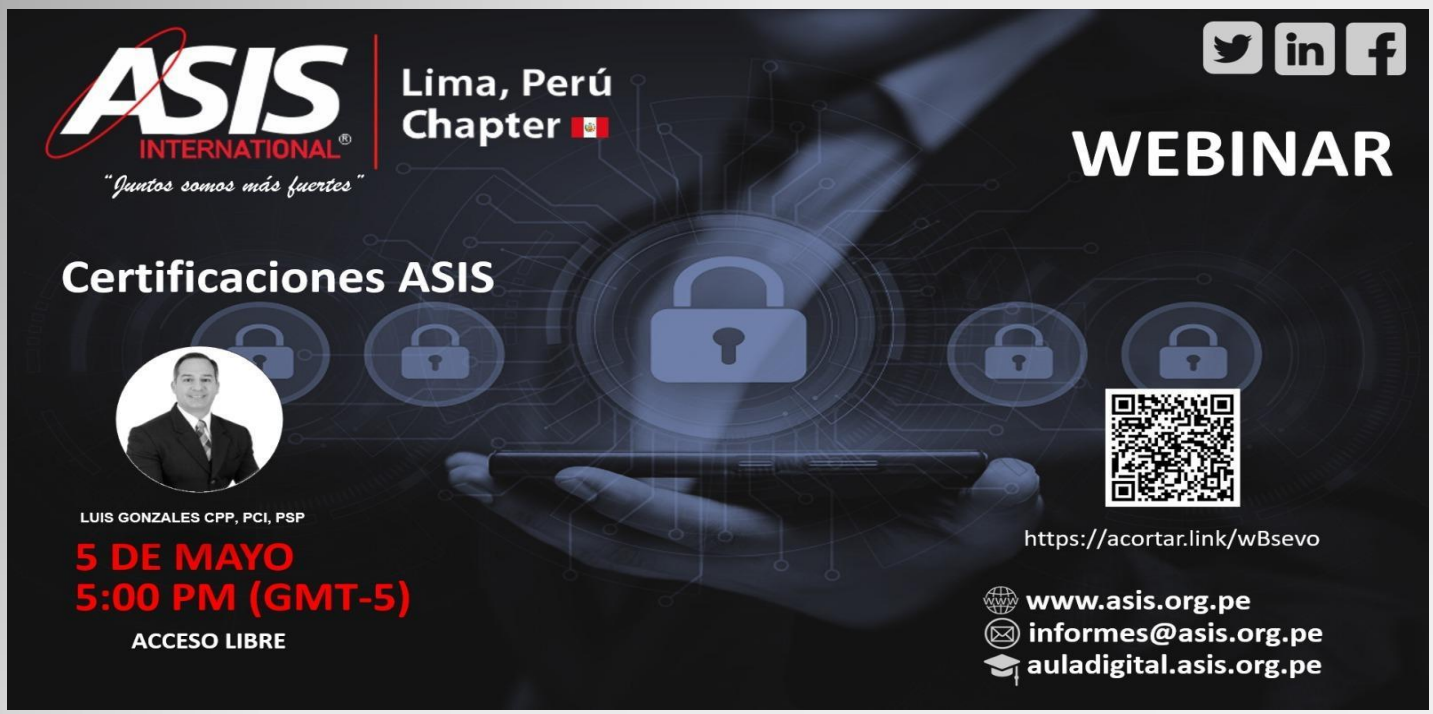
ASIS INTERNATIONAL® Lima, Perú Chapter

Universidad Nacional Federico Villarreal

Workshop: Futuros profesionales en la seguridad

En esta oportunidad como parte de su trabajo de integración con la comunidad académica ASIS Perú realizó un workshop presencial denominado "Futuros profesionales en la seguridad" que tuvo como objetivo fundamental presentar a los alumnos universitarios de las carreras de ingeniería de sistemas, administrativa, software, industrial, informática y afines, las posibles especialidades de seguridad en las que pueden desempeñarse a futuro. El evento realizó el día jueves 25 de mayo de 2023 desde las 9:00 hasta las 13:00 horas Perú en el auditorio de la FIIS - UNFV (Universidad Nacional Federico Villarreal).

PUBLICACIONES EN REDES



El webinar abordó el tema de las 04 certificaciones que brinda ASIS (CPP: Certificación en gestión de seguridad, PCI: Certificación en investigaciones, PSP: Certificación en seguridad física, APP: Certificación en Gestión Fundamental de Seguridad), los requisitos de elegibilidad y las áreas de conocimiento según la experiencia profesional que se tenga, el proceso para completar la solicitud. Asimismo, se brindó información sobre los beneficios de obtener una certificación ASIS International. El evento virtual tuvo una asistencia de 173 participantes conformado por miembros de ASIS de diferentes capítulos y público en general.

El webinar abordó el tema de la incertidumbre en el mundo de la seguridad, es decir la sensación de la inseguridad, por desconocer lo que vendrá en el futuro en un corto, mediano o largo plazo. La importancia de la visión holística de la seguridad empresarial y corporativa, cómo en tiempos de crisis se deben reinventar las empresas. Asimismo, se mencionaron los tipos de incertidumbre (probabilidad, ambigüedad, complejidad) y los tips (acciones) para manejar la incertidumbre. El evento virtual tuvo una asistencia de 121 participantes conformado por miembros de ASIS de diferentes capítulos y público en general.

PUBLICACIONES EN REDES

El webinar abordó la conflictividad social y desafíos para la seguridad corporativa. Estos desafíos incluyen la necesidad de anticiparse a posibles escenarios, implementar medidas de seguridad adecuadas, proteger a los empleados y activos, mantener la continuidad del negocio y establecer canales de comunicación efectivos con las autoridades y las partes interesadas para gestionar la conflictividad de manera segura y efectiva. El evento virtual tuvo una asistencia de 140 participantes conformado por miembros de ASIS de diferentes capítulos y público en general.

El 25 de mayo se realizó el segundo conversatorio de presidentes de cada capitulo de ASIS International para seguir promoviendo el desarrollo, profesionalización y el mejoramiento continuo de la seguridad. El evento virtual tuvo una asistencia de 189 participantes conformada por miembros de ASIS de diferentes capítulos y público en general, el propósito de cada evento realizado permitirá el incremento de la Plana de miembros y Profesionales Certificados.

NEWSLETTER

Perú Edición **04/2023**

ASIS INTERNATIONAL® | Lima, Peru Chapter

Directiva 2023

ASIS PERÚ

Presidente
- Maurice Frayssinet Delgado

Vicepresidente
- Jorge Quevedo Hermoza

Secretaria
- Patricia Fernández Muriel

Tesorero
- Cristian Valenzuela Morales

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

CERTIFICACIONES ASIS INTERNATIONAL

CPP Certified Protection Professional
Board Certified in Security Management

Certificado en Protección Profesional (CPP)

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

PCI® Professional Certified Investigator
Board Certified, ASIS International

Certificado de Investigador (PCI)

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

PSP® Physical Security Professional
Board Certified, ASIS International

Certificado de Profesional en Seguridad Física (PSP)

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

APP® Associate Protection Professional
Board Certified In Security Management Fundamentals

Profesional de Protección Asociado (APP)

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

Síguenos en: