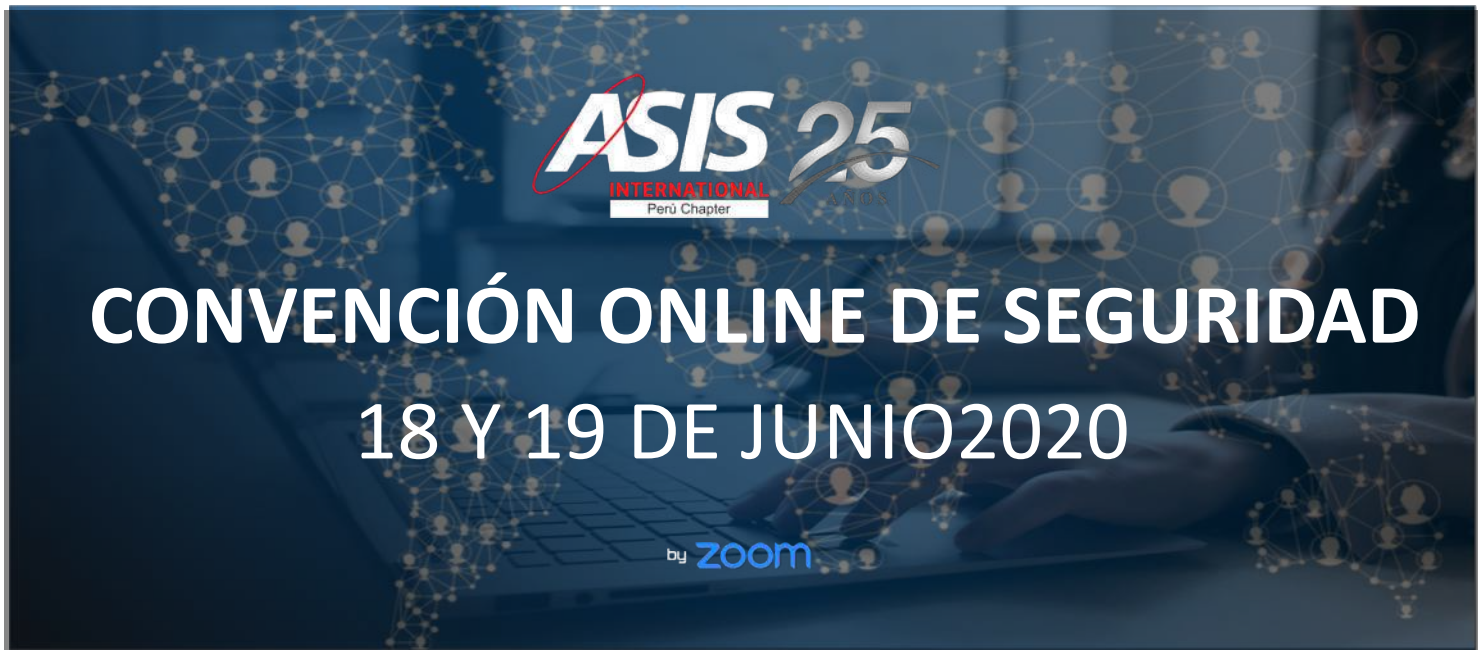
NEWSLETTER

Perú Edición **06/2020**



Editorial

En este mes estamos de anversario.

ASIS PERÚ cumple 25 años que sólo ha sido posible gracias al voluntariado y liderazgo voluntario de los miembros de ASIS PERÚ.

Nuestro capítulo asume el reto de trabajar para que sus miembros puedan tener un soporte a través nuestro y enfocado en el plan estrátégico 2020-2024 de ASIS International realizará acciones con el fin de proponer acciones de valor a sus miembros.

En esta edición se incluyen artículos ciberataques, ciberdelincuencia y sobre nuestra Primera Convención ONLINE de Seguridad.

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

Lo que la pandemia de COVID-19 nos enseña sobre la ciberseguridad y cómo prepararse para el inevitable ciberataque global

- COVID-19 muestra que el mundo corre un gran riesgo de interrupción por pandemias, ataques cibernéticos o puntos de inflexión ambiental.
- Deberíamos prepararnos para una ciber pandemia global similar a COVID que se propagará más rápido y más lejos que un virus biológico, con un impacto económico igual o mayor.
- La crisis del coronavirus proporciona información sobre cómo los líderes pueden prepararse mejor para tales riesgos cibernéticos.

La mayor parte del mundo está experimentando condiciones de vida altamente atípicas como resultado de COVID-19. En el apogeo de la pandemia, más de 2 mil millones de personas estaban bajo algún tipo de bloqueo, y el 91% de la población mundial, o 7.1 mil millones de personas, viven en países con controles fronterizos o restricciones de viaje debido al virus.

Sería reconfortante pensar que esto es simplemente una "falla" que interrumpe un estado de cosas esencialmente estable, y que el mundo volverá a la "normalidad" una vez que la medicina y la ciencia hayan domesticado el virus.

Confortante e incorrecto.

¿Has leído?

Por qué la ciberseguridad es más importante que nunca durante la pandemia de coronavirus

COVID-19 no es el único riesgo con la capacidad de interrumpir rápida y exponencialmente la forma en que vivimos. La crisis muestra que el mundo es mucho más propenso a las perturbaciones causadas por pandemias, ataques cibernéticos o puntos de inflexión ambiental de lo que indica la historia.

Nuestra "nueva normalidad" no es COVID-19 en sí misma, son incidentes similares a COVID.

Y una ciber pandemia es probablemente tan inevitable como una futura pandemia de enfermedad. El momento de comenzar a pensar en la respuesta es, como siempre, ayer. Para comenzar ese proceso, es importante examinar las lecciones de la pandemia de COVID-19 y utilizarlas para prepararse para un futuro ciberataque global.

Lección # 1: Un ataque cibernético con características similares al coronavirus se propagaría más rápido y más lejos que cualquier virus biológico.

La tasa de reproducción - o R0 - de COVID-19 está en algún lugar entre dos y tres sin ningún distanciamiento social, lo que significa que cada persona infectada pasa el virus a otras dos personas. Este número afecta la velocidad de propagación de un virus; El número de personas infectadas en el estado de Nueva York se duplicaba cada tres días antes del cierre.

Por el contrario, las estimaciones de R0 de los ataques cibernéticos son 27 y superiores. Uno de los gusanos más rápidos de la historia, el gusano Slammer / Sapphire 2003, duplicó su tamaño aproximadamente cada 8,5 segundos, extendiéndose a más de 75,000 dispositivos infectados en 10 minutos y 10.8 millones de dispositivos en 24 horas. El ataque WannaCry 2017 explotó una vulnerabilidad en los sistemas Windows más antiguos para paralizar más de 200,000 computadoras en 150 países; fue detenido por parches de emergencia y el descubrimiento accidental de un "interruptor de apagado".

El equivalente cibernético de COVID-19 sería un ataque autopropagante que utilizara uno o más exploits de "día cero", técnicas para las que todavía no hay parches y firmas de software antivirus específicas disponibles. Lo más probable es que ataque todos los dispositivos que ejecutan un único sistema operativo o aplicación común.

Dado que los ataques de día cero rara vez se descubren de inmediato (Stuxnet usó cuatro exploits de día cero separados y se escondió en los sistemas durante 18 meses antes de atacar), tomaría un tiempo identificar el virus y aún más para evitar que se propague. Si el vector fuera una aplicación de red social popular con, digamos, 2 mil millones de usuarios, un virus con una tasa reproductiva de 20 podría tardar cinco días en infectar a más de mil millones de dispositivos.

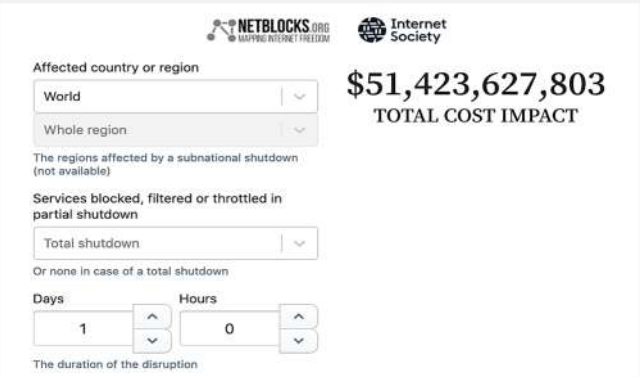
Lección # 2: El impacto económico de un cierre digital generalizado sería de la misma magnitud, o mayor, que lo que estamos viendo actualmente.

- Si el ciber-COVID reflejara la patología del nuevo coronavirus, el 30% de los sistemas infectados serían asintomáticos y propagarían el virus, mientras que la mitad continuaría funcionando con un rendimiento severamente degradado, el equivalente digital de estar en cama durante una semana. Mientras tanto, el 15% sería "borrado" con la pérdida total de datos, lo que requeriría una reinstalación completa del sistema. Finalmente, el 5% estaría "bloqueado", lo que haría que el dispositivo fuera inoperable.
- El resultado final: millones de dispositivos se desconectarían en cuestión de días.

https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus/

Lo que la pandemia de COVID-19 nos enseña sobre la ciberseguridad y cómo prepararse para el inevitable ciberataque global

- La única forma de detener la propagación exponencial de ciber-COVID sería desconectar completamente todos los dispositivos vulnerables entre sí y de Internet para evitar infecciones. Todo el mundo podría experimentar el bloqueo cibernético hasta que se desarrolle una vacuna digital. Se bloquearían todas las comunicaciones comerciales y las transferencias de datos. El contacto social se reduciría a personas contactables mediante visitas en persona, teléfono fijo de cobre, correo postal o radio de onda corta.
- Un solo día sin internet le costaría al mundo más de $ 50 mil millones. Un bloqueo cibernético global de 21 días podría costar más de $ 1 billón.



El bloqueo cibernético también introduciría nuevos desafíos para las economías que dependen digitalmente. Durante los incendios forestales australianos de 2020, los cortes de energía y los daños a la infraestructura de los teléfonos móviles dieron a los ciudadanos una nueva apreciación por las radios FM que funcionan con baterías. Pero si el ciber-COVID asolara un país, ¿qué estaciones de radio seguirían funcionando sin sistemas digitales de grabación y transmisión? ¿Podrían retroceder estados como Noruega, que ha completado su transición a la radio digital?

Lección # 3: La recuperación de la destrucción generalizada de los sistemas digitales sería extremadamente difícil.

Reemplazar el 5% de los dispositivos conectados del mundo requeriría alrededor de 71 millones de dispositivos nuevos. Sería imposible para los fabricantes aumentar rápidamente la producción para satisfacer la demanda, especialmente si los sistemas de fabricación y logística se veían afectados. Para los sistemas que sobreviven, habría un importante cuello de botella en los parches y la reinstalación.

La concentración geográfica de la fabricación de productos electrónicos crearía otros desafíos. En 2018, China produjo el 90% de los teléfonos móviles, el 90% de las computadoras y el 70% de los televisores. Señalar con el dedo sobre la fuente y el motivo del ataque cibernético, así como sobre la competencia para ser el primero en la fila de suministros, conduciría inevitablemente a tensiones geopolíticas.

¿Cómo podemos prepararnos para el ciber-COVID?

La pandemia de COVID-19 proporciona información sobre cómo los líderes pueden prepararse para un riesgo de "cola gorda":

1. Los ciberataques sistémicos generalizados no solo son posibles o plausibles; deberían ser anticipados. Como hemos visto con COVID-19, incluso un breve retraso en la respuesta puede causar un daño exponencial.
2. El éxito de Nueva Zelanda en la lucha contra la pandemia demuestra que las acciones tempranas y decisivas y la comunicación clara y consistente aumentan la resiliencia. Es imposible prepararse para cada riesgo potencial, pero tanto el sector público como el privado deberían invertir en ejercicios de escenarios para reducir el tiempo de reacción y apreciar la variedad de opciones estratégicas en caso de que ocurra un ataque.
3. COVID-19 ha revelado la importancia de la coordinación internacional entre las partes interesadas. La cooperación entre los líderes del sector público y privado también es crítica, particularmente cuando se trata de mitigación. El Centro para la Ciberseguridad en el Foro Económico Mundial es solo un ejemplo de una organización que aborda los desafíos sistémicos de ciberseguridad y mejora la confianza digital en instituciones, empresas e individuos.
4. Del mismo modo que COVID-19 ha presionado a las personas y organizaciones a buscar sustitutos digitales para las interacciones físicas, los líderes gubernamentales y empresariales deberían pensar en lo contrario. El "retroceso digital" y los planes de continuidad son esenciales para garantizar que las organizaciones puedan continuar operando en caso de una pérdida repentina de herramientas y redes digitales, como Maersk aprendió durante el ataque cibernético NotPetya en 2017, que eliminó 49,000 computadoras portátiles e impresoras y borró todo contactos desde sus teléfonos sincronizados con Outlook. Una parte necesaria de la transformación digital es tener información sensible e importante almacenada y accesible en forma física e impresa.

Pero quizás la lección más importante: COVID-19 era un riesgo conocido y anticipado. Entonces, también, es el equivalente digital.

Vamos a estar mejor preparados para eso.

https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus/

18 Y 19 DE JUNIO2020

CONVENCIÓN ONLINE DE SEGURIDAD

ASIS INTERNATIONAL Perú Chapter 25 AÑOS

Desafíos y compromisos para los Profesionales de Seguridad.
En el marco de las actividades por el 25 aniversario de ASIS PERÚ desarrollaremos la CONVENCIÓN ONLINE DE SEGURIDAD. Un ciclo de conferencias virtuales a desarrollarse el jueves 18 y viernes 19 de junio del presente año, preparadas especialmente para el intercambio de conocimientos y experiencias entre líderes de seguridad y especialistas del sector.

by zoom

ASIS PERÚ comprometido con la profesionalización de la Seguridad propone es esta oportunidad abordar los temas de Privacidad de Datos, estión del Fraude, Cultura de Seguridad y el Valorde las Certificaciones en la Gestión Empresarial.Jornada dedosdías dedicada también a la integración en nuestra región Nuestro compromiso, seguir fortaleciendo laCultura deSeguridad.

Apoyo Institucional

ACFE Lima Chapter asbanc

Colaboradores

tecem SEGURIDAD EN AMÉRICA ces

18 Y 19 DE JUNIO2020

CONVENCIÓN ONLINE DE SEGURIDAD

by zoom

ASIS INTERNATIONAL Perú Chapter 25 AÑOS

Cómo los ciberdelincuentes usan estafas de coronavirus para atacar a las víctimas

Cuando las personas tienen miedo, a menudo quieren aprender más sobre la amenaza que enfrentan para tener una sensación de control. Esta es una respuesta humana normal. Pero existen ramificaciones para la iberseguridad cuando los malos actores explotan esa respuesta, como lo hicieron durante la pandemia de coronavirus.

A finales de marzo de 2020, los analistas de KnowBe4, una plataforma de formación de concientización de seguridad y simulación de phishing, detectaron una nueva tendencia de correo electrónico de phishing que advirtió a los destinatarios que habían estado expuestos directamente al virus a través del contacto con un colega, amigo o miembro de la familia e instó a los destinatarios a imprima un formulario de contacto de emergencia adjunto para llevarlo a la clínica de emergencia más cercana.

El correo electrónico parecía ser enviado desde un hospital, lo que lo hizo especialmente alarmante y convincente.

"Para los malos, este es un entorno rico en objetivos que aprovecha los miedos y las emociones intensas de los usuarios finales durante esta pandemia", dijo Eric Howes, investigador principal de laboratorio de KnowBe4. "Los empleados deben ser muy cautelosos cuando se trata de correos electrónicos relacionados con COVID-19, y deben estar capacitados y educados para esperarlos, identificarlos con precisión y manejarlos de manera segura".

Desafortunadamente, la alerta de KnowBe4 no fue única. Desde que comenzó el brote de coronavirus en China en diciembre de 2019 y se convirtió en una pandemia en marzo de 2020, los ciberdelincuentes se han involucrado cada vez más en actividades maliciosas para obtener ganancias u obtener acceso a la información.

La Organización Mundial de la Salud (OMS) emitió una advertencia a principios de 2020 de que los delincuentes se hacían pasar por la OMS en un intento de robar dinero o información confidencial.

Los ciber actores enviaban correos electrónicos de phishing, solicitando a los destinatarios sus nombres de usuario y contraseñas, para hacer clic en enlaces maliciosos o para abrir archivos adjuntos maliciosos.

El Departamento de Justicia de los EE. UU. (DOJ) también ordenó a los abogados de los EE. UU. Que estén en alerta por fraudes que se aprovechan de los preocupados por COVID-19.

"La pandemia es lo suficientemente peligrosa sin que los malhechores busquen beneficiarse del pánico público y este tipo de conducta no puede ser tolerada", dijo el fiscal general de Estados Unidos William Barr en un comunicado.

El FBI publicó un anuncio de servicio público el 20 de marzo, advirtiendo que había visto un aumento en los estafadores que aprovechaban la pandemia de COVID-19. La Oficina aconsejó a los ciudadanos que estén atentos a correos electrónicos falsos de los Centros para el Control y la Preparación de Enfermedades (CDC) de los EE. UU. Que afirman ofrecer información sobre el virus, incluidos enlaces y archivos adjuntos.

El FBI también advirtió al público que sea cauteloso con cualquier persona que venda productos que afirman prevenir, tratar, diagnosticar o curar COVID-19.

"Esté atento a los productos falsificados, como los productos desinfectantes y el equipo de protección personal, incluidas las máscaras de respiración N95, gafas, máscaras faciales, batas y guantes", explicó la Oficina.

En una sesión informativa sobre amenazas en marzo, la firma de ciberseguridad Crowdstrike dijo que comenzó a notar la tendencia de los actores de amenazas que usaban temas de coronavirus en sus mensajes en febrero de 2020. MUMMY SPIDER, un atacante criminal motivado financieramente conocido por el malware Emotet, comenzó a usar un coronavirus. esquema relacionado para atacar a las víctimas japonesas, dijo Adam Meyers, vicepresidente de inteligencia de amenazas de Crowdstrike.

"Después de que el contenido de correo electrónico de una víctima ha sido robado, MUMMY SPIDER identifica los hilos de correo electrónico por la línea de asunto (por ejemplo, Re:) y formula una respuesta al hilo", según el Informe de Inteligencia de Amenazas 2020 de Crowdstrike. "Esta táctica aumenta la probabilidad de que un destinatario abra un archivo adjunto malicioso (o haga clic en un enlace) porque el remitente parece ser alguien con quien se comunicó previamente y la línea de asunto coincide con un hilo de conversación anterior que tuvo con esa persona".

https://www.asisonline.org/security-management-magazine/articles/2020/06/how-cyber-criminals-use-coronavirus-scams-to-target-victims/

Cómo los ciberdelincuentes usan estafas de coronavirus para atacar a las víctimas

Velvet Chollima de Corea del Norte (el nombre que Crowdstrike usa para referirse a un actor de amenaza de estado nación de Corea del Norte) estaba específicamente dirigido a personas que hablaban tanto coreano como inglés en la época en que Corea del Sur estaba siendo golpeada por el coronavirus.

"El momento se alinea hasta cuando los surcoreanos hubieran estado interesados en algo relacionado con el coronavirus y más probable que abrieran un documento", explicó Meyers.

Crowdstrike también ha visto actividad de ransomware relacionada con COVID-19. En el estado estadounidense de Illinois, el Distrito de Salud Pública de Champaign-Urbana confirmó que su sitio web estaba en peligro por el ransomware. El distrito notificó al FBI y al Departamento de Seguridad Nacional de los EE. UU., Según The News Gazette, y finalmente pudo restaurar su sitio web.
Sin embargo, el ataque de ransomware demostró cómo la tendencia de Big Game Hunting (BGH) continuará en 2020 y durante la pandemia. BGH se refiere a la tendencia de enfocarse en las instituciones que necesitan tener sus operaciones en funcionamiento en todo momento, como un hospital o una empresa de servicios públicos.

"Esto se refiere a lo que estamos viendo y lo estamos siguiendo muy de cerca", dijo Meyers.
Este tipo de ataques estimuló a los expertos en ciberseguridad a unirse para proteger y responder a las amenazas cibernéticas contra los servicios de salud. La iniciativa, llamada Cyber Volunteers 19 (CV19), facilita un servicio voluntario de emparejamiento para proporcionar acceso a servicios de salud a un grupo de expertos en ciberseguridad, junto con soporte para inteligencia de amenazas, conciencia de seguridad, planificación de continuidad comercial y más. Hasta el 17 de marzo, CV19 dijo que más de 1,000 personas habían indicado que querían ser voluntarias para ayudar con el esfuerzo.

"COVID-19 está afectando a un gran número de personas, ya sea directa o indirectamente", escribió Sarah Smith, directora de seguridad y resiliencia, en una publicación de blog para CV19. “Es vital proteger los servicios de atención médica de primera línea de edificios, instalaciones y fallas de TI, para garantizar que las personas puedan tener acceso a la atención y el apoyo que necesitan. Al trabajar juntos,podemos permitir la continuidad y disponibilidad de estos servicios esenciales ".

"Nuestro objetivo es hacer que la seguridad sea lo más simple posible para las personas", dijo Spitzner en un seminario web organizado por SANS sobre la preparación de las fuerzas de trabajo para ir a distancia. "Están abrumados, y se podría pensar que [la autenticación multifactor y las redes privadas virtuales] son simples: para muchas personas son aterradoras y confusas".

Es por eso que Spitzner sugiere asociarse con el equipo de comunicaciones para enviar mensajes internos de seguridad cibernética para que los empleados sean conscientes de las amenazas para que sepan qué buscar y, lo ideal, no caer en ellas.
Tonia Dudley, asesora de soluciones de seguridad de Cofense y miembro de la junta de la Alianza Nacional de Seguridad Cibernética, advirtió contra el uso de temas de coronavirus en campañas de simulación de phishing. En cambio, las organizaciones deberían centrarse en qué buscar en los correos electrónicos de phishing y en las medidas básicas de seguridad que deben tomarse mientras trabajan desde casa.

Spitzner also said organizations should communicate with staff about how to report actividad sospechosa o posibles incidentes.
"Accesible, empático, servicial, eso es lo que nosotros, como equipo de seguridad, tendremos que ser para nuestro equipo durante estos difíciles tiempos de transición", dijo.
Para ayudar aún más a las organizaciones que realizan la transición al trabajo remoto, SANS también lanzó un kit de implementación de trabajo desde el hogar. El kit proporciona información general sobre cómo identificar ataques comunes de ingeniería social, cómo configurar una red Wi-Fi segura, cómo crear una contraseña segura, cómo actualizar dispositivos que no son corporativos y cómo hablar con los miembros de la familia: quién también podría estar usando la misma red Wi-Fi, sobre cómo estar seguro en línea. “Muévase rápidamente y asegure esa fuerza de trabajo remota. Decide cuáles son los comportamientos clave en los que enfocarte ”, dijo Spitzner. “La parte más difícil no es decidir qué enseñar, sino qué cortar y qué no enseñar. Priorice la menor cantidad de riesgos que tienen el mayor retorno de la inversión ".

En el lado positivo, a medida que las personas se adaptan al trabajo remoto, que puede convertirse en la norma durante la pandemia donde se requieren medidas drásticas de distanciamiento social, más personas se darán cuenta de los marcadores de un correo electrónico de phishing o un mensaje fraudulento, y las herramientas de seguridad obtendrán es mejor bloquearlos directamente, dice David London, director senior de The Chertoff Group, que se enfoca en la gestión de riesgos cibernéticos y la planificación de respuesta a incidentes.
Durante el próximo año, a medida que el mundo pasa por períodos de distanciamiento social para mitigar los brotes de coronavirus, London dice que es optimista sobre la capacidad de las organizaciones para manejar la transición.

https://www.asisonline.org/security-management-magazine/articles/2020/06/how-cyber-criminals-use-coronavirus-scams-to-target-victims/

NEWSLETTER

Perú Edición **06/2020**

DIRECTIVA

Percy Quispe **MBA, CIP**
Presidente

Martín Gálvez
Vicepresidente

Luis González **CPP, PSP**
Secretario

Carlos Prado
Tesorero

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