NEWS LETTER

ASIS INTERNATIONAL® Lima, Peru Chapter

Perú Edición 03/2023

Editorial

Las certificaciones ASIS, desempeñan un papel crucial en la seguridad corporativa al proporcionar un estándar reconocido globalmente para evaluar y validar las habilidades y conocimientos de los profesionales en este campo. Estas certificaciones demuestran el compromiso con las mejores prácticas de seguridad y brindan confianza a los empleadores y clientes. Al obtener una certificación ASIS, los profesionales mejoran su credibilidad y aumentan sus oportunidades de empleo y avance profesional en el campo de la seguridad corporativa. Las certificaciones ASIS son fundamentales para garantizar la calidad y competencia en la industria de la seguridad corporativa en eso radica la importancia de las actividades que se realizan en el capítulo de ASIS Perú.

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 NEXTGEN

La Gestión de Seguridad en escenarios volátiles

Carlos Lezameta Maldonado

Ingeniero Industrial trilingüe; miembro activo de ASIS International – Chapter Perú y de la International Founder of Protection Officers (IFPO). Especializado en Gestión de Operaciones, Gestión de Riesgos & Compliance. MBA, Máster Internacional en Gestión de Operaciones y Máster en Innovación y Sostenibilidad realizados en CENTRUM y EADA (España), respectivamente. Sólidos conocimientos en Seguridad Estratégica Corporativa, Enterprises Security Risk Management – ESRM, realizado en el Centro de Estudios de Seguridad – CES, Advanced Technologies for Executives desarrollado por IBM y Auditor Interno BASC. Más de 10 años de experiencia en empresas transnacionales del rubro de la seguridad, hidrocarburos, industrial, retail, consumo masivo y otros. Responsable de la gestión operativa, la mejora continua y continuidad del negocio, planificación, control y evaluación de proyectos, establecer estrategias comerciales e implementar soluciones integradas de seguridad a medida.

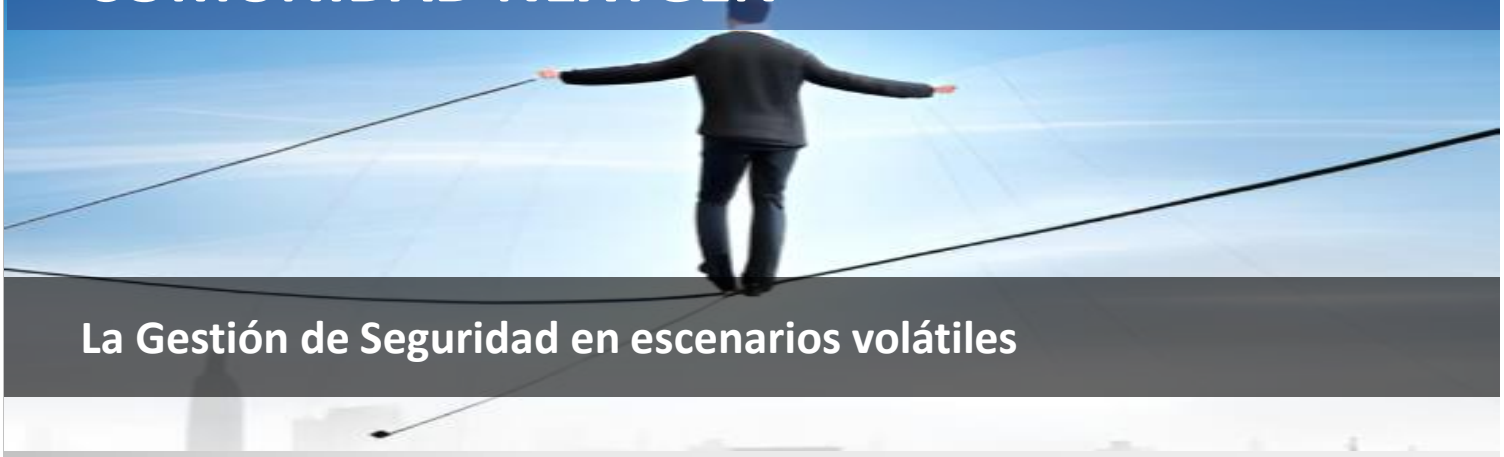
Nos encontramos bajo una realidad sumamente delicada para el país. El predominio de las diferencias ideológicas y políticas están impactando en diferentes formas a la economía nacional, el abastecimiento y, sobre todo, en la fragmentación de la sociedad representada en la violencia y formas de actuar de los sectores más vulnerables de nuestras regiones. Estos escenarios en donde las entidades públicas y las empresas privadas también vienen siendo afectadas, nos hace pensar si realmente nos encontramos preparados para los cambios tan volátiles que los factores externos pueden generar.

Los cambios repentinos y agresivos por amenazas del entorno muchas veces conllevan a tomar decisiones complejas y críticas en corto tiempo, por ello las organizaciones deben mantener una sólida gestión de seguridad donde se cuente con la intervención y el involucramiento de todas las áreas que forman parte de la cadena de valor del negocio. Es fundamental tener identificados todos los procesos críticos por cada área; asimismo, las estrategias y gestiones que mantendrían la continuidad del negocio ante la materialización de alguna amenaza.

El concepto de prevención toma más fuerza con el pasar de los años; la importancia de la cultura de seguridad y de su difusión en todas las áreas de una organización, demuestra el interés en implementar mejores controles, sostenibles y adecuados a los procesos para cada tipo de escenario, independientemente, de la complejidad a la cual se encuentra expuesto. Pienso que aún nos encontramos en un proceso largo de adaptación y desarrollo de la seguridad predictiva; pero, el simple hecho de que algunas empresas han comenzado a profundizar y evidenciar gestiones de éxito es un gran paso.

Definitivamente se debe contar con un soporte adecuado y herramientas que permitan manejar estos escenarios eficientemente, tomando en cuenta que siempre se presentan nuevos contextos, modalidades y amenazas dependiendo de la exposición a dicho entorno. Mantener actualizados los análisis de riesgos o estudios de seguridad, tener un comité de crisis donde participen todas las áreas estratégicas, contar con planes de contingencia actualizados en base a las reestructuraciones organizacionales, canales de comunicación ágiles, recursos, funciones y otros; son los primeros cimientos que permitirán plantear soluciones y buenas decisiones. En este camino, independientemente de las amenazas, se debe priorizar la continuidad del negocio, donde hay que seguir promoviendo la maximización de la rentabilidad, mediante estrategias de optimización de recurso, ahorro en costos y mayores ingresos; pero, sin dejar de ser seguros, de proteger el patrimonio empresarial y, sobre todo, la integridad de nuestros colaboradores.

COMUNIDAD NEXTGEN

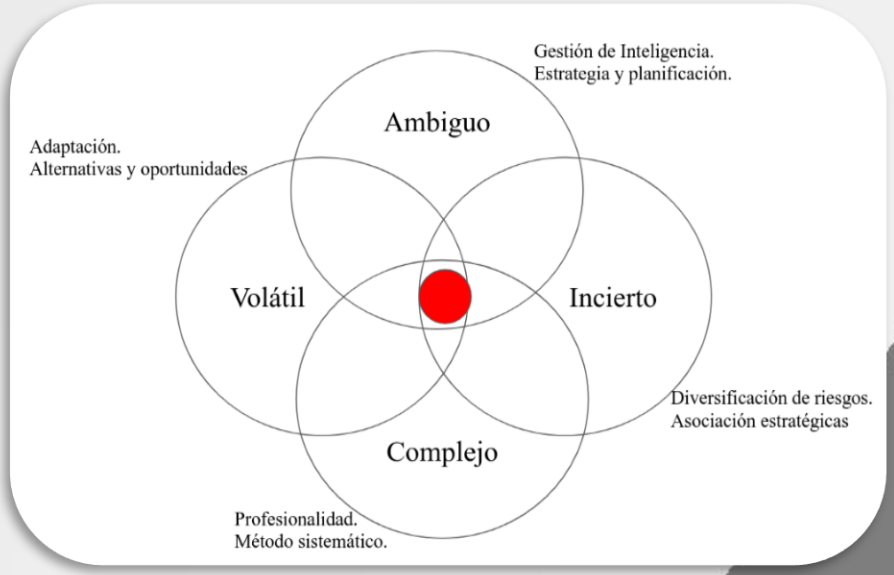


La Gestión de Seguridad en escenarios volátiles

Siempre hay que buscar el factor positivo dentro de un escenario complejo. La volatilidad en estos tiempos es una gran oportunidad de mejora para las empresas y, sobre todo, una gran ventaja para las áreas de seguridad en presentar propuestas que ameriten alguna inversión, mejoras en los flujos de procesos, cambios o mejora de perfiles, capacitaciones y, aplicar nuevas herramientas de gestión. Si consideramos el último punto, el Enterprise Security Risk Management (ESRM) direcciona la administración de los riesgos en forma más estratégica, completa e integrada. Lamentablemente, no se está aprovechando todo su potencial, cuando el profesional de seguridad puede utilizarlo para proponer mejoras integradas, haciendo responsable a cada líder de proceso con sus respectivos equipos. En este camino, se busca ser más resilientes administrando de forma proactiva los riesgos identificados.

En el momento que las metas organizacionales se ven afectadas por el impacto generado, se comienzan a tomar atajos fomentando el desorden; por lo tanto, las buenas prácticas de seguridad pasan a un segundo plano, creando vulnerabilidades internas que pueden ser aprovechadas para beneficios propios con la participación de agentes externos. En este aspecto, es importante que los líderes sean los primeros en identificar la problemática, comunicarla adecuadamente y trabajar muy de la mano con las áreas de seguridad, buscando el respeto al proceso, controles y la mayor transparencia posible, sin generar mayores contratiempos.

Hay que buscar ser aliados estratégicos de todas las áreas, conocer los procesos y controles implementados o por implementar, participar de la toma de decisiones a nivel corporativo y siempre trabajar en equipo. En tiempos difíciles es donde más se requiere serenidad, temple en situaciones críticas, utilizar adecuadamente toda la información de fuentes confiables y dar recomendaciones mediante el previo análisis que den certidumbre a la organización.



COMUNIDAD CIBERDEFENSA

Dependencia Tecnológica del Mundo Ciber
"Juntos Somos más Fuertes"

MAG FAP (r) Augusto García Calderón Sandoval

Magister en Administración y Doctrina Aeroespacial, Magister en Desarrollo y Defensa Nacional, Magister en Recursos Humanos, Ingeniero de Sistemas. Experto en alta Dirección y Planificación estratégica, en sistemas de información, mejoramiento de procesos de calidad basados en soluciones integrales con tecnología digital. Experto en Ciberseguridad y Ciberdefensa, ejecutivo con 30 años de experiencia. Administrador, Director, Gerente de Tecnología, Comandante del Grupo de Operaciones en el Ciberespacio FAP, Comandante de Operaciones de Ciberdefensa de las Fuerzas Armadas del Perú, entre otros cargos y responsabilidades. Calificado en las mejores universidades del país (Ulima, UCatolica, ESAN, CENTRUM, UPiura, URicardo Palma, CAEN) y extranjero (USA, Canadá, México, Argentina, Colombia). **Actualmente Líder de la Comunidad de Ciberdefensa de ASIS Perú.**

"La dependencia tecnológica cada día es mayor, se está perdiendo sensibilidad, el calor humano está siendo remplazado por calor eléctrico digital, el desarrollo dúctil y sensible de la familia se está perdiendo, por la frialdad de la transportación de las comunicaciones"; algo así escuchamos a menudo de nuestros amigos y familiares más longevos, y porque no darles la razón, tiempo de meditar. Sin embargo, la natural evolución humana demanda de mayor productividad y desarrollo. Las formas de vida de una civilización moderna no debe ser excluyente del desarrollo de la civilización, el afecto siempre existirá.

Pues cuándo utilizamos nuestros teléfonos inteligentes para mantenernos en contacto con nuestros seres queridos ingresamos a las redes sociales compartimos información de trabajo desarrollamos nuestras necesidades básicas del día a día, dirigimos un negocio, estamos inmersos en un ecosistema digital, el cual pensamos que es seguro fiable y protegido, sin embargo, cada día nos enfrentamos a riesgos y amenazas de sustracción de información de captura de datos cuyo resultado afecta tanto al desarrollo de la persona, la familia, una organización inclusive a un estado, por tanto es necesario que el esfuerzo conjunto en pro de salvaguardar los intereses nacionales incluya un estado de seguridad y confianza digital en un concepto de unidad.

¡Y esté es el corolario para desarrollar el presente articulo y expresar que es lo que está haciendo el estado por nosotros!

Nuestro país a través de la Secretaría de Gobierno y Transformación digital De la Presidencia del Consejo de Ministros, formuló la Estrategia Nacional de Seguridad y confianza digital[1], cuya estructura contiene ejes, que define el estado de confianza como resultado de la aplicación y gestión de un conjunto de medidas proactivas y reactivas frente a riesgos que afecten la seguridad de las personas, la prosperidad económica y social, y obviamente la seguridad nacional, asimismo; establece que la confianza digital es el resultado de cuán veraces, predecibles, éticas, proactivas y transparentes, además de seguras inclusivas y confiables son las interacciones digitales que se generan entre personas, empresas y entidades públicas con el propósito de desarrollar la economía digital y su transformación. También ha desarrollado el equipo de trabajo **Pe-Cert** vinculado al uso obligatorio de la NTP-27001 para implantar un Sistema de Gestión de Seguridad de la Información, lo interesante de este pilar, es que contiene un enfoque transversal de un gobierno digital, desde la identidad digital, servicios digitales, procedimientos administrativos, datos, interoperabilidad seguridad digital y su arquitectura; lo cual permite disminuir brechas en la seguridad, garantizar los servicios brindados al ciudadano reduciendo riesgos entre otros, formulando políticas claras en ciberseguridad.

1 https://www.gob.pe/institucion/pcm/informes-publicaciones/1998221-estrategia-nacional-de-seguridad-y-confianza-digital

COMUNIDAD CIBERSEGURIDAD

Dependencia Tecnológica del Mundo Ciber
"Juntos Somos más Fuertes"

De lo expresado describe como visión, que el Perú sea reconocido como un líder en la confianza y en el entorno digital, incluyendo los ámbitos de la Protección de Datos personales, la transparencia, la economía digital, la seguridad digital y la protección del consumidor en el entorno digital, acelerando el desarrollo nacional y la reducción de las brechas sociales para contribuir al desarrollo. En cuanto a los objetivos de la política nacional de transformación digital, indica que es prioritario garantizar el acceso a internet de calidad para todos los ciudadanos, se observa que requiere vincular la economía digital a la reactivación y competitividad de los procesos productivos del país asimismo; desarrollar en la administración pública servicios digitales empáticos con la ciudadanía, fortalecer el talento de todos los ciudadanos para producir tecnología digital y aprovechar sus beneficios de manera tal, que en forma permanente se incentive la cultura de innovación y gestión segura con ética e inteligencia de datos, tecnología digital e inteligencia artificial, que es esencial para el funcionamiento básico de nuestra economía, la operatividad de nuestras infraestructuras críticas, la fortaleza de nuestra democracia e instituciones democráticas la privacidad de nuestros datos y comunicaciones y nuestra Defensa Nacional, subraya que: ***"Hemos aprendido que la conectividad digital debe ser una herramienta que eleve y empodere a las personas de todo".***

En el mismo contexto del desarrollo de la Ciberseguridad y haciendo un paralelismo con la Estrategia Nacional de Ciberseguridad de USA, ellos expresan claramente que el mundo digital no debe considerarse una herramienta para la represión y coerción por ello, es que se está preparando para afrontar el reto de tomar una posición de fuerza, liderando junto a sus aliados más cercanos y trabajando con socios de todo el mundo el compartir una visión de futuro digital honesta confiable y brillante[2]. El primero de marzo del presente año, el presidente de los Estados Unidos Joe Biden, presentó la estrategia de ciberseguridad, expresando: ***"Los pasos que damos y las decisiones que tomamos hoy determinan un rumbo de nuestro mundo en las próximas décadas, cuando desarrollamos y aplicamos reglas y normas de conductas en el ciberespacio debemos garantizar que internet siga siendo abierta libre global interoperable fiable y segura, anclada en valores universales que respeten los derechos humanos y la libertades fundamentales".***

Pusieron al mundo en conocimiento, que se está entrando en una nueva fase de dependencia digital cada vez mayor impulsados por tecnologías emergentes y sistemas cada vez más complejos e interdependientes los cambios drásticos de las próximas décadas abrirán nuevas posibilidades para el desarrollo humano y la prosperidad, al tiempo que se multiplicarán los riesgos sistémicos que plantean los sistemas inseguros, la interconectividad, la nueva generación está derrumbando la frontera entre los mundos digitales y físico, exponiendo algunos de nuestros sistemas más esenciales a las perturbaciones de nuestras fábricas, redes eléctricas e instalaciones de tratamiento de aguas entre otras infraestructuras críticas y esenciales.

2 https://www.gob.pe/institucion/pcm/informes-publicaciones/1998221-estrategia-nacional-de-seguridad-y-confianza-digital

COMUNIDAD CIBERSEGURIDAD

Dependencia Tecnológica del Mundo Ciber
"Juntos Somos más Fuertes"

Se están deshaciendo cada vez más de los activos antiguos de control analógicos y están incorporando rápidamente tecnología operativa digital y las tecnologías inalámbricas avanzadas el internet de las cosas y los activos basados en el espacio, incluidos los que permiten el posicionamiento la navegación y el cronometraje de para usos civiles y militares, la vigilancia medioambiental la meteorología y las actividades cotidianas basadas en internet desde la banca a la telemedicina es decir desplazando los sistemas esenciales en línea y haciendo que los ciberataques sean inherentemente más destructivos e impactante para nuestra vida cotidiana. Es entonces que vemos que la colaboración profunda y duradera entre países interesados de un ecosistema digital será, sobre la base de lo que se puede hacer como defendible resistente y a lo alineado a los valores.

Haciendo una interpolación de la estrategia de seguridad y confianza digital del Perú y la estrategia emitida por USA, tenemos similitudes, se infiere que los pilares de USA están orientados a defender las infraestructuras críticas, desarticular y desmantelar a los actores de las amenazas, así como influir en las fuerzas del mercado para impulsar la seguridad y la resistencia, invertir en un futuro resiliente y forjar alianzas internacionales para perseguir objetivos compartidos comunes, y que ello será fundamental para su desarrollo.

Deseo concluir que el mundo tiene su norte natural evolutivo e imparable, seguiremos incrementado el desarrollo tecnológico, su dependencia tecnológica del mundo Ciber, nos da y dará confort, bienestar, salud, etc., pues el avance de la digitalización, la telemedicina, la robótica, el OT, la IA, cibernética, el ciberespacio, espacio entre otros, no tiene retorno.

Por ello, sean Estrategias, Política, Pilares, Objetivos, acciones u otros términos vinculados a la ciberseguridad nacional, existe un común denominador en un contexto de país líder en tecnología y un país en vías al desarrollo sostenible, en el cual los términos de cooperación, colaboración, contribución continua, son imprescindibles, porque la capacidad de una persona para generar ciberataques puede desestabilizar por la asimetría del IQ, praxis y el conocimiento a un país causando enormes destrucciones, y consecuencias irreparables. Entonces no esperemos a que nos apaguen la luz, a que supriman las posibilidades de desarrollo económico, tecnológico ni evolutivo, la tarea es de todos los hombres y mujeres embebidos de ética, valores con sentido de bien universal porque ***"Juntos somos más fuertes".***

COMUNIDAD WIS (WOMEN IN SECURITY)

¿Estás compartiendo demasiado? La importancia de la privacidad y seguridad en las redes sociales

Ximena Cuzcano Chávez

Ingeniera de Sistemas de la Universidad de Lima.

Especialización en Ciberseguridad. Experiencia laboral en el sector público y privado en materia de seguridad de la información, privacidad, protección de datos personales, concientización, ethical hacking e inteligencia artificial.

Actualmente laborando en el Centro de Operaciones de Seguridad Nacional (SOC Nacional) del Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros.

En la última década hemos podido apreciar a la tecnología como herramienta clave en la innovación. Las redes sociales, por ejemplo, han revolucionado la manera en cómo nos comunicamos y relacionamos. La creciente popularidad de las redes sociales ha traído diversos beneficios como conectar con familiares y conocidos, conocer gente nueva cuyos intereses son similares al nuestro. Podemos conversar, intercambiar conocimientos, enviar fotografías y videos, organizar grupos y eventos, y hasta promocionar y ejecutar un modelo de negocio.

No obstante, con una cantidad significativa de personas utilizando redes sociales, la privacidad del usuario se ha convertido en una preocupación cada vez mayor.

El comportamiento del usuario varía significativamente según el tipo de plataforma que esté utilizando. En particular, cuando se trata de redes sociales, la interacción entre usuarios es un factor clave en el uso de estos. Por ejemplo, en las redes sociales, los usuarios a menudo se enfocan en interactuar con otros usuarios, ya sea publicando contenido propio, manteniéndose actualizados con las últimas tendencias o mostrando su aprobación mediante un ***"Me Gusta"*** o comentario. En cambio, en el e-commerce, el comportamiento del usuario se centra en la búsqueda y compra de productos en línea.

Cuando los usuarios se sienten motivados a compartir información en las redes sociales, a menudo no son conscientes de los riesgos de privacidad que esto puede conllevar. Por ejemplo, publicar una foto que revela su ubicación podría poner en peligro su seguridad personal, pero el deseo de compartir experiencias y momentos con amigos y familiares suele ser más fuerte. En ese sentido, el comportamiento prevalece sobre la consideración de la privacidad.

La falta de conciencia sobre la privacidad en redes sociales trae como consecuencia un gran número de perfiles de usuarios que describen abiertamente sus pasatiempos e intereses, utilizando un lenguaje claro y específico. Como resultado, esta información puede ser utilizada por terceros para dirigir anuncios o para recopilar información personal de los usuarios sin su conocimiento o consentimiento.

Por ejemplo, un usuario puede compartir sus planes de fin de semana en su red social favorita sin saber que la información puede ser usada por adversarios para allanar su casa en el momento en que este se encuentre de vacaciones. Además, los usuarios a menudo comparten información personal indirectamente, como su ubicación, edad, familiares y amigos, lo que puede ser aprovechado por criminales para llevar a cabo estafas o actividades delictivas.

COMUNIDAD WIS (WOMEN IN SECURITY)

¿Estás compartiendo demasiado? La importancia de la privacidad y seguridad en las redes sociales

Es bien sabido que la privacidad del usuario es una parte crucial de la seguridad en las redes sociales. Lo que las personas publican o comparten podría potencialmente comprometer su privacidad y seguridad en línea.

Las plataformas de redes sociales limitan la privacidad con su configuración predeterminada, a pesar de que este sea un aspecto importante en la seguridad del usuario. Por esta razón, es crucial que los usuarios accedan a la configuración de privacidad para modificar sus opciones de protección y asegurarse de que su información personal esté resguardada.

Sin embargo, una de las principales dificultades a las que se enfrentan los usuarios es el desconocimiento sobre cómo acceder a las opciones de configuración de privacidad. Por ejemplo, veamos qué pasos debe seguir un usuario para limitar la visibilidad de su perfil a otros usuarios, en algunas plataformas de redes sociales:

- **Facebook:** *Configuración > Privacidad > ¿Quién puede ver tus futuras publicaciones?*
- **Twitter:** *Configuración y privacidad > Privacidad y seguridad > Audiencia y etiquetado > Protege tus tweets*
- **LinkedIn:** *Ajustes y privacidad > Visibilidad > Editar tu perfil público*

Si bien las preocupaciones por la seguridad y privacidad de los usuarios son una debilidad de las plataformas de redes sociales, también lo son por parte de los mismos usuarios. Diversos estudios señalan que los usuarios dedican menos esfuerzos a hacer los cambios adecuados en su configuración de privacidad en las redes sociales que en otros aspectos de la seguridad.

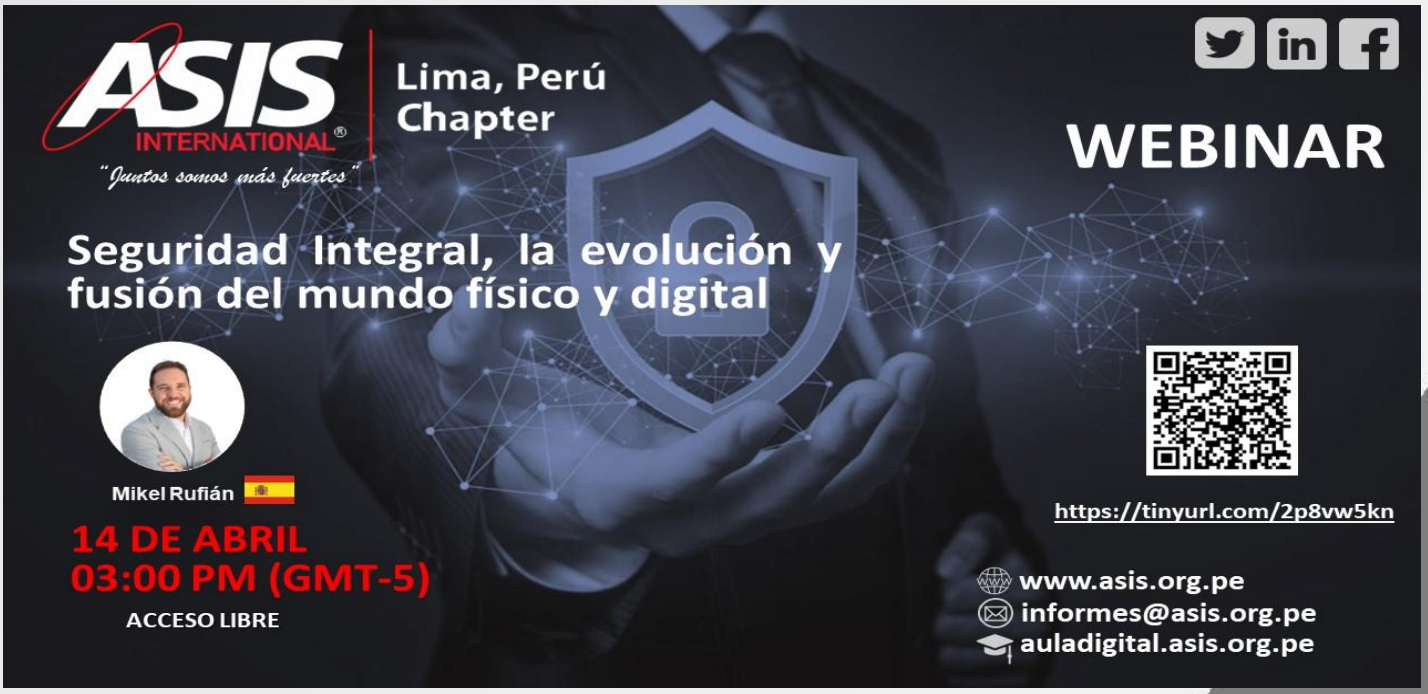
En el siguiente video podemos observar cómo en cuestión de minutos se puede recopilar información sobre una persona a través de sus redes sociales. Este video es un ejemplo claro de cómo una persona malintencionada podría obtener nuestra información personal para realizar acciones perjudiciales en nuestra contra. Al final del video, se muestra incluso la posibilidad de conocer nuestra ubicación exacta.

- https://youtu.be/irIRtA489BA

Es importante que los usuarios comprendan los riesgos y tomen medidas para proteger su privacidad, evitando divulgar información personal innecesaria y configurando adecuadamente sus opciones de privacidad en las plataformas de redes sociales. Al hacerlo, pueden disfrutar de una experiencia más segura y satisfactoria en línea.

PUBLICACIONES EN REDES

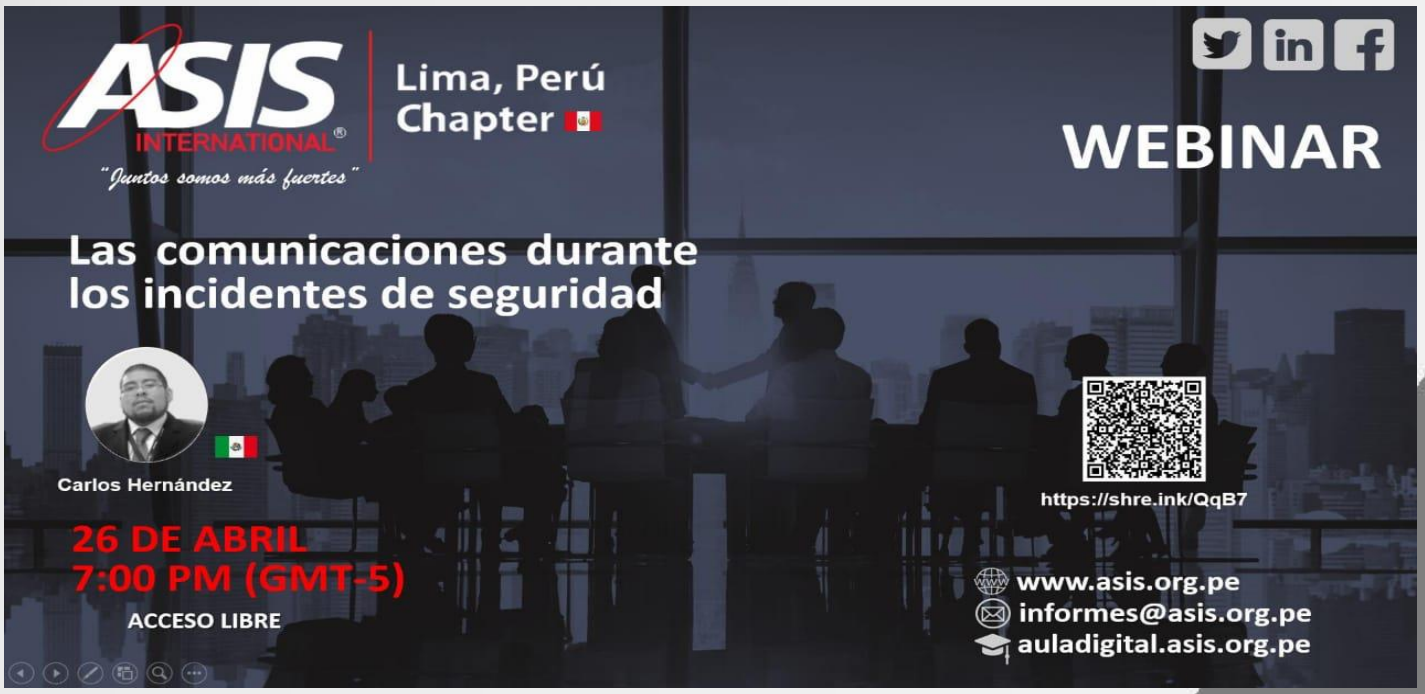
El webinar abordó la importancia de las investigaciones en la gestión de riesgos corporativos, es fundamental para comprender los riesgos a los que se enfrenta una empresa, evaluar su impacto potencial y tomar decisiones informadas. Asimismo, proporcionan información clave para desarrollar estrategias de mitigación efectivas, proteger los activos corporativos y garantizar la continuidad del negocio en un entorno empresarial cada vez más complejo y dinámico. El evento virtual tuvo una asistencia de 80 participantes conformado por miembros de ASIS de diferentes capítulos y público en general



El webinar abordó la importancia de la seguridad integral y su evolución, la dependencia de las personas con la tecnología y las vulnerabilidades que conlleva tanto en el mundo físico como digital. La seguridad integral es la evolución y fusión del mundo físico y digital para proteger los activos de una organización, en un entorno donde la tecnología desempeña un papel crucial, la seguridad integral abarca la protección de la información, la seguridad informática, la gestión de riesgos y la seguridad física para garantizar la protección integral de una empresa en todos los aspectos. El evento virtual tuvo una asistencia de 100 participantes conformado por miembros de ASIS de diferentes capítulos y público en general

PUBLICACIONES EN REDES

El 21 de abril se realizó el primer 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 264 participantes conformado 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.



El webinar abordó el tema de las estrategias de respuesta, es decir el cómo comunicarse, cómo responder ante los diferentes actores relevantes (medios de comunicación, comunidades, entre otros) durante un incidente de seguridad. El evento virtual tuvo una asistencia de 166 participantes conformado por miembros de ASIS de diferentes capítulos y público en general.

NEWSLETTER

ASIS INTERNATIONAL® | Lima, Peru Chapter

Perú Edición **03/2023**

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

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: