NEWSLETTER

Perú Edición **05/2020**

Editorial

ASIS PERÚ se prepara para celebrar sus 25 años.

Ante la crisis actual ha decidido realizar la Primera Convención ONLINE de Seguridad los detalles en esta edición.

Asimismo, durante este mes continuamos con las actividades de beneficio de nuestros miembros y la comunidad de seguridad.

Incluimos articulos sobre Ciberseguridad, las jornadas de Webinars y el Valor de las certificaciones.

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".

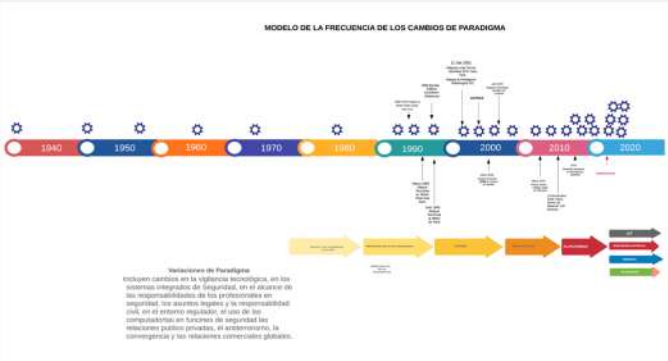
INDICE

INCREMENTO DE VELOCIDAD EN LA FRECUENCIA DE CAMBIO DE PARADIGMAS APLICADOS A LA SEGURIDAD PARA ENFRENTAR RIESGOS DISRUPTIVOS.

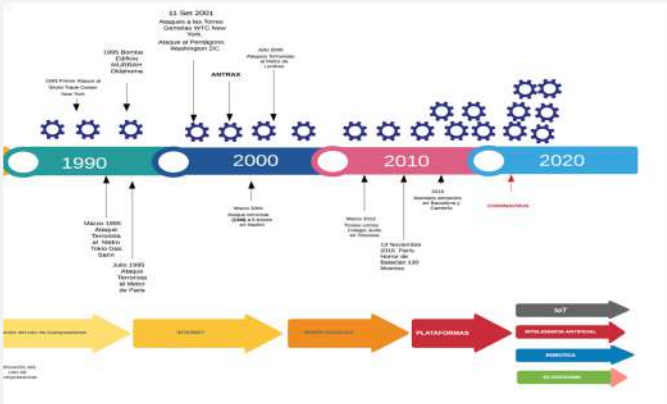
Aldo Schwarz Cossu CPP, DSE
Miembro del Consejo Consultivo ASIS PERÚ
Director en Gestión de Riesgos Corporativos y Director del Instituto de Desarrollo de Competencias en Securitas Perú

He resaltado intencionalmente con rojo las palabras de este título que requieren una dedicación especial ya que estas palabras están siendo muy utilizadas actualmente para explicar y entender comportamientos.

De acuerdo a la RAE el significado de **Paradigma e**s descrito de la siguiente manera: *"Teoría o conjunto de teorías cuyo núcleo central se acepta sin cuestionar y que suministra la base y modelo para resolver problemas y avanzar en el conocimiento"*



La Frecuencia de cambio de Paradigmas obedece al comportamiento relacionado con los grandes cambios o modelos en un período de tiempo. En esta línea de tiempo se han graficado momentos de nuestra historia en donde las circunstancias de momento obligaron a las empresas y a la sociedad a romper los paradigmas existentes y establecer nuevos modelos para enfrentar los momentos.



En el siguiente gráfico se puede observar que a partir de los 90s se empiezan a producir cambios en los paradigmas de Seguridad como consecuencia de la manifestación de nuevas amenazas terroristas principalmente caracterizado por ataques con bombas a los medios de transporte masivo en Europa. En la década del 2000 el evento que rompió muchos paradigmas, principalmente entemas de seguridad fue el ataque del 11 de Setiembre del 2001 a las Torres del WTC de New York y al Pentágono en Washington. Hasta ese momento el Paradigma que imperaba en la sociedad norteamericana se podría resumir en lo siguiente:

La probabilidad de que se secuestre un avión de pasajeros para utilizarlo como misil dirigido contra objetivos estratégicos era impensable.

Las amenazas externas contra los intereses de los Estados Unidos estaban muy bien protegidos por la mejor Fuerza Armada del Planeta.

Cuantas cosas cambiaron después de este Ataque. Todos los cambios que se realizaron demandaron nuevos modelos, nuevos protocolos, nuevas leyes, nuevas condiciones y formas de trabajo, nuevos estándares, integración de esfuerzos entre la Seguridad Privada, la Segurida Pública y las Fuerzas Armadas. La forma de pensar y de hacer las cosas fue diferente a partir de ese año.

En un sentido amplio y centrándonos en el campo de la seguridad, principalmente en América Latina, "El Paradigma" sobre la gestión de seguridad siendo iluminada e inspirada por el *"sentido común"* de los líderes que administran y dirigen los negocios y recurren a profesionales que no se encuentran capacitados ni actualizados con los cambios de paradigmas en el cambio de la seguridad. Esto cambia en el mundo más rápido de lo que parece.

A consecuencia directa de la globalización, la Gestión de Seguridad dejó de ser un asunto que puede manejarse con el sentido común, ahora existen Normas estandarizadas de Gestión, existen, al igual que en el campo de la medicina, los médicos van descubriendo nuevas enfermedades, nuevos tratamientos, nuevas formas de intervenciones quirúrgicas y medicinas y las comparten con sus colegas en simposiums y conferencias. En el campo de la Seguridad Corporativa o Empresarial sucede exactamente lo mismo, las formas y metodologías de identificar y evaluar los riesgos, la implementación de nuevos modelos de gestión, con nuevos conceptos, nuevos criterios que son actualizados constantemente, estos nuevos conocimientos son evaluados y analizados y luego de pasar por filtros de críticas constructivas son documentadas y compartidas a través de instituciones renombradas conformadas por profesionales en el campo de la Seguridad Empresarial como en el caso de ASIS International, organización a la cual pertenezco desde hace 27 años y he podido ser testigo de los cambios y actualizaciones, que van mucho más allá del simple uso del sentido común.

INCREMENTO DE VELOCIDAD EN LA FRECUENCIA DE CAMBIO DE PARADIGMAS APLICADOS A LA SEGURIDAD PARA ENFRENTAR RIESGOS DISRUPTIVOS.

"El cambio de Siglo y las circunstancias relevantes a nivel global en el campo de la seguridad nos está forzando a romper Paradigmas".

El cambio de Siglo y las circunstancias relevantes a nivel global en el campo de la seguridad, El Terrorismo Internacional, Los Cyber Ataques, Las Fuerza Politicas que buscan cambiar los Sistemas económicos, La Corrupción, La Inmigraciones masivas, La Delincuencia Organizada, etc. están forzando a la humanidad a romper los paradigmas que nos dominaban, es decir, se ha obligado a cambiar las formas así como la gestión de los riesgos, debiendo pensar en diferente forma para enfrentar las nuevas amenazas.

Los seres humanos preferimos mantener nuestra actitud frente a los riesgos dentro de una zona de comfort sin percatarnos de la evolución de amenazas en nuestro entorno.

Lamentablemente tenemos que recibir un input muy fuerte para ***reaccionar***, siendo la reacción, en la mayor cantidad de veces tardía, por no haber estado preparado, por que nunca se lo imaginaron y esta reaccción termina siendo mal implementada, con consecuencias y pérdidas muy grandes. .

El cambio en las tendencias de la gestión de seguridad del modo reactivo al modo predictivo

El nuevo siglo ha ido cambiado la tendencia en el campo de seguridad de los negocios transformándose del MODO REACTIVO muy popular en las últimas cuatro décadas del siglo XX, pasando por el MODO PROACTIVO que se implementó inmediatamente después del ataque al World Trade Center en el año 2001 y se empezó a hacer muy común el término "*Riesgo de carácter Disruptivo"*. Una década después fueron desarrollándose modelos para el cambio al nuevo MODO PREDICTIVO; es decir, monitoreo permanente del entorno, no solo para efectos de mitigación de los riesgos sido para enfrentarlos en forma efectiva y eficiente, tratando de evitar que el riesgo se materialize ó para minimizar las pérdidas, garantizando la continuidad de los negocios si en caso el riesgo es inevitable.

La Tecnología.- ¿Es realmente la solución a los Problemas?

Venimos siendo testigos de la evolución del empleo de la tecnología para la solución de los problemas de seguridad, no obstante la aceptación de nuevas tecnologías aun es considerado más un gasto que una inversión, basando siempre estas decisiones en el mismo paradigma que nos resistimos a romper.

La Pandemia generada por el CORONAVIRUS ha sido la manifestación de un "Riesgo de carácter Disruptivo" que pese a que desde el año 2015 se había anunciado e identificado la potencialidad destructiva, fue consideraba con muy poca probabilidad de ocurrencia y no se habría tomado en cuenta que su aparición podría haber producido grandes consecuencias a la humanidad tanto en vidas humanas como económicas. Una vez más estamos siendo forzados a romper paradigmas o romper las teorías y los modelos y hacer las cosas de otra forma. Lo que se ha podido ver en esta desesperación por establecer nuevos modelos aplicando una vez más el sentido común. Los fabricantes y comercialzadores de equipos electrónicos han buscado la oportunidad para hacer las ventas de su vida, muchas veces atribuyendo soluciones tecnológicas de alto costo que al final solo satisfacen una parte de la solución de los problemas y que luego de adquirirlos e implementarlos se evidencia que no era la solución.

De la misma manera que en el campo de la medicina, imáginemos una gran amenaza a la dentadura de los ciudadanos de una localidad, el gremio de dentistas de esta localidad se encuentran tan desactualizados que aun conservan la costumbre de emborrachar a los pacientes para extraerles los dientes, y el único tratamiento a las afecciones dentales que conocen es la extracción de las piezas dentales; sin embargo con esta prácticas le ha funcionado su oficio, han solucionado los dolores de dientes y muelas y no se han visto obligados ni forzados por nadie para hacerlo de otra manera.

Es evidente conocido que existen nuevos modelos y teorías en la medicina dental, nuevos protocolos, herramientas, medicinas y tratamientos que se aplican en un mundo que se encuentra mucho más avanzado que evita la extracción como primera y única solución. En esta imaginaria pequeña localidad que está pasando por una situación que ataca a los dientes, ¿Cual sería la capacidad de planificar y establecer los requerimientos para la solución de esta gran afección que los abruma? .

Aparecen vendedores de equipos de todo tipo, dentro de ellos vendedores de Tomografía Axial Computarizada y ofrece sus mejores equipos para evaluar todo el cuerpo humano y también la dentadura de los pacientes. Nunca en estas etapas de convencimiento se comentan los costos de mantenimiento preventivo ni correctivo tampoco de los costos de los repuestos ni de la capacitación para su operación.

INCREMENTO DE VELOCIDAD EN LA FRECUENCIA DE CAMBIO DE PARADIGMAS APLICADOS A LA SEGURIDAD PARA ENFRENTAR RIESGOS DISRUPTIVOS.

Aparecen vendedores de equipos de todo tipo, dentro de ellos vendedores de Tomografía Axial Computarizada y ofrece sus mejores equipos para evaluar todo el cuerpo humano y también la dentadura de los pacientes. Nunca en estas etapas de convencimiento se comentan los costos de mantenimiento preventivo ni correctivo tampoco de los costos de los repuestos ni de la capacitación para su operación.

Existen dos posibilidades: Que se compre el Tomógrafo y que al final no les resuelva el problema y segundo que no compre nada por el precio.

Las atribuciones del equipo de Tomografía Axial Computarizada seguramente les resolvería el problema de los dentistas; sin embargo no se percataron, por ignorancia, de existía un equipo de rayos X de uso dental, que les hubiera permitido resolver el problema a un menor costo y cada dentista tendría uno en su consultorio.

En el campo de la Seguridad las teorías, los modelos y las formas ya existen, solo tienen que abrirse las mentes para entenderlas y ponerlas en práctica.
Para empezar, en nuestra cultura empresarial se deben de romper tres paradigmas fundamentales:

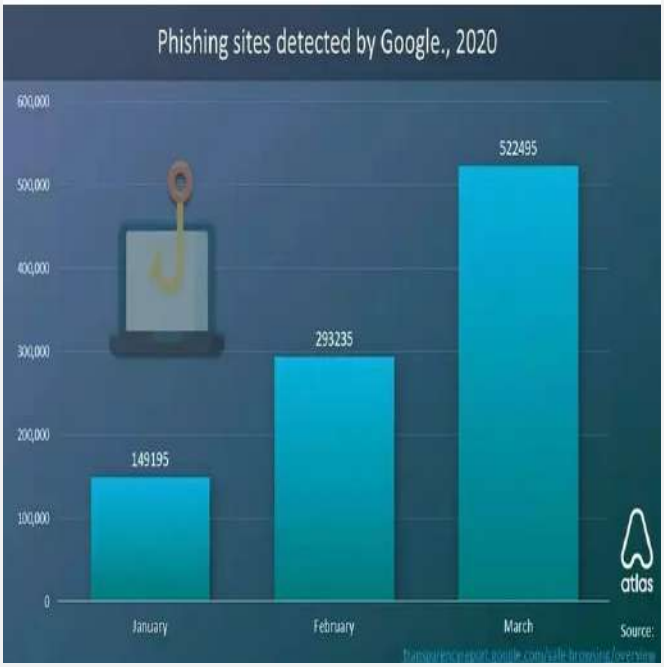
PARADIGMA Nº 1
"El profesional retirado de las Fuerza Armadas y/o Fuerzas Policiales con los conocimientos y experiencias adquiridas mientras vistieron uniforme obedecía a un Perfil requerido por las empresas en el siglo XX, lamentablemente estos conocimientos ya no son eficaces tampoco eficientes ni suficientes para administrar los nuevos riesgos del Siglo XXI"
Existen nuevos modelos, nuevos criterios, nuevos conceptos que se han ido desarrollando en los últimos 20 años que necesariamente requieren ser aprendidos y que van a diferir de lo aprendido en las Fuerza Armadas o Fuerzas Policiales, Los Oficiales estarán obligados a desaprender lo que conocían y adquirir nuevos conocimientos acerca de la gestión de seguridad moderna en el campo empresarial y hacer un esfuerzo personal en mantenerse actualizado. Si el profesional que hace gestión de seguridad hoy en día no está preparado y certificado en sus conocimientos las probabilidades de agregar valor en su gestión son casi nulas y lo mas peligroso es que se convierta en una potencial vulnerabilidad para su organización.

PARADIGMA Nº 2
"La nueva tecnología per sé por más desarrollada que sea no resolverá los problemas de seguridad de una empresa o corporación si no se cumple con satisfacer los requerimientos específicos para la solución de un problema tanto en efectividad como en eficiencia."
La Tecnología es un elemento de soporte ó apoyo a la gestión de seguridad. La calidad técnica de las personas que hagan uso de la tecnología deberán estar calificados.
Para hacer el diseño de un modelo de Seguridad que sea eficaz y eficiente se requerirá primeramente desarrollar un diagnóstico, identificando las amenazas, las vulnerabilidades los riesgos, la probabilidad de ocurrencia, cuantificar las pérdidas en caso de que los riesgos se manifiesten y una vez aceptados estos estudios asesorar en la toma de decisiones para definir las formas en que se gestionarán cada uno de los Riesgos, esto en función del calculo de pérdidas esperadas, probabilidad de ocurrencia, vulnerabilidades, costo de la implementación y la tasa de Rotorno de la Inversión. Luego de tomadas estas decisiones el Profesional de Seguridad hará uso de sus conocimientos actualizados para desarrollar los controles a través de un Plan de Protección a la medida que deba integrar tres grandes elementos:
Politicas, Procedimientos y Protocolos.
Personal seleccionado capacitado y entrenado en forma permanente.
Tecnología específica para el monitoreo de los agentes de riesgo identificados, que puede ser detección de conductas, desviaciones en el cumplimiento de políticas y protocolos del sistema de Protección, registro de datos que se convertirán en información para la toma de decisiones, etc.
Este Plan de Protección deberá estar perfectamente balanceado en costos versus riesgos y el profesional de Seguridad deberá ser capaz de sustentar tanto el rendimiento operativo del Plan así como la justificación financiera mediante un adecuado "Retorno de la Inversión"

PARADIGMA Nº 3
"El precio más bajo en Seguridad no es necesariamente la mejor decisión."
Debemos estar preparados para entender que las cosas ya no volverán a ser iguales y la forma hacer la gestión de Seguridad será muy diferente a la que hemos estado acostumbrados.
Debemos de prepararnos

3 maneras en la que los gobiernos pueden abordar la ciberseguridad en un mundo post-pandemia

La pandemia de COVID-19 ha incrementado el uso y la dependencia del uso de internet, en la medida que las personas han necesitado trabajar y estudiar desde casa.
Durante la crisis, los ciberataques se han incrementado a nivel mundial.
Los Gobiernos pueden abordar la ciberseguridad en un mundo post-pandemia, si trabajan juntos para ajustar marcos nacionales, aumentan la cooperación internacional y homogenización de las campañas de sensibilización.
La pandemia de COVID-19 ha acelerado la transformación digital y ha aumentado la dependencia en servicios digitales. El incremento del teletrabajo o lo la educación a distancia causado por el "distanciamiento social" generó un incremento del 50% en el tráfico de datos de varios mercados.
Durante esta crisis, los ciberataques se han incrementado a nivel mundial, incluyendo aquellos contra infraestructura critica para instituciones de salud, quienes han sido objetivo de ataques de ransomeware. Datos del sector privado revelan un marcado aumento de 350% en sitios web dedicados al "phishing" desde el inicio de la pandemia. Países como el Reino Unido y los Estados Unidos han informado que un número creciente de ciberdelincuentes y otros grupos maliciosos en línea, están explotando la situación actual para su beneficio personal, y que cibercriminales han usado los paquetes de estímulo como tema de engaños para el "phishing".



De igual modo, el incremento en el uso de herramientas y servicios digitales ha traído una mayor atención de los gobiernos a estos temas. Esto representa una oportunidad para trabajar en las amenazas cibernéticas y unificar esfuerzos que permitan garantizar un internet más abierto, seguro, confiable e incluyente, oportunidad que en otras circunstancias hubiera tomado mucho más tiempo en darse.

A pesar de los actuales desafíos, la comunidad cibernética tiene la oportunidad de trabajar unida para garantizar que la seguridad, la privacidad y los derechos digitales estén garantizados. Aprovechar esta oportunidad necesita que los gobiernos adelanten tres acciones especificas:

1. Ajustar los marcos nacionales

Los países necesitan ser más ágiles para actualizar o desarrollar estrategias nacionales de ciberseguridad, así como su marco legal y regulatorio con respecto al ciberespacio. Estas iniciativas deben tener un enfoque de múltiples partes interesadas, lo que incluye prestar mucha atención a la construcción de capacidades de respuesta a incidentes en todos los sectores. Los gobiernos no pueden actuar solos y la participación de la comunidad técnica y el sector privado son esenciales para desarrollar capacidades efectivas de resiliencia.
La armonización de la legislación también debería ser una prioridad. Hoy, la Convención de Budapest es la convención más global e inclusiva dedicada a la lucha contra la ciberdelincuencia. Ha sido ratificada por 55 países y otros 10 han solicitado su adhesión. La Organización de Estados Americanos (OEA) ya ha recomendado la adhesión a esta Convención, y las organizaciones internacionales y los países deberían considerar este instrumento como un medio para lograr la cooperación internacional inmediata para el intercambio de información y la investigación transfronteriza. Los derechos digitales, los derechos a la privacidad y la libertad de expresión nunca deben olvidarse.

2. Incrementar la cooperación internacional

A medida que el intercambio de información ha aumentado desde que estalló COVID-19, necesitamos mantener este impulso, catalizarlo y formalizarlo en todos los asuntos cibernéticos. La ciberseguridad requiere cooperación internacional, y hay una necesidad de incrementar la confianza, a todos los niveles, entre países e industrias. Mañana habrá un nuevo "virus" o un "enemigo común" en el ciberespacio. Por lo tanto, nuestra colaboración a nivel político, técnico y político será vital para protegernos y permitirnos trabajar juntos para encontrar una solución.

https://es.weforum.org/agenda/2020/06/3-maneras-en-la-que-los-gobiernos-pueden-abordar-la-ciberseguridad-en-un-mundo-post-pandemia/

3 maneras en la que los gobiernos pueden abordar la ciberseguridad en un mundo post-pandemia

Un buen ejemplo de cooperación internacional es la red hemisférica regional CSIRTAmericas: una comunidad de Equipos de Respuesta a Incidentes de Seguridad Cibernética (CSIRT) en el hemisferio occidental. Durante situaciones de crisis como Wannacry, y ahora con la pandemia actual, esta comunidad ha podido reunirse virtualmente para compartir información en tiempo real para intercambiar conocimientos e información y poder abordar los desafíos regionales.

3. Unificar los esfuerzos de sensibilización

Educar, educar y educar.

Nadie es inmune a un incidente cibernético ni a un "mal clic". Debemos aumentar los esfuerzos de sensibilización en todas las edades y niveles, independientemente de la industria. Es de suma importancia comenzar a enseñar a los jóvenes sobre ciberseguridad. En esta era de rápido avance tecnológico, los niños necesitan sumergirse en la tecnología a una edad temprana para comenzar a aprender las habilidades que usarán a lo largo de sus vidas. Sin embargo, deben estar capacitados para aprovechar al máximo esta oportunidad, mientras se mantienen protegidos y conscientes de sus riesgos.

Los gobiernos y el sector privado deben unir esfuerzos y trabajar en campañas de sensibilización unificadas. Iniciativas como “Para. Piensa. Conéctate." pueden servir como línea de base para otras iniciativas. Además, los usuarios nunca deben ser la última línea de defensa en ciberseguridad, ya que también deben desempeñar un rol educativo amplificando el alcance de las campañas de concienciación. La ciberseguridad es una responsabilidad compartida.

También debemos impulsar un enfoque inclusivo de género en los asuntos cibernéticos. Organizaciones como la Comisión Interamericana de Mujeres ya han reconocido los impactos diferenciales de COVID-19 en la vida de las mujeres, incluyendo el aumento de la violencia contra las mujeres y las niñas en Internet. Además, las mujeres están soportando una carga significativa del impacto económico del COVID-19, particularmente en lo que al empleo se refiere. Esto justifica la incorporación de las consideraciones de género en nuestras políticas relacionadas con la ciberseguridad como sector generador de empleo.

A medida que la pandemia de COVID-19 acelera la transformación digital, es esencial que los países revisen su postura cibernética e implementen medidas concretas en un esfuerzo por promover una Internet segura y confiable. Estas tres acciones estratégicas (ajustar los marcos nacionales, incrementar la cooperación internacional y unificar los esfuerzos de sensibilización) deben tomarse como pasos iniciales hacia la construcción de un nivel de confianza digital más fuerte, y así permitir un entorno de ciberseguridad robusto en el mundo posterior a la pandemia.

https://es.weforum.org/agenda/2020/06/3-maneras-en-la-que-los-gobiernos-pueden-abordar-la-ciberseguridad-en-un-mundo-post-pandemia/

WEBINARS


ASIS INTERNATIONAL REGION 8C
WEBINAR
CONFLICTOS SOCIALES
Presentación
Carlos Flores, CPP
RVP Región 8C
05 DE MAYO DE 2020
Argentina 12:00 hrs
Bolivia 11:00 hrs
Chile 11:00 hrs
Paraguay 11:00 hrs
Perú 10:00 hrs
Uruguay 12:00 hrs
Expositores
René Navajas
ASIS Bolivia
Guillermo Holzmann
ASIS Chile
Aldo Schwarz, CPP
ASIS Perú
ACCESO LIBRE
www.asisonline.lat


ASIS INTERNATIONAL REGION 8C
WEBINAR
SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO
Orientación para su Implementación
Presentación
Herbert Calderón, CPP, PCI, PSP
ASIS SRVP Región 8
12 DE MAYO DE 2020
Argentina 12:00 hrs
Bolivia 11:00 hrs
Chile 11:00 hrs
Paraguay 11:00 hrs
Perú 10:00 hrs
Uruguay 12:00 hrs
Expositores
Osmar Florenciañez, CPP
ASIS Paraguay
Carlos Landó, CPP
ASIS Argentina
ACCESO LIBRE
www.asisonline.lat

Ciberseguridad en la red de quinta generación: Promesas increíbles, riesgos importantes

Belisario Contreras
Gerente, Programa de Ciberseguridad, Organización de los Estados Americanos (OEA)
Es miembro del Consejo de la Agenda Global sobre el Futuro de la Ciberseguridad en el Foro Económico Mundial (WEF) y también es miembro de la Universidad de Oxford. En esta capacidad, ha sido un orador frecuente en eventos internacionales y regionales del ciberespacio, prestando atención al impacto específico que estos temas tienen en la región de ALC

Ciberseguridad en la red de quinta generación: Promesas increíbles, riesgos importantes
La tecnología inalámbrica de quinta generación (5G) formará la columna vertebral de las futuras economías y servicios públicos. Las sociedades recientemente interconectadas dependerán críticamente de nuevas aplicaciones innovadoras.
A continuación Resumen de la Publicación del Departamento de Estado de EE.UU.

SEGURIDAD EN LA RED DE QUINTA GENERACIÓN (5G) PROMESAS INCREIBLES, RIESGOS IMPORTANTES

La quinta generación (5G) de la tecnología inalámbrica será la espina dorsal del futuro desrrrollo económico y de los servicios públicos. Las nuevas sociedades que trabajen en redes dependerán críticamente de nuevas aplicaciones innovadoras. Los países deben tomar medidas ahora para salvaguardar sus redes emergentes 5G porque los riesgos no pueden ser más grandes.
MUCHA MÁS VELOCIDAD QUE LOS TELÉFONOS INTELIGENTES
La 5G ha de transformar todos los aspectos de nuestras vidas al permitir el uso de asombrosas nuevas aplicaciones:
Autos, autobuses y trenes autónomos.
Telecirugia que conecta a los cirujanos con los pacientes separados por grandes distancias.
Infraestructura crítica más eficiente, como las redes eléctricas y los sistemas de agua.
Millones de artefactos conectados en red, incluyendo aplicaciones "inteligentes" para los enseres domésticos.
Potenciales usos ilimitados todavía no inventados.

LAS REDES 5G DEBEN SER CONSTRUIDAS CON CUIDADO PARA PROTEGER A LA CIUDADANIA

Para lograr las promesas de la 5G, los países deben tomar medidas ahora para asegurarse de que sus redes 5G serán seguras:

La privacidad se verá amenazada si hay "puertas traseras" intencionales por donde se puedan extraer los datos personales de los ciudadanos.
La seguridad y la salvedad se verán amenazadas si ataques con "interruptores de emergencia" pueden perturbar o apagar las redes 5G.
Los derechos humanos se verán amenazados si hay "ciudades inteligentes" que usen las tecnologías de vigilancia para limitar las libertades personales y señalar a ciudadanos vulnerables.
Las economías se verán amenazadas si los derechos de propiedad intelectual pueden ser robados.
La soberanía se verá amenazada si los países confían en redes controladas por gobiernos autoritarios.

¿EN QUIEN SE PUEDE CONFIAR PARA CONSTRUIR SU FUTURA 5G?

Las normas nacionales para las redes 5G deben tomar en cuenta el país y el modelo de gobierno donde tienen sus sede las empresas de los equipos y los programas informáticos de 5G.
No puede haber confianza cuando los vendedores están sometidos a manipulaciones secretas por un gobierno autoritario como el de la República Popular China, que carece de un poder judicial independiente y de un estado de derecho que impida el uso incorrecto de los datos.
Nuestros expertos técnicos consideran que ningún arreglo técnico pueda mitigar los riesgos generales de permitir los equipos de Huawei y ZTE en cualquier lugar de la infraestructura de la red 5G.
Ericsson (de Suecia), Nokia (de Finlandia) y Samsung (de Corea del Sur) tienen equipos excelentes y costos competitivos y no están sometidos al capricho de regímenes autoritarios.

ESTADOS UNIDOS APOYA UN FUTURO DE 5G SEGURO PARA TODOS

Acogemos favorablemente la colaboración con asociados y aliados para garantizar nuestra seguridad compartida en un futuro de 5G.
Permitir a equipos de compañías de China en cualquier lugar de la red 5G crea riesgos inaceptable: para la seguridad nacional, la infraestructura crítica, la privacidad y los derechos humanos.
Hemos tomado medidas para permitir el acceso solo de equipos confiables en todos los componentes de la red 5G.
Estados Unidos reconsiderará cómo interconectarse y compartir información con países que tengan comprometida su seguridad en la red 5G.

https://www.asis.org.pe/blog/item/156-gestion-de-riesgos-ante-el-covid-19

WEBINARS

19 al 22 de Mayo de 2020

ACCESO LIBRE

zoom

Martes 19 May

ASIS INTERNATIONAL | ASIS Buenos Aires, Argentina Chapter

ASIS INTERNATIONAL REGION 8C

WEBINAR - Elaboración de Planes de prevención de Seguridad de la Información en redes sociales y para el trabajo remoto.

Martes 19 de mayo
Argentina: 18:00hs
Bolivia: 17:00hs
Chile: 17:00hs
Paraguay: 17:00hs
Perú: 16:00hs
Uruguay: 18:00hs

Presentación: Lic. Ali Ferrer, PSP, CPP

Oradoras:

- Esp. Ing. Cintia Gioia. Ing. en Informática. Especialista en Criptografía y Seguridad Teleinformática (EST).
- Roxana Dominguez Fundadora de Mamá en Línea ONG

ACCESO LIBRE

asisonline.org | ASIS

Miércoles 20 May

ASIS INTERNATIONAL Latin American Advisory Council

LOS INVITA AL WEBINAR GRATUITO DENOMINADO:

"APRENDIZAJES DE LA PANDEMIA COVID-19 PARA LAS EMPRESAS DE SEGURIDAD PRIVADA"

CON LOS SIGUIENTES PANELISTAS:

TATIANA SCATENA | G4S | RVP ASIS INTERNACIONAL REGIÓN - BA BRASIL
ALEX OMAR GARRIDO, CPP | PROTEGER S.A PANAMÁ | ARVP REGIÓN 7C. PANAMÁ
CARLOS FLORES, CPP | DIRECTOR GENERAL VISEPORT | RVP ASIS INTERNACIONAL REGIÓN 8C. URUGUAY.
JOEL JUÁREZ BLANCO PRESIDENTE DE LA ASOCIACIÓN MEXICANA DE EMPRESAS DE SEGURIDAD PRIVADA AMESP. MÉXICO

MODERA: ARMANDO ZÚÑIGA, CPP. PRESIDENTE GRUPO IPS. MIEMBRO ASIS INT CAPÍTULO 217 MÉXICO.

MIÉRCOLES 20 DE MAYO DEL 2020
09:00 HORAS (CENTROAMÉRICA)
10:00 HORAS (PANAMÁ/PERÚ/CIUDAD DE MÉXICO)
12:00 HORAS (BUENOS AIRES/SAO PAULO)

INSCRIPCIONES EN WWW.ASISONLINE.LAT

Jueves 21 May

ASIS INTERNATIONAL Perú Chapter | Organiza: Comité Women In Security (WIS)

WEBINAR
LA INTELIGENCIA EMOCIONAL Y SU IMPORTANCIA EN EL CAPITAL HUMANO

Expositora

Ana Rocio Sabogal Henao
Presidenta
Grupo Altum

21 DE MAYO DE 2020
HORA: 04:00 PM

Moderadora

Milagros Céspedes Álvarez
Directora General de CES
WIS LATAM & WIS Liason Perú

Expositor

Jorge Castro
Gerente de Seguridad
REPSOL – Perú

ACCESO LIBRE

www.asis.org.pe

Viernes 22 May

BENEFICIOS DEL EMPLEO DE DRONES EN APOYO A LA EMERGENCIA SANITARIA

EXPOSITORES:

WEBINAR

Camilo Mendoza Arango
(OFICIAL FAC)

Marco Antonio Garrido Smith
(CPP, MBA, CSSO)

Organiza: ASIS INTERNATIONAL REGION XIII

ACCESO LIBRE zoom

22 de Mayo

10:00 (Hora Ecuador)

www.asis.org.pe

El valor de las certificaciones y estándares de ASIS International para tu actividad

El valor de las certificaciones y estándares de ASIS International para tu actividad

En nuestras organizaciones muchas veces en forma diaria a través de comentarios, reuniones, sanciones, despidos, nos enteramos de problemas como: el empleado no cumple el perfil, el gerente no sabe desempeñarse en sus funciones, las ventas han disminuido, se hizo un mal mantenimiento a la maquinaria, el sindicato esta desmedido en su comportamiento, los accidentes no han disminuido, conflictos legales, auditorías con observaciones, incendios, robos, fraudes, interrupción del negocio.

Lo comentado anteriormente son problemas muchos de ellos cotidianos, comunes en una organización, que muchas veces pasan desapercibidos, los denominan problemas del "día a día". Sin embargo, estos problemas pueden descontrolarse y llegar a dañar a un proceso o en general a la organización, si es que no se intervienen en su momento. La gran pregunta sería: ¿quién debería intervenir en corregir, evitar, prevenir, medir?

La respuesta es que la misma organización debería tener una visión holística de los problemas y/o errores, esto significa que una situación así debería, ser tomada preventivamente y corregida antes que ello dañe el proceso y sea irrecuperable. Esta madurez de la organización en prevenir sus problemas está en el campo de la cultura que la organización posee. En nuestro caso, muchas veces somos participes de dichos reportes de fallas en el proceso en la cual en todos los casos interviene el ser humano. Y como gestores debemos ser conscientes de que las personas pueden equivocarse. Respecto a ello el error humano puede ser visto de dos formas: el enfoque personal y el enfoque sistémico. Cada enfoque representa un modelo de la causa del error y cada modelo genera dos filosofías claramente diferentes de la gestión del error.

muchas veces no sabemos a donde recurrir u orientarnos.

Mientras que el enfoque personal se centra en el error individual, reprochando a las personas su olvido, falta de atención o debilidad moral, el enfoque sistémico reconoce que la variabilidad humana es un aspecto que se debe contener para evitar los errores. En este enfoque, las organizaciones altamente confiables, cuyos índices de accidentes y errores son muy inferiores al promedio de la industria a la que pertenecen, trabajan fuertemente para reducir esa variabilidad. Para mejorar los procesos, de nada sirve el enfoque personal, porque no es factible cambiar la naturaleza humana, y es preciso entonces actuar sobre el sistema.

Se ha estimado que el 91 % de estos incidentes son causados por errores humanos. De ahí la importancia de reducir estos errores y como consecuencia abatir estos desagradables costos.

Los problemas cotidianos comentados anteriormente evidencian:

Malos procedimientos de incorporación de funcionarios.

Mala comunicación organizacional.

Ausencia de controles de funcionamiento o mantenimiento de la ingeniería. Errores en la gestión de seguridad industrial.

Fallas en la gestión legal.

Falta de controles en los estándares normas ISO.

En todo este análisis observamos fallas de los procesos, así como fallas humanas, está en la organización trabajar arduamente en minimizar estos aspectos desde la creación de la conciencia y con ello corregir los errores en todo sentido sin minimizarlos y evitar consecuencias catastróficas. Existe un recurso que muchas veces olvidamos: que es el conocimiento, las experiencias de otros profesionales, así como de la forma de cómo solucionaron sus problemas críticos, en industrias similares a las tuyas o mas complicadas y peligrosas.

Este compendio de conocimientos se encuentra muy bien desarrollado en las guías, estándares y a través del proceso de obtención las certificaciones de ASIS Internacional.

Estos documentos y requisitos de obtención de las certificaciones están escritos y diseñados en base al conocimiento, experiencias, buenas prácticas para la solución de problemas, y ejemplos de procesos que muchas veces no sabemos a donde recurrir u orientarnos.

CONVENCIÓN ONLINE DE SEGURIDAD

ASIS INTERNATIONAL Perú Chapter 25 AÑOS

by zoom

18 Y 19 DE JUNIO 2020

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.

ASIS PERÚ comprometido con la profesionalización de la Seguridad propone es esta oportunidad abordar los temas de Privacidad de Datos, Gestión del Fraude, Cultura de Seguridad y el Valor de las Certificaciones en la Gestión Empresarial.

Jornada de dos días dedicada también a la integración en nuestra región.

Nuestro compromiso, seguir fortaleciendo la Cultura de Seguridad.

NEWSLETTER

Perú Edición **05/2020**

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: