ASIS INTERNATIONAL
CAPÍTULO MÉXICO 217

Reunión Mensual

JUNIO 2022

Fecha: 7 de Junio 2022.
Plataforma ZOOM.
Patrocinador: Grupo PAPRISA.
Asistentes: 98.

ASIS Capítulo México llevó a cabo su sexta reunión mensual del año, comenzó con las palabras de Manuel Zamudio, coordinador de la comunidad ITS quien leyó el código de ética de los miembros de la asociación de profesionales de la seguridad. Se dio la bienvenida a los nuevos socios y se les invitó a que se unieran a las comunidades de ASIS.

A continuación, se presentó a Jimena Bernal, Directora de Comunicación y Marketing de Grupo PAPRISA, con 22 años de experiencia. Son una de las empresas líderes en SEGURIDAD PRIVADA en México.
GRUPO PAPRISA está integrado por diez empresas, todas orientadas a ofrecer las mejores soluciones de seguridad y protección.
Garantizan la continuidad de tu negocio a través de sus servicios, tecnologías y sistemas innovadores.

Se presentó a los panelistas Gigi Agassini, Alberto Friedmann, Fernando Gómez, CPP, Víctor Martínez, Eduardo Zepeda y moderador Manuel Zamudio con el Panel "Convergencia de: Planes de Continuidad, Comité de Crisis y Ciberataques".

Comenzó Víctor Martínez comentando que la convergencia son las funciones de gestión de seguridad, riesgo que trabajan juntas sin problemas para abordar la seguridad de manera integral y cerrar las brechas y vulnerabilidades que existen en los espacios entre funciones.
La convergencia esta enfocada en unir la seguridad física, seguridad corporativa área de TI y la continuidad de los negocios.

Gigi Agassini, CPP comentó que uno de los grandes riesgos que aumento 14 mil % fue el phishing del 2018 al 2019, sin embargo hoy los expertos dicen que los crímenes cibernéticos para el 2022 como numero 1 esta el ransomware, 2trabajo remoto, 3 business email compromise, 4 amenazas internas.

En México apenas 3 de cada 10 empresas se han digitalizado, es muy importante considerar todos los riesgos que hoy afectan la continuidad de negocios y las distintas variables que tenemos que revisar en el análisis de riesgo para las empresas. Incluso el riesgo de contar con personal que aún no brinca a la transformación digital debe ser considerado para lograr su inserción a esta nueva realidad con buenas prácticas.

Fernando Gómez compartió el tema de "Comité de Crisis" en general, lo conforman: el presidente de la compañía, un técnico del área jurídica, el responsable del área de personal, el responsable de comunicación, un técnico del área afectada y una secretaria. El número de integrantes es variable, y dependerá de la gravedad de la crisis.

La mayoría de las empresas, sin importar su tamaño, tienen un equipo de confianza que se reúne y toma decisiones ante determinados temas o problemas que puedan surgir. Ese equipo se denomina comúnmente Comité de Crisis y es una institución dentro de la organización, conformada por un grupo de personas previamente definidas, cuya principal finalidad es la de actuar rápida y efectivamente frente a una situación que afecte a la compañía. Su objetivo principal es detectar y gestionar el conflicto hasta darle una resolución.

El Ing. Alberto Friedmann como experto en sistemas recomendó visualizar la vulnerabilidad de los sistemas de información y aplicativos de software.
Las amenazas, en un entorno dinámico de interconectividad, pueden venir de cualquier parte, sea interna o externa, e íntimamente relacionada con el entorno de las organizaciones. Las vulnerabilidades son una debilidad en la tecnología o en los procesos asociados con la información, y como tal, se consideran características propias de los sistemas o de la infraestructura que lo soporta.
Para mantener un cierto grado de protección de la información conectada a la red, las organizaciones, entidades y personas en general, deben comprender que su seguridad, y las formas en que esta se trata de vulnerar, mejoran constantemente; por tanto, lo principal y primero es entender cómo pueden sucederse estos ataques y en qué consisten dichas amenazas, con el fin de poder remediarlas de la mejor forma posible.

Finalmente Eduardo Zárate compartió que una de las mejores maneras de proteger tus datos es haciendo una copia de seguridad. De esa manera, si eres víctima de algún robo o le sucede algo a tu ordenador, tendrás una copia duplicada de todo. Recuerda que debes realizar una copia de seguridad regularmente. También puedes configurar el equipo para que se actualice de forma automática.
Una empresa que mantiene a salvo su información sensible cuenta con una buena reputación sobre los competidores, por este motivo es importante la seguridad de la información.