NEWS ADSI FLASH
www.adsi.pro

Índice

Próximo Martes con... La Seguridad Portuaria

Ponencia a cargo de

Bernat Baró i Casanovas

Director de Seguridad Corporativa del Port de Barcelona

La Seguridad Corporativa del Puerto

Nuestros Patrocinadores

Próximo Martes con... La seguridad Portuaria

Martes 16 de octubre a las 19:00 horas

Sala Port de Barcelona en World Trade Center, Terraza 1ª planta edificio norte – Moll de Barcelona

El próximo martes 16 de octubre a las 19:00 horas celebramos un nuevo martes con... En esta ocasión bajo el título "La Seguridad Portuaria" a cargo de Bernat Baró i Casanovas, Director de Seguridad Corporativa del Port de Barcelona.

La ponencia tendrá lugar en la Sala Port de Barcelona sita en el World Trade Center, Terraza 1ª planta edificio norte del Moll de Barcelona a las 19:00 horas, se ruega puntualidad, la recepción se llevará a cabo a partir de las 18:00 horas.

Bernat Baró nos dará un repaso por la historia del Port de Barcelona ofreciendonos datos geográficos de actividad y económicos. Nos hablará de su hubicación estratégica, del movimiento de mercancías y de pasajeros.

Nos adentrará en el modelo de seguridad basado en circulos concentricos, sobre las distintas zonas portuarias, públicas, semi restringidas y restringidas, así como sobre las medidas de Seguridad y Protección, control de pasajeros y control de equipajes.

Nos explicará como está organizada la Seguridad del Port de Barcelona, que prioridades tienen, que tipos de delitos persiguen, cual es la separación organizativa de funciones.

También nos hablará sobre la Seguridad Corporativa Portuaria del S. XXI, depenencias orgánicas, dependencias funcionales, como está constituido el Comité Consultivo de Proteción Portuaria.

Nos explicará el trabajo de los cinco cuerpos policiales presentes en el Port de Barcelona, cuales son las competencias de cada uno de ellos.

Y finalizará con un repaso sobre normativa portuaria. En definitiva una interesantísima ponencia y una oportunidad única de ver como se trabaja en uno de los puntos estratégicos de la ciudad.

Bernat Baró i Casanovas es Director de Seguridad del Port de Barcelona desde noviembre de 2012, anteriormente fue Comisario de Barcelona del Cos de Mossos d'Esquadra.

Durante su larga trayectoria profesional ha acumulado numerosas condecoraciones y distinciones, como la Medalla de Honor al Mérito Policial en la categoría de Plata por su colaboración con la Guardia Urbana o la Cruz Blanca de Honor al Mérito Policial con Distintivo Verde por su colaboración con el Cuerpo Nacional de Policía. También ha sido condecorado con la Medalla del Institut de Seguretat Pública de Catalunya por su colaboración e investigación científica en el ámbito de la Seguridad.

Fue Vicepresidente de la Asociación Catalana de Criminólogos, Coordinador de Área de los World Police Games organizados en Barcelona y Presidente de la Asociación Profesional de la Escala Superior de Mossos d'Esquadra entre otros.

Ha publicado distintos artículos y a realizado numerosas comparecencias en medios de comunicación de TV y Radio.

- Para la buena organización del evento, será imprescindible **confirmación previa de asistencia**, para ello se deberá enviar un e-mail a secretario@adsi.pro con copia a tesoreroadsi@adsi.pro anotando en Asunto *"Asistencia Martes con... 16 de octubre"*.

Cena anual de ADSI 2018

Jueves, 22 de noviembre, 20:00 horas.
Hotel Fairmont - Rey Juan Carlos I Barcelona

Av. Diagonal, 661-671 Barcelona 08028

El jueves 22 de noviembre, un año más, **ADSI** celebrará el evento de mayor relevancia de nuestra Asociación, la **Cena Anual de ADSI**.

La **Cena Anual de ADSI** se constituye como el mayor punto de encuentro de **socios, patrocinadores** y amigos de nuestra Asociación.

En el transcurso de la Cena se efectuarán los siguientes actos:

- Entrega de los **Premios ADSI 2018**
- Discurso del **Presidente de ADSI, Don. Francisco Poley**

Durante la cena dispondremos de un espacio donde charlar relajadamente para comentar nuestras experiencias de este año y los planes de futuro para el siguiente.

Para evitar que el control de acceso al acto pueda retrasar el inicio de los mismos, os rogamos la máxima puntualidad. El mostrador de acreditaciones se abrirá a las 19:30 h, media hora antes del comienzo del aperitivo.

Precios de asistencia a la Cena Anual 2018:

- **Socio de ADSI** **60,00 €**
- **No Socios de ADSI** **85,00 €**

INSCRIPCION DE SOCIOS A LA CENA ANUAL

Rogamos a todos los socios de **ADSI** que deseéis asistir a este importante evento de nuestra Asociación, nos lo comuniquéis antes del **18 de NOVIEMBRE**.

Para ello pulse en INSCRIPCION y rellene el formulario que aparece:

INSCRIPCION

Seguidamente recibirán un mail de confirmación.

Como siempre, emitiremos el correspondiente cargo por el evento para facilitar los trámites a nuestros asociados.

INSCRIPCION DE NO SOCIOS Y EMPRESAS A LA CENA ANUAL

Aquellas personas, profesionales, amigos o acompañantes que no sean Socios de **ADSI**, así como empresas que deseen asistir a **la Cena Anual**, **pueden dirigir su petición de reserva de plaza, o de mesas por parte las empresas, hasta el 18 de NOVIEMBRE**, a los correos electrónicos:

Luis Gomez: secretario@adsi.pro
Elvira Marquez: tesorero@adsi.pro

Indicando en el asunto del correo *"Cena Anual ADSI 2018"* y adjuntando el correspondiente justificante del pago del importe de la cena.

El pago deberá realizarse a la siguiente cuenta bancaria de la Asociación:

CAIXA D'ENGINYERS ES56 3025 0004 3314 3323 5294

Indicando como referencia ***Inscripción cena Anual ADSI 2018***, haciendo constar nombre y apellidos de las personas inscritas, o bien el número total de plazas reservadas, cuando se trate de empresas que todavía no conozcan los datos de sus invitados.

Premios ADSI 2018

Luis Gómez
Secretario ADSI

El día **1 de octubre** se inició el plazo de presentación de candidaturas para los **Premios ADSI 2018** que anualmente concede la **Asociación** con motivo de su Asamblea General Ordinaria y Cena anual.

Los **Premios ADSI** pretenden, de conformidad con lo establecido en el **Reglamento de los Premios ADSI**, el reconocimiento público de aquellas personas o entidades, privadas o públicas, nacionales o internacionales, relacionadas con la Seguridad Privada y Pública, cuya actuación se haya hecho merecedora de dicha distinción, y que se hayan destacado por:

- Orientar sus acciones y esfuerzos a fomentar o divulgar la seguridad,
- El conjunto de su trayectoria profesional,
- Haber realizado algún hecho o actuación relevante que, desde el punto de vista de los valores humanos, esté relacionada con la Seguridad durante el período de valoración de los premios.

Se distinguen las tres especialidades siguientes:

- Premio **ADSI** en **"Agradecimiento a la tarea en favor de la Seguridad"**.
- Premio **ADSI** en **"Reconocimiento a la trayectoria profesional"**.
- Premio **ADSI** a los **"Valores humanos relacionados con la Seguridad"**.

El **Reglamento de los Premios ADSI** establece que:

- El plazo de presentación de Candidaturas será del 01 al 31 de octubre,
- Que en los Premios a los "Valores humanos relacionados con la seguridad" sólo se valorarán por el Jurado hechos o actuaciones acaecidas en la anualidad anterior al inicio del plazo de candidaturas con la excepción que si durante el periodo de presentación se produjeran actuaciones relevantes que podrán también ser presentadas al objeto de no demorar un año su posible reconocimiento y perder así la inmediatez del valor de la misma,
- Que las candidaturas pueden ser propuestas por:

  - La Junta Directiva de **ADSI**.
  - Expresidentes de **ADSI**.
  - Defensor del Socio.
  - Los socios de **ADSI**, con el soporte expreso de un mínimo de 4 asociados.

Las candidaturas propuestas por los Socios de **ADSI** deben documentarse mediante escrito-propuesta, dirigido al Secretario de **ADSI** (secretario@adsi.pro), adjuntando la relación (nombre, apellidos y DNI) de los Socios que avalan la propuesta, haciendo constar el nombre, apellidos, teléfono y dirección de correo electrónico del "Socio portavoz de la propuesta".

Toda candidatura detallará los datos de identificación y contacto de los candidatos presentados y el premio al que se presentan, así como la descripción de los méritos en que se sustenta la candidatura.

Han de presentarse tantos documentos individuales como candidaturas deban ser evaluadas por el Jurado, no aceptándose ninguna propuesta que contenga múltiples aspirantes a los premios.

Los **Premios ADSI** serán entregados en el transcurso de la **CENA ANUAL DE ADSI** que tendrá lugar el próximo 22 de noviembre.

El objetivo de los **Premios ADSI** es buscar el reconocimiento público de los premiados cuya actuación se haya hecho merecedora del premio, por ello os invitamos a que nos hagáis llegar todas aquellas candidaturas que consideréis meritorias de reconocimiento para su valoración por parte de **Jurado de los Premios ADSI.**

Las candidaturas deberán enviarse entre el 01 y el 31 de octubre. Transcurrida dicha fecha no se aceptará candidatura alguna.

Adjuntamos archivo del Reglamento de los Premios **ADSI**

Puerto de BCN, Maersk... Una oleada de ciberataques "estratégicos" golpea Catalunya

Fuente: El Confidencial
Mercè Molist

Las redes informáticas del puerto de Barcelona sufrieron hace unos días uno de los ciberataques más virulentos que se recuerdan en años y del que apenas se han ofrecido detalles. Este dejó KO a la red corporativa del puerto, que tardó al menos seis días en recuperarse. La ola del tsunami alcanzó a algunas de las empresas que trabajan con el puerto, como la naviera danesa Moller-Maersk. Otras empresas de la ciudad cayeron también bajo ataques similares e incluso a los Mossos d'Esquadra se les cayó la red, aunque desde este cuerpo de fuerzas de seguridad aseguran que se trató de una incidencia aislada. Fuentes conocedoras del caso del puerto de Barcelona han confirmado a Teknautas que se trató de un ciberataque con 'ransomware'. Exacto, el mismo tipo que Wannacry, el mayor ciberataque a nivel mundial que se recuerda de este tipo y que tumbó miles de empresas en todo el mundo.

Los virus 'ransommware' cifran el contenido de los ordenadores que infectan y piden un rescate para descifrarlo. Si la empresa afectada tiene copias de seguridad, el incidente se reduce a reinstalar sistemas y las copias. Sin embargo, cuando el número de ordenadores afectados es importante, esta tarea puede alargarse en el tiempo.

Esto es lo que habría pasado en el puerto de Barcelona, donde un número indeterminado de servidores quedaron inutilizados por un ataque que se detectó la madrugada del día 20 de septiembre. La organización insiste en que las operaciones portuarias no se vieron afectadas, pudiendo los buques entrar y salir del puerto sin problemas, pero la operativa de carga y descarga se tuvo que realizar de forma manual. El puerto es una de las infraestructuras estratégicas de la ciudad. Estos puntos son precisamente los más buscados por los 'hackers' para lanzar sus ataques.

Medios especializados en logística y puertos como "El Vigía" relatan un panorama más dantesco para las oficinas del puerto, donde las comunicaciones con el exterior se cortaron, obligando al personal a utilizar medios de comunicación alternativos, como el correo particular o WhatsApp, dado que el correo corporativo no funcionaba.

Fuentes oficiales del puerto de Barcelona han confirmado a Teknautas que el correo interno estuvo varios días inoperativo a causa del incidente. También han mencionado la existencia de servicios que seguían sin funcionar pasados cinco días del ataque porque, aseguran, había "ficheros encriptados". A la pregunta de si el ciberataque se debió a un ransomware, la responsable aseguró que no podía "ni desmentirlo ni afirmarlo".

Según los expertos consultados por Teknautas, la teoría del 'ransomware' como arma del ataque es la que tiene más fuerza, vista la lenta recuperación de los sistemas informáticos de las oficinas. Si hubiesen sufrido un bombardeo o ataque de Denegación de Servicio (DDoS), la recuperación habría sido más rápida, afirma el experto en ciberseguridad Miquel Colobran.

La línea del tiempo del ataque podría haber sido, según Colobran, la siguiente: el 14 de septiembre se puso en marcha una nueva plataforma digital dentro de la web del puerto, PierNext. "Esta plataforma podría tener un agujero de seguridad por el que habría entrado el 'ransomware'", afirma el experto.

El 18 de septiembre, dos días antes de descubrirse el ataque, el puerto promocionaba desde su cuenta en Twitter un artículo premonitorio aparecido en la plataforma PierNext y titulado: "¿Están los puertos preparados para manejar ataques de hackers?". Colobran opina que cuando se publicó este artículo, el virus ya habría entrado y estaría propagándose por los sistemas informáticos del puerto. En el artículo, el Responsable de Seguridad de Información del puerto, Cristian Medrano, afirma: "En algún momento, tu organización sufrirá un ataque que tendrá éxito".

Pero el ataque de hace unos días no se habría quedado solo en el puerto de Barcelona sino que habría afectado también a algunos de sus clientes, concretamente la naviera danesa Moller-Maersk. Trabajadores de la delegación en Barcelona de esta multinacional han asegurado a este diario que su red corporativa se cayó en diversas ocasiones.

"Hoy (por el 25 de septiembre) hemos seguido con problemas, hemos sufrido una caída de servidores por la madrugada, después han aislado a la red del Puerto de Barcelona y hemos podido recuperar conexión". La naviera no ha querido hacer declaraciones oficiales sobre el incidente.

Según Miquel Colobran, esta caída o caídas de la red en Maersk significaría que "o bien el 'ransomware' estaba intentando entrar en sus redes, o bien las afectaciones en la red del puerto habrían provocado problemas en la red de Maersk". El mismo día, 25 de septiembre, caía también la red interna de la policía catalana, que estuvo inoperativa 40 minutos, aunque fuentes de Mossos niegan categóricamente cualquier relación con el ataque del puerto.

Durante los mismos días del ataque al puerto hubo al menos otra empresa en Barcelona afectada por un ataque de 'ransomware'. Se trata de una empresa mediana dedicada a las tecnologías de la información cuyo nombre no ha trascendido, a la que el virus cifró toda la información interna de la empresa. Al funcionar de forma correcta los sistemas de backu, solo fue necesario hacer una reinstalación.

Este 'ransomware', explica uno de los expertos que trabajó en la reparación, no se mandaba por correo electrónico sino que era de los que buscan agujeros en las redes corporativas y se cuelan automáticamente, sin intervención humana: "Una vez conseguido el acceso, instalan el 'ransowmare' y se expanden por las unidades compartidas de la red". El nombre del ransomware era Brrr Dharma y justo aquella semana acababa de salir una nueva versión.

No se descarta que otras empresas de la ciudad fuesen atacadas por el mismo virus, aunque no lo hayan hecho público por temas de imagen. Tampoco sería descabellado que el 'ransomware' que atacó el puerto fuese el mismo Brrr Dharma, que estaría corriendo por las redes catalanes a la búsqueda de agujeros por los que "colarse".

El puerto de Barcelona no es tampoco el primero en vivir uno de estos ataques dentro del sector de los transportes marítimos. El 27 de junio lo sufrió la naviera Moller-Maersk. Afectó a 80 puertos de todo el mundo, con pérdidas de entre 170 y 250 millones de euros. El 'ransomware', llamado Petya, llegó de hecho hasta los terminales de carga que tiene APM, subsidiaria de Maersk, en el puerto de Barcelona.

Los puertos de Amberes y Róterdam también sufrieron, en 2011 y 2013 respectivamente, sendos ciberataques. Los puertos son considerados infraestructuras críticas, lo que hace más delicado cualquier incidente que suceda en ellos y les obliga a seguir normativas específicas, como el Plan Nacional de Protección de Infraestructuras Críticas en España.

Pero la securización de estas infraestructuras está aún en sus inicios y nadie está a salvo, explica a Teknautas el director del Centro de Ciberseguridad Industrial, José Valiente: "El incidente del puerto habría afectado también a otros operadores de infraestructuras críticas porque a día de hoy la mayoría está construyendo sus capacidades de prevención y respuesta frente a incidentes de tecnología operacional".

Precisamente el puerto de Barcelona acaba de poner en marcha su Oficina Técnica de Seguridad y otras mejoras como la incorporación de un sistema de información y gestión de eventos (SIEM) a su plan de ciberseguridad. Valiente muestra el lado positivo del ataque del 'ransomware': "No hay mejor impulsor que los incidentes tecnológicos de alto impacto para que la organización aumente el presupuesto y las capacidades".

Y es que toda medida es poca cuando el puerto de Barcelona es considerado un "smart port" o puerto inteligente que ha incorporado multitud de servicios avanzados, como la gestión del alumbrado, la automatización de las entradas y salidas, la monitorización del tráfico interno de vehículos y varios proyectos de sensores, además de que el 90% de gestiones se realizan de forma telemática. Un 'ransomware' infiltrado en este entramado puede crear, realmente, el caos absoluto.

Una ronda nocturna de vigilancia por el Conde Duque

Fuente: Yorokobu
David García

Hemos hecho una ronda nocturna por el Conde Duque de Madrid, de la mano de sus Vigilantes de Seguridad

Se han cerrado las puertas del Centro Cultural Conde Duque, al que todos los vecinos del barrio llaman «el cuartel» por un motivo rotundamente poderoso: lo fue. Es de noche. Sopla una ligera brisa que presagia que el otoño va pidiendo rebeca para las puestas de sol. Son las nueve y media de la noche y se oye el golpe del portón de entrada. ¡Pom!

Aunque parezca que el cuartel es inexpugnable, una puerta junto a los contenedores de basura del final de la calle Negras se abre como invitación a participar en la ronda nocturna. Mati, vigilante del Conde Duque, tendrá compañía esta noche de jueves en el primero de sus paseos rutinarios por el recinto.

Cada dos horas y media, la vigilante de seguridad o alguno de sus compañeros repasan el estado del edificio por riguroso turno. Cada vez, uno se adentra en los pasillos negros mientras otro vigila todo desde la multipantalla del centro de control. Comprueban las posibles luces encendidas; si una gotera amenaza lo que se custodia en el interior; si los espíritus burlones tratan de llamar la atención de cualquiera o solo lo consiguen con Íker Jiménez. Solo dos personas se quedan hablando con el Conde Duque cuando el sol se marcha.

A La Ronda, una visita nocturna organizada por el Centro Cultural Conde Duque y el Ayuntamiento de Madrid y creada por la artista visual Edurne Rubio, se accede por el callejón trasero del inmenso edificio, un pasaje que separaba al cuartel del Palacio de Liria, la principal residencia madrileña del ducado de Alba.

Tanto el Palacio de Liria como el Cuartel del Conde Duque se construyeron en terrenos de la casa de Alba y, de hecho, el centro militar no se bautizó en honor al Conde Duque de Olivares, sino del III duque de Berwick y Liria, también conde de Lemos, promotor de la construcción del palacio de los Alba. Vamos, un Fitz-James Stuart de toda la vida.

Ese callejón, antes abierto, es la cicatriz que unía a dos edificios adosados de forma casi siamesa. «Aunque ahora está cerrado porque solo se utiliza para que entren los vehículos a cargar y descargar, la Duquesa de Alba y su familia lo utilizaban para salir de casa sin llamar la atención de los paparazzi», explica Mati a sus 40 acompañantes de ronda.

Hace tiempo que la Duquesa de Alba dejó de huir enamorada por los callejones pero, incluso en esta noche de septiembre, una tenue luz brilla en una de las ventanas del palacio. Al fin y al cabo, es la hora de sacar rendimiento a la cuenta de Netflix tanto en casa de los duques como en los pisos de los bufones.

De los Alba a los madrileños

El edificio dejó de ser el cuartel que alojaba a la Guardia de corps. La bosta de caballo, las marchas militares y los reclutas de hormonas disparadas abandonaron el edificio hace décadas. Desde entonces, la mole ha tenido diferentes usos.

Así lo explica a mitad del recorrido Guadalupe, una vecina del barrio que lleva viviendo en él los 56 años que lleva en este mundo. Edurne Rubio tira de manos libres y habla por teléfono desde el recién abierto torreón del Conde Duque. «Estuvo la Guardia Mora de Franco y sus caballerizas aunque yo viví la decadencia de aquello. En los jardines próximos, yo ya solo veía cuatro burros y dos caballos famélicos», contesta la vecina desde la cercana azotea del Museo ABC de la Ilustración.

En los años 60, el Conde Duque pasó a ser de titularidad municipal. «El cuartel estaba muy abandonado, y desde la asociación juvenil en la que nos movíamos en el barrio, hicimos una cacerolada para que esto se convirtiese en un polideportivo. Nos mandaron a fregar porque en aquella época todavía se hacían esas cosas», recuerda Guadalupe.

Después de aquello, el Ayuntamiento de Madrid usó el edificio como sede de cobros de las multas de tráfico, según explica la vecina.

El centro cultural con el que habla Mati

Un rato antes del encuentro telefónico con Guadalupe, la visita comienza por el subsuelo. Ahora mismo, el Conde Duque es un centro cultural que cobija una buena parte de la memoria de Madrid. En los sótanos que recorren Mati y su expedición, oscuros a esta hora, se guardan la hemeroteca y el Archivo General de la Villa de Madrid.

Es ahí donde comenzó la ronda y es ahí donde se ubica el almacenaje inmenso y continuo de las viejas hojas censales del padrón municipal. Como explica también por llamada telefónica en manos libres la directora del archivo, Gloria Donato, «las estanterías contienen los libros encuadernados con hojas desde el año 1846. Nuestro trabajo es clasificar toda esa información para que todo lo que no está informatizado sea fácilmente accesible».

En silencio, iluminados solo por la luz de 40 pequeñas linternas, se ordenan por casa, luego por edificio y luego por distritos todos los vecinos que alguna vez vivieron en Madrid. O, como explica Gloria Donato, los que venían de visita larga. «Los registros tienen una V o una T. La V cataloga al que era vecino de Madrid, pero si la suegra venía seis meses, se señala con una T de transeúnte».

Ahora solo hace falta estar bajo el cielo de Madrid para ser madrileño, «así que los registros se han simplificado y ya no incluyen datos como la parroquia de bautismo o los salarios que cobraban asistentas, médicos o militares», dice la archivera municipal.

Cuando Mati abre la puerta a la siguiente estancia, uno recoge en el bolsillo la sensación de pertenencia a una colmena que lleva hirviendo un buen puñado de siglos y camina siguiendo la luz de su linterna metálica.

Mientras, ella explica que no siempre fue vigilante. «A mí, lo de la seguridad me gustaba. Me presenté hace años a una oposición a policía pero la cosa no cuajó», dice. Desde hace algo más de dos años, abandonó lo que había hecho toda la vida, cine, y se calzó la defensa y los grilletes en el cinturón. «Llevo algo más de año y medio en el Conde Duque y eso me permite llevar a cabo mi trabajo de vigilante, que me gusta mucho, en un lugar en el que se respira creatividad. Las dos cosas por el precio de una».

Además, el tiempo ha hecho que Mati entienda el idioma en el que habla el Conde Duque. Ella le cuenta sus cosas al edificio, le canta y le escucha. Conoce cada rincón, cada extintor y la historia de cada estancia. Conoce el despilfarro que supone que el antiguo Museo de Arte Contemporáneo se mantenga cerrado, con todos los muebles y enseres embalados desde hace más de una década. Dinero gastado, dinero no usado.

Conoce hasta las rejas del suelo del patio que expelen el olor a papel viejo, a archivo y un aliento a una temperatura diferente a las del aire de Madrid. Son las rejas de ventilación de los archivos y las que ayudan a mantener el ecosistema de conservación adecuado. A ella le gusta pararse y oler, sentir al Conde Duque.

Cuando quiere escuchar, Mati para un instante –la ronda no deja pausas muy largas– en el Museo de Arte Contemporáneo. Allí, junto al despacho de Ramón Gómez de la Serna, se zambulle en el silencio oscuro de la sala. Quizás, Mati ha perdido la percepción del Conde Duque como visitante, pero ha ganado la apreciación emocional del espacio. De alguna manera, el Conde Duque respira y vive. De esta manera, Centro Cultural Conde Duque, antiguo cuartel de caballería, habla con quienes deambulan por sus espacios.

¡Socorro! ¡Hemos detectado una brecha de seguridad!

Fuente: Abogacía Española

Marián Rojo Setien. Abogada especializada en Tecnologías de la Información

Clientes, proveedores, trabajadores, videovigilancia… los datos están por todas partes, imprescindibles para el día a día de cualquier compañía.

Todo tratamiento de datos entraña cierto nivel de riesgo. Todos los días, alrededor del mundo se producen millones de brechas de seguridad. No podemos cometer el error de pensar que a nosotros nunca nos va a pasar, o que los datos que manejamos no merecen protección.

Pero… ¿Qué es una brecha de seguridad?

El propio Reglamento General de Protección de Datos (RGPD) las define como "todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos."

El RGPD habla de "violaciones" de seguridad. Sin embargo, la Agencia Española de Protección de Datos prefiere el término "brechas", según explica en su "Guía para Gestión y Notificación de Brechas de seguridad".

¿Qué dice el RGPD? ¿Y la normativa anterior?

Desde el 25 de mayo de 2018 es aplicable el Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; más conocido como Reglamento General de Protección de Datos (RGPD).

Esta normativa obliga a las empresas a notificar la violación de la seguridad de los datos personales a la autoridad de control competente tan pronto como tengan conocimiento de que se ha producido, y a más tardar en un plazo de 72 horas; salvo que pueda demostrarse, atendiendo a su responsabilidad proactiva, que no existe riesgo para los derechos y libertades de las personas.

La obligación de notificar las brechas de seguridad no es nueva. Ya venía introducida por la Ley General de Telecomunicaciones (Ley 9/2014, de 9 de mayo), pero únicamente referida a operadores de servicios de comunicaciones electrónicas y a prestadores de servicios de confianza. También se refería a ella el Reglamento de Desarrollo de la LOPD en relación a la obligación de incluir en el Documento de Seguridad un mecanismo para la gestión de incidencias.

Con el nuevo Reglamento se amplían los supuestos en que es obligatoria esta comunicación, extendiéndose a todos los responsables de tratamiento de datos de carácter personal, siempre que puedan verse afectados los derechos y libertades de las personas.

Además, si de la quiebra de seguridad pudiera derivarse un alto riesgo para los interesados, también habrá que comunicárselo a éstos, para que puedan tomar al respecto las medidas oportunas.

Cómo actuar si se produce una brecha

Importante contar con un plan de acción previamente establecido. En primer lugar, diseñaremos un procedimiento para la detección de incidencias. Podemos disponer de sistemas de alertas, programas informáticos especializados, revisiones periódicas de los sistemas… Para ello pueden sernos muy útiles los recursos que ofrecen organismos como INCIBE.

Cualquier brecha de seguridad debe ser registrada y documentada. Llevaremos un registro de incidencias, que contenga la información sobre el suceso en cuestión. Tendremos en cuenta el tipo de amenaza, su contexto, categorías y tipos de afectados y las consecuencias que hayan podido derivarse del mismo.

Además, siempre que la misma haya podido afectar a los derechos y libertades de los interesados, debemos proceder a notificarla a la autoridad de control competente(en España la Agencia Española de Protección de Datos, AEPD), tan pronto como nos sea posible, y en todo caso, en un plazo máximo de 72 horas desde que tuvimos conocimiento de la misma. El art. 33 del RGPD regula el procedimiento para la notificación de brechas de seguridad

La AEPD mantiene habilitado un mecanismo electrónico para la notificación al que puede accederse a través del siguiente enlace: https://sedeagpd.gob.es/sede-electronica-web/

Si de la brecha de seguridad se derivaran perjuicios graves para los interesados, también habrá que comunicarles a estos la incidencia en el plazo máximo de 72 horas, para que puedan tomar las medidas oportunas.

De forma paralela debemos proceder a dar respuesta al incidente. Para ello, una vez más, es recomendable tener preparado de antemano un plan de actuación. En estos momentos de tensión debemos mantener la calma y actuar según el esquema que previamente hayamos diseñado para este tipo de situaciones. La respuesta dependerá mucho de la categoría de incidencia a la que nos enfrentemos, pero siempre trataremos de contener la situación evitando que el mal se expanda y agrave y, posteriormente, poner remedio al mismo tratando de garantizar la continuidad del negocio minimizando el riesgo para los derechos y libertades de los interesados.

Una vez solventado el problema, debemos realizar un seguimiento del mismo, a fin de evitar que la misma situación pueda volver a producirse en el futuro.

¿Qué pasa si no cumplo?

La protección de datos de carácter personal es un derecho fundamental y como tal está especialmente protegido.

Como señala el Considerando 85 del RGPD, una violación de la seguridad de los datos de carácter personal puede "suponer daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la pseudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión"

La Agencia Española de Protección de Datos ha manifestado reiteradamente que el hecho de notificar una brecha de seguridad no tiene por qué suponer el inicio de un procedimiento sancionador para la compañía ni mucho menos culminar con una sanción.

Habrá que determinar el nivel de responsabilidad de la misma y si ésta había tomado todas las medidas oportunas para evitar el incidente, siguiendo con el principio de responsabilidad proactiva que recoge el RGPD. También habrá que tener en cuenta si se ha producido la efectiva lesión a los derechos y libertades de los interesados.

Tampoco podemos olvidar que cualquier brecha de seguridad puede suponer un daño reputacional a la compañía más grave aún que cualquier sanción que se le llegue a imponer, por lo que más vale prevenir que curar.

Con respecto a los daños y perjuicios que el interesado haya podido sufrir, el artículo 82 del RGPD señala que "Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos", salvo que puedan demostrar que han cumplido fielmente con sus obligaciones. Dicha indemnización tendrá que ser solicitada ante la jurisdicción ordinaria.

En conclusión

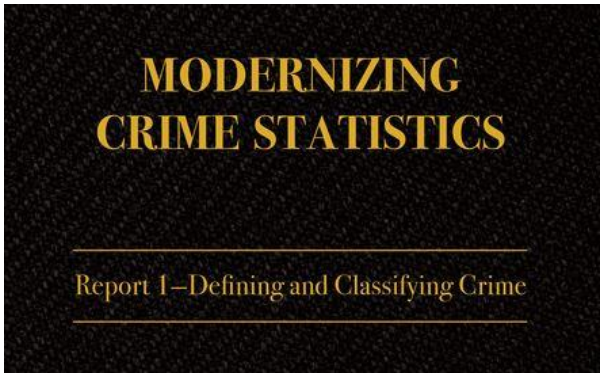
Vivimos en un mundo hiperconectado en el que el tráfico de datos se ha convertido en moneda de cambio habitual, por lo que establecer las medidas oportunas para evitar los fallos de seguridad, así como los mecanismos de respuesta rápida para su correcta gestión en caso de producirse, debe ser una prioridad en el contexto empresarial.

Con una buena planificación, el asesoramiento adecuado y la correcta gestión, podremos minimizar las consecuencias de un problema que, tarde o temprano, toda empresa está destinada a padecer.

El largo camino de modernizar las estadísticas sobre criminalidad

Fuente: Notes de seguretat

Uno de los muchos problemas por resolver en el ámbito de la seguridad es cómo conocer y medir los hechos que causan inseguridad, principalmente los delitos. Las principales herramientas existentes (estadística policial y encuestas de seguridad) son complementarias y tienen ventajas e inconvenientes, y resulta complicado combinar los resultados obtenidos en cada una de ellas.



Académicos y profesionales de los Estados Unidos debatieron, entre diciembre de 2013 y enero de 2017, cómo modernizar los sistemas e instrumentos para medir la delincuencia en su país. El encargo provenía de dos oficinas del Departamento de Justicia, el FBI y la Oficina de Estadísticas de Justicia (BJS, por su sigla en inglés), y tenía que cubrir tres ámbitos:

- uno sustancial: desarrollar una nueva clasificación de los delitos;
- uno metodológico: proponer un sistema de recogida de los datos, y
- uno de implementación: recomendar cómo hay que llevar a cabo la recogida de los datos.

El primer informe de este grupo de expertos se publicó en mayo de 2016 y daba respuesta al primero de los ámbitos, la clasificación de los hechos delictivos. El objetivo era tener una visión de conjunto de las tipologías delictivas, a partir, entre otras fuentes, de los datos policiales y de los datos de encuestas.

El sistema de clasificación actual se basa en criterios establecidos entre 1929 y 1930, y se caracteriza por recoger pocos hechos que están regulados de modo muy parecido en todos los EE.UU. Por lo tanto, aunque es una clasificación pragmática y útil, también es demasiado rígida y estricta, y una de las voluntades del nuevo sistema de clasificación es que constituya un marco que permita incorporar nuevas figuras delictivas que puedan aparecer en un futuro.

La nueva clasificación se realiza con finalidades estadísticas y pretende que cualquier hecho delictivo pueda encajar en alguna categoría, pero sólo en una. Las definiciones de la clasificación ponen el énfasis en conductas, sin la voluntad de que estas tengan que corresponderse con las tipologías penales. Aunque la clasificación se piensa en relación con las infracciones penales, también tiene en cuenta que el análisis se hará sobre incidentes, que pueden incluir más de un hecho delictivo o relacionar a una o más víctimas o a uno o más autores.

Además de revisar el sistema actual, los precedentes históricos y las necesidades de los diferentes usuarios de las estadísticas de criminalidad, también han analizado otras experiencias en modernización de las estadísticas. Entre ellas, destaca la Clasificación Internacional de Delitos con Finalidades Estadísticas (ICCS, por su sigla en inglés), aprobada por las Naciones Unidas el año 2015 y que se establece como un estándar internacional que se ha tomado como marco de referencia incorporando modificaciones para tener en cuenta la realidad propia del país (como incidentes con armas de fuego).

Así, la nueva clasificación propuesta contiene 11 categorías de primer nivel (más genéricas), que, con alguna pequeña diferencia, se corresponden con las de ICCS:

1. Actos que conducen a la muerte o intentan causar la muerte
2. Actos que causan daño o intentan causar daño a las personas
3. Actos injuriosos de naturaleza sexual
4. Actos de violencia o amenazas de violencia contra las personas relacionados con la propiedad
5. Actos que sólo atentan contra la propiedad
6. Actos relacionados con sustancias controladas[1]
7. Actos relacionados con el fraude, la estafa o la corrupción
8. Actos contra el orden público y la autoridad
9. Actos contra la seguridad nacional
10. Actos contra el medio natural o contra los animales
11. Otros actos delictivos no clasificados en las demás categorías

Este primer nivel de categorías se va subdividiendo, con mayor o menor detalle, hasta llegar a un máximo de cuatro niveles (X.X.X.X), con lo cual se obtienen 189 categorías diferentes (ICCS llega a 230 categorías).

La clasificación se acompaña de unos atributos o etiquetas que permiten una explotación adicional e, incluso, una reclasificación posterior. Estos atributos están relacionados con el incidente o con las distintas infracciones, víctimas o autores relacionados con cada incidente.

Próximamente complementaremos la información con el resultado del segundo informe, publicado en marzo de 2018, en que se propone el sistema de recogida de datos y cómo implementarlo.

El informe completo se puede consultar *aquí*

¿Sabes cómo proteger tu pyme de un cibercrimen?

Instituto Nacional de Ciberseguridad

En la mayoría de los ataques a las empresas casi siempre hay un importante factor humano. Por supuesto, la tecnología ofrece muchas oportunidades para que el delincuente ejecute su fechoría y para que su alcance sea mayor pero, precisamente por esto, tenemos que preparar nuestros negocios y a nuestros empleados tanto como podamos.

¿Qué puede pasar?

Si perdemos los datos de nuestro negocio, nos roban los de nuestros clientes o somos objeto de algún fraude por Internet, en muchos casos para una pyme no quedaría más remedio que cerrar la empresa o declararla en bancarrota.

Estos son algunos riesgos y engaños a los que nos exponemos:

1. Los USB pueden tener datos confidenciales y no es difícil que los perdamos o que nos los roben. También a veces encontramos memorias USB que intencionadamente están a nuestro alcance o nos lo ofrece alguien que parece de confianza, pero que están infectados con malware. ¡Desconfía!
2. Pueden llegarnos llamadas de falsos servicios técnicos que nos convencen para que les dejemos entrar remotamente a nuestro ordenador y desde ahí robar datos, ejecutar comandos, etc.
3. Sospecha si un suministrador te pide que pagues en una cuenta diferente, con urgencia, ya que en realidad no es el suministrador, ha sido suplantado.
4. Recibimos correos de phishing que nos piden mediante engaños que iniciemos sesión en una página que es «igualita» por ejemplo, a la de nuestro banco o la de Hacienda. Si picamos pueden capturar nuestros datos de acceso a esas cuentas.
5. Si dejamos los routers con la configuración por defecto, son vulnerables, ya que cualquiera con algo de conocimiento técnico podría conseguir la contraseña de este modelo.
6. Cuando recibimos correos con facturas que son aparentemente de organizaciones con las que tratamos (multas de tráfico, transportistas, etc.) y que nos piden que paguemos el importe en una cuenta que no es la habitual.
7. Si recibimos correos urgentes que aparentemente proceden de nuestro jefe en el que nos pide que hagamos un ingreso, generalmente con urgencia, o le enviemos cierta información confidencial.

¿Cómo los evitamos?

Muchos de estos ataques tienen su origen en empleados bien descuidados, bien poco entrenados y en algunas ocasiones malintencionados. Estas son algunas de las medidas que tienes que poner en marcha en tu organización:

- Establece políticas sobre el uso de los dispositivos de trabajo en la oficina y en movilidad: portátiles, móviles, ordenadores, servidores, acceso remoto, etc.
- Habilita el acceso a la información sólo a quien la necesite. Vigila quién accede a qué carpetas y qué cambios hace en ellas.
- Asegúrate de que tus empleados utilizan contraseñas robustas, las cambian con frecuencia y no las comparten ni reutilizan. Comprueba que en los servicios críticos y cuentas con privilegios de administrador se utiliza doble factor de autenticación. Habilita gestores de contraseñas seguros para almacenar las contraseñas.
- Educa a tus empleados sobre los riesgos en Internet. Fomenta que antes de realizar cualquier pago o envío de información confidencial se realicen comprobaciones con el jefe inmediato o con otro compañero.
- Haz que tus empleados firmen acuerdos de confidencialidad que se extiendan más allá de la finalización de sus contratos.
- Pon en marcha políticas de uso y acceso a la información; clasifícala para identificar aquella que no puede salir de la empresa. Incorpora medidas para protegerla y evitar fugas.
- Realiza backups con frecuencia, comprueba que sabes cómo recuperarlos y almacénalos en un lugar seguro. Los incidentes ocurren y lo mejor y más efectivo para recuperarse, es tener un plan B.
- No ignores los mensajes de actualización del software y de los antivirus. El software desactualizado es más vulnerable, los delincuentes tienen formas de descubrirlo y «armas» preparadas para lanzar ataques a todo el que se despiste.

¿Y qué más puedes hacer?

Si ya cumples con lo anterior, estás alineando tu negocio con la ciberseguridad. ¡Felicidades! No obstante, recuerda que esto es un proceso continuo, ¡no puedes bajar la guardia!

¿Que son los ataques DoS y DDoS?

Fuente: Oficina de Seguridad del Internauta

Seguro que has leído y escuchado muchas veces hablar sobre los ataques de denegación de servicio, pero, ¿sabes realmente lo que son? A priori, parece un término muy técnico, pero este ataque es muy sencillo de comprender. Además, es uno de los más utilizados por los ciberdelincuentes a nivel mundial, por lo que es importante entender en qué consiste.

Un ataque de denegación de servicio, tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado. Este ataque puede afectar, tanto a la fuente que ofrece la información como puede ser una aplicación o el canal de transmisión, como a la red informática.

Los servidores web poseen la capacidad de resolver un número determinado de peticiones o conexiones de usuarios de forma simultánea, en caso de superar ese número, el servidor comienza a ralentizarse o incluso puede llegar a no ofrecer respuesta a las peticiones o directamente bloquearse y desconectarse de la red.

Existen dos técnicas de este tipo de ataques: la denegación de servicio o DoS (por sus siglas en inglés Denial of Service) y la denegación de servicio distribuido o DDoS (por sus siglas en inglés Destributed Denial of Service). La diferencia entre ambos es el número de ordenadores o IP´s que realizan el ataque.

En los ataques DoS se generan una cantidad masiva de peticiones al servicio desde una misma máquina o dirección IP, consumiendo así los recursos que ofrece el servicio hasta que llega un momento en que no tiene capacidad de respuesta y comienza a rechazar peticiones, esto es cuando se materializa la denegación del servicio.

En el caso de los ataques DDoS, se realizan peticiones o conexiones empleando un gran número de ordenadores o direcciones IP. Estas peticiones se realizan todas al mismo tiempo y hacia el mismo servicio objeto del ataque. Un ataque DDoS es más difícil de detectar, ya que el número de peticiones proviene desde diferentes IP´s y el administrador no puede bloquear la IP que está realizando las peticiones, como sí ocurre en el ataque DoS.

Los ordenadores que realizan el ataque DDoS son reclutados mediante la infección de un malware, convirtiéndose así en bots o zombis, capaces de ser controlados de forma remota por un ciberdelincuente. Un conjunto de bots, es decir, de ordenadores infectados por el mismo malware, forman una botnet o también conocida como red zombi. Obviamente, esta red tiene mayor capacidad para derribar servidores que un ataque realizado por sólo una máquina.

Para comprobar si nuestro equipo está infectado por este tipo de malware y pertenece a una red zombi, sin que seamos conscientes, podemos hacer uso del servicio AntiBotnet que detectará si nuestra red pertenece a una botnet.

¿Por qué se realizan estos ataques y a quién afectan?

Como hemos visto, los ataques de denegación de servicio son utilizados para inhabilitar un servicio ofrecido por un servidor, haciendo colapsar el sistema aprovechando sus vulnerabilidades. El objetivo de los ciberdelincuentes es provocar un perjuicio, tanto a los usuarios que se abastecen del servicio, como al administrador que lo ofrece, inhabilitando su funcionalidad y provocando pérdidas, tanto económicas, como de prestigio.

Hasta el momento, El mayor ataque de denegación de servicio ocurrido en la historia se produjo, el 28 de febrero de 2018, a una conocida plataforma de proyectos colaborativos. Dejando sin funcionamiento la plataforma unos 10 minutos en total, de manera intermitente. Este ataque fue realizado de forma distribuida, es decir, con un ataque DDoS. A pesar de toda la seguridad de la que disponía la plataforma, no pudo afrontar el bombardeo de 126,9 millones de paquetes o lo que es lo mismo, unos 1,35 terabits por segundo recibidos. Este ataque fue realizado a través de una red botnet utilizando servidores de diversas entidades.

¿Cómo evitarlo?

Como usuarios debemos revisar la configuración de nuestros routers y firewalls para detectar IP´s inválidas o falsas, que provengan de posibles atacantes. Normalmente, nuestro Proveedor de Servicios de Internet (ISP) se encarga de que nuestro router esté al día con esta configuración.

Por otro lado, las Organizaciones y empresas que proveen estos servicios, deben proteger tanto su red, como toda su infraestructura para poder evitar que estos ataques puedan afectar al desempeño de su trabajo y como consecuencia derivada de ello, a sus clientes. Si una empresa se ve afectada por un ataque de denegación de servicio (DoS) perderá la confianza de sus clientes y descartarán la contratación de sus servicios.

Noticias

SCATI, fabricante de sistemas de video IP inteligentes, confía su Dirección General en Alfonso Mata, el hasta ahora Director Comercial, para liderar su crecimiento a nivel mundial.

Alfonso Mata se incorporó al equipo **SCATI** en 2005, donde comenzó a trabajar como gestor de ventas de grandes cuentas en España para después liderar la Dirección Comercial del país y más tarde también de EMEA (Europea Middle East & África) y Centro América hasta asumir la Dirección Comercial Global.

Ingeniero en Telecomunicaciones, Mata, es director de seguridad homologado por el Ministerio de Interior del Gobierno de España y cuenta con una dilatada experiencia laboral en el mercado de la seguridad.

Con este cambio en la Dirección General, **SCATI** confía en afianzar su marca en los mercados en los que opera actualmente y mantener su crecimiento y su posición como líder en ofrecer soluciones de video especializadas en entidades financieras en el mercado español y latinoamericano.

"Durante años, Alfonso ha demostrado sus grandes cualidades para la dirección; por ello confiamos plenamente en que su experiencia y compromiso con el desarrollo de **SCATI** le van a permitir pilotar con éxito esta nueva etapa de crecimiento y liderazgo tecnológico", comenta Alfonso Gil, Presidente de **SCATI**.

Formación

Formaciones de enfoque práctico sobre áreas y sectores de conocimiento de AECOC

Más Información en el siguiente enlace

Cursos Especializados de Dirección 2018

Más información y programa en el siguiente enlace

II Jornada de RPAS y Seguridad Privada, el 30 de octubre en Madrid

Analizar el escenario abierto por la nueva normativa sobre drones y su impacto sobre el sector es el objetivo de la II Jornada de RPAS y Seguridad Privada que se celebrará el próximo 30 de octubre en Madrid bajo la organización de Peldaño, en colaboración con la revista Cuadernos de Seguridad.

El evento contará con expertos de primer nivel para abordar temas de máximo interés para el sector tanto en el campo normativo como en el ámbito de la industria y generación de negocio.

Regístrate en la web *https://www.dronesyseguridad.com/* para hacerte con una de las plazas limitadas.

La jornada se abrirá con la ponencia Normativa actual sobre el uso de RPAS en España, a cargo de la Agencia Española de Seguridad Aérea, AESA. Seguidamente, tendrá lugar la intervención de Policía Nacional sobre Normativa de Seguridad Privada y su aplicación a RPAS.

Desde el Centro Nacional de Protección de Infraestructuras Críticas y Ciberseguridad (CNPIC) se abordará el papel de los RPAS en la Protección de Infraestructuras Críticas. mientras que la Guardia Civil expondrá su labo de Control de RPAS en el Aeropuerto Adolfo Suárez Madrid-Barajas.

A continuación, se ofrecerán sendas ponencias sobre Integración de sistemas y operaciones de seguridad con RPAS y el desafío de la Seguridad ante los Drones, antes de dejar paso a la mesa redonda

sobre Retos y oportunidades de los RPAS en la industria de la Seguridad, que pondré el broche final a la Jornada.

El evento cuenta con el apoyo de Eulen Seguridad, Casmar-AIProx, Aircatdrone y Thales y da continuidad a la primera edición celebrada en 2016.

Está dirigido fundamentalmente a directores y gestores de la Seguridad de entidades públicas y privadas y a profesionales tanto de empresas de Seguridad como de RPAS y centros de formación.

Consulta el programa en *https://www.dronesyseguridad.com/*

Legislación

ORDEN DEF/1012/2018, DE 19 DE SEPTIEMBRE, POR LA QUE SE CREA LA RED DE LABORATORIOS DEL MINISTERIO DE DEFENSA.

PDF de la disposición en el siguiente enlace

ORDEN PCI/978/2018, DE 20 DE SEPTIEMBRE, POR LA QUE SE REGULAN LOS CURRÍCULOS DE LA ENSEÑANZA DE FORMACIÓN PARA LA INCORPORACIÓN A LA ESCALA DE OFICIALES DEL CUERPO DE LA GUARDIA CIVIL MEDIANTE LAS FORMAS DE INGRESO POR ACCESO DIRECTO SIN TITULACIÓN UNIVERSITARIA Y POR PROMOCIÓN PROFESIONAL; SE DICTAN LAS NORMAS DE EVALUACIÓN, Y DE PROGRESO Y PERMANENCIA EN EL CENTRO DOCENTE DE FORMACIÓN; Y SE REGULAN LAS TITULACIONES QUE PERMITEN EL INGRESO.

PDF de la disposición en el siguiente enlace

Revistas

Seguritecnia Nº 456. Septiembre

Nuevo número de **SEGURITECNIA**, con reportajes, entrevistas y artículos, destacando:

- **Editorial:** Ley NIS: servicios esenciales más seguros
- **Seguripress**
- **Especial:** Seguridad Aeroportuaria
- **Entrevista:** Santiago Cortés. Jefe de la División de Seguridad de ENAIRE

Enlace: ver revista digital

Cuadernos de Seguridad Nº 336. Septiembre

En este número de **CUADERNOS DE SEGURIDAD**, además de las secciones habituales de «Seguridad», «Cuadernos de Seguridad estuvo allí», «Estudios y Análisis», o «Actualidad, el lector encontrará:

- **Editorial:** «El mundo cambia, nosotros también».
- **En Portada:** «Seguridad, clave en las instalaciones sanitarias».
- **Entrevistas:** «Fernando Bocanegra. Director de Seguridad Corporativo SERMAS».
- **Artículos:** «La Dirección de Seguridad desde la perspectiva de la Gerencia Hospitalaria».

Enlace: ver revista digital

¿Quieres ser Socio de ADSI – Asociación de Directivos de Seguridad Integral?

Para iniciar el proceso de alta como Asociado, envíe un e-mail a secretario@adsi.pro , indicando nombre y apellidos, una dirección de correo y un teléfono de contacto.

En cuanto recibamos su solicitud le enviaremos el formulario de Solicitud de Admisión.

¿Quién puede ser socio de ADSI – Asociación de Directivos de Seguridad Integral?

Puede ser socio de **ADSI**:

- Quien esté en posesión de la titulación profesional de Seguridad Privada reconocida por el Ministerio del Interior (T.I.P. de Director de Seguridad, Jefe de Seguridad, Detective Privado o Acreditación de Profesor de Seguridad Privada).
- Todo Directivo de Seguridad que posea, a criterio de la Junta Directiva de la Asociación, una reconocida y meritoria trayectoria dentro del sector.