NEWS ADSI FLASH

www.adsi.pro

Índice

- Nuestros Patrocinadores.. 2
- VI Jornada de Seguridad Privada en Catalunya..... 3
- Security Forum 2019..... 4
- Cinco cambios que han hecho de los estadios un lugar seguro 5
- Santa Coloma de Gramanet y Premià de Dalt rescatan la figura del Sereno..... 7
- Más presión que nunca para el director de seguridad de la información..... 8
- Buch resalta la "cooperación" entre policías y vigilantes en el Dia Català de la Seguretat Privada.... 9
- ¿Quienes han de contar con un Delegado de Protección de Datos?..... 10
- ¿Cuáles son los elementos fundamentales de la prevención según el Reglamento de los servicios de prevención?..... 12
- ¿Sabes cómo mejorar la ciberseguridad de tu organización? Implanta un Plan Director de Seguridad..... 14
- Primeros pasos para mejorar la seguridad de nuestros datos..... 16
- Noticias..... 18
- Formación 18
- Legislación 19
- Revistas..... 19

VI Jornada de Seguridad Privada en Catalunya

06 de marzo de 2019

Entrada reducida para socios de ADSI

Asociación de Directivos de Seguridad Integral

ADSI

Nuestros Patrocinadores

avigilon
AXIS COMMUNICATIONS
DATABAC Soluciones completas de identificación
FERRIMAX ADVANCEDSECURITYSYSTEMS
Honeywell THE POWER OF CONNECTED
ILUNION
iNV Seguridad
LANACCESS
LOCKEN SMART ACCESS SOLUTIONS
METROPOLIS www.metropolisgrupo.com
PROSEGUR Seguridad de confianza
PYCSECA seguridad
SABICO seguridad
SCATI VIDEO MANAGEMENT SYSTEMS
SISMEDE DESIGNING SECURITY

VI Jornada de Seguridad Privada en Catalunya

Junta Directiva

ADSI junto a la revista 'Seguritecnia' y ACAES volverán a organizar este encuentro que permitirá a los asistentes conocer la realidad de la Seguridad Privada en Cataluña de la mano de profesionales y empresas del sector que operan allí, así como también gracias a la visión que aporten las autoridades catalanas y los responsables de las Fuerzas y Cuerpos de Seguridad.

Tras el significativo éxito de ediciones anteriores, la Asociación de Directivos de Seguridad Integral (**ADSI**) vuelve a organizar este encuentro profesional junto con la revista Seguritecnia y con la Asociación Catalana de Empresas de Seguridad (ACAES).

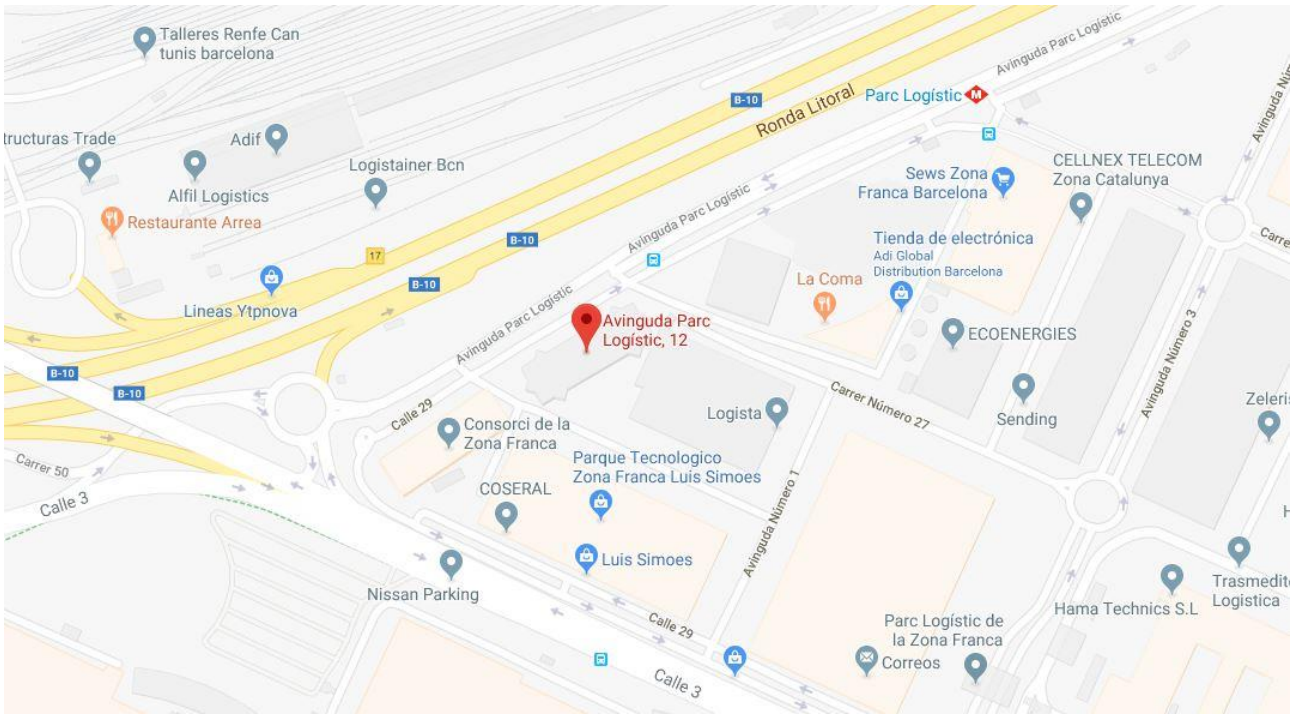
El encuentro, que tendrá lugar en el Cellnex Telecom de Barcelona el próximo 6 de marzo, permitirá a los asistentes conocer la realidad de la Seguridad Privada en Cataluña respecto a la normativa, problemáticas y situaciones de interés además de compartir las últimas novedades en Seguridad. Todo ello de la mano de autoridades catalanas y de responsables de las Fuerzas y Cuerpos de Seguridad y profesionales del sector de la seguridad.

Entradas
85 € IVA (INCLUIDO) *Entrada general*
60 € IVA (INCLUIDO) *Entrada reducida* SOLO PARA ASOCIADOS **ADSI**, ACAES Y FUNDACIÓN BORREDÁ

Avinguda Parc Logístic, 12 (Metro Parc Logístic)
Edificio Cellnex Telecom
Barcelona.

Registro y Programa en el *siguiente enlace*

Para más información mandar un email a: *borrmart.eventos@borrmart.es*



Security Forum 2019

https://www.securityforum.es/

Security Forum celebrará en 2019 su séptima edición. Un evento que se ha posicionado como un referente en el sector de la seguridad gracias a sus valores diferenciales.

El mejor escaparate de innovación donde mostrar novedades y avances tecnológicos. Una oportunidad para generar negocio en torno al mercado de la Seguridad. Esta edición contará de nuevo en la zona de exposición con áreas de CCTV, integración de sistemas, seguridad física, ciberseguridad, prevención y control de incendios, control de accesos, IP/REDES… Este año el evento continuará con su apuesta por la innovación incorporando los sectores profesionales de Hotelería y Contact Center.

El martes 28 de mayo se celebrará la primera jornada, dedicada a la seguridad global. Descubriremos desde una visión multidisciplinar aspectos y perfiles relacionados con la seguridad de gran interés para los profesionales de la seguridad.

El miércoles 29 de mayo se celebrará la segunda jornada, centrada en Ciberseguridad. Un escenario internacional para debatir sobre nuevas amenazas de la mano de los más importantes expertos en ciberseguridad.

Además el congreso contará con la colaboración de diferentes entidades y profesionales de reconocido prestigio en el sector de la ciberseguridad, asegurando el alto nivel del programa.

Durante Security Forum se celebrarán los Expert Panels, un foro de debate donde las empresas presentarán las últimas tendencias en tecnología y debatirán con los profesionales sobre las posibilidades de aplicación en el entorno empresarial.

Charlas de transferencia tecnológica entre las empresas que aportan soluciones tecnológicas y los profesionales de la gestión, consultoría e instalación de sistemas de seguridad.

INFORMACIÓN PRÁCTICA

CCIB. Centro de Convenciones Internacional de Barcelona. Plaza de Willy Brandt, 11-14 – 08019 – Barcelona.

Entrada por acceso "A". Desde plaza de Llevant por zona peatonal (junto a Plaza Leonardo Da Vinci).

info@securityforum.es

10:00h a 18:30 h

28 y 29 de mayo de 2019.

+34 914 768 000

Cinco cambios que han hecho de los estadios un lugar seguro

Fuente: El País
J. Pedraza

La consolidación de figuras como los directores de seguridad en cada club, los informes exhaustivos sobre actos antideportivos en cada partido o la sofisticada tecnología que permite identificar a los infractores han reducido drásticamente la violencia

Los números son contundentes. El pasado año se registraron cuatro infracciones de seguridad de las calificadas como muy graves en los estadios españoles. Muy lejos de las 150 que se produjeron en la temporada 2014/15, según refleja la Memoria de la Comisión Estatal contra la Violencia, el Racismo, la Xenofobia y la Intolerancia en el Deporte. En esa categoría entra lo peor que puede ocurrir en un recinto: actos violentos con muertos o heridos, lanzamiento de bengalas con daños personales, violar la prohibición de acceso a los campos… También se han conseguido frenar las peleas entre grupos violentos o agresiones de estos a otros aficionados. Si en la 2015/16 se registraron 30 de estos incidentes en La Liga Santander, La Liga 1|2|3 y Copa del Rey, el año pasado esta cifra se redujo a 17, prácticamente la mitad.

El cambio ha sido radical y ha ocurrido en apenas cuatro años. Los estadios de fútbol se han convertido en zonas más seguras gracias especialmente a las medidas impulsadas por los legisladores y La Liga. Hay un control más estricto de los violentos, todos los clubes cuentan de forma obligatoria con un director de seguridad, la tecnología de la seguridad se ha sofisticado y la vigilancia y denuncias han aumentado.

Fernando Bernal es el director de seguridad del Sevilla FC desde 2015. Anteriormente era oficial de la Unidad de Intervención Policial, que se encarga de velar por la seguridad y el orden público en la mayoría de los partidos. Su visión de lo que ha ocurrido es, por lo tanto, doble: "La profesionalidad y coordinación de las fuerzas de seguridad públicas y privadas en estos grandes dispositivos no tiene parangón en Europa. Todo gracias a una legislación que arranca con la Ley 19/2007 y que se sigue mejorando. Además, creo que la labor pedagógica y de concienciación que se ha hecho en este país ha sido importantísima. La mentalidad del aficionado ha cambiado mucho en muy poco tiempo".

Coincide Juan Carlos Privado, coordinador de seguridad del área de Integridad y Seguridad de La Liga, que señala además un punto de inflexión en la lucha contra la violencia en el fútbol: "Fue la muerte de Francisco Javier Romero, el hincha del Deportivo de La Coruña conocido como Jimmy, la que provocó el compromiso definitivo de clubes e instituciones y la creación de un plan estratégico que ha dado sus frutos". Fue en noviembre de 2014. Desde entonces, la transformación se ha producido en cinco ejes principales, como apuntan ambos expertos. Estos son los pilares del cambio:

Todos los clubes cuentan con directores de seguridad obligados a intercambiar información

Cada club tiene un director de seguridad, que además ha de ser la misma persona durante toda la temporada, salvo casos excepcionales. Estos responsables están obligados a comunicarse entre sí antes del partido de sus equipos para intercambiar información. Además, son los responsables de establecer los dispositivos de seguridad privada para cada choque en contacto permanente con la otra figura clave: el coordinador de seguridad, que es el mando policial al mando en cada evento.

"Lo habitual es que haya dos comunicaciones formales para cada partido, que se producen por vía telefónica y escrita, y otras muchas informales según se aproxima el encuentro", desarrolla Fernando Bernal. El club visitante entrega al local unos formularios en los que se indica cuántas entradas se han vendido de las que han sido puestas a disposición de la afición foránea, cómo van a viajar y hospedarse el equipo y sus fans y, si se da el caso, qué grupos pueden suponer una amenaza. Esa información se suma al resto de cálculos (importancia del partido, rivalidad entre los equipos, previsión de afluencia al campo…) para evaluar el nivel de riesgo del partido, y a partir de ahí, el modelo de dispositivo de seguridad que establecerán las autoridades policiales y el club.

"En el caso del Sánchez Pizjuán [un estadio de casi 45.000 espectadores que casi siempre se acerca al lleno], solemos contar con 240 vigilantes de seguridad privada apoyados por 110 auxiliares de seguridad en un partido de riesgo normal". Antes, la comunicación no estaba regulada. Los directores de seguridad de los clubes, si existían, no tenían por qué conocerse unos a otros. Ahora incluso se convocan reuniones periódicas entre ellos y las fuerzas policiales para mejorar los protocolos.

Violentos identificados y fuera de las gradas. 150 individuos no pueden pisar un estadio en España

Los grupos violentos están identificados y más controlados. La afición visitante tiene ahora entradas nominativas. Para acceder a la zona del estadio reservada y especialmente acotada para ellos, los aficionados deben presentar su DNI o pasaporte, y que este coincida con lo que se lee en la entrada. Los clubes de La Liga Santander y La Liga 1|2|3 han expulsado, arrinconado o minimizado a sus grupos más radicales para que no supongan un problema. "Muchos los han sustituido por gradas de animación, que además acceden al estadio mediante control biométrico, con su huella dactilar", subraya Juan Carlos Privado. Si algún hincha incurre en actos violentos dentro o fuera del estadio, se expone a ser vetado de cualquier evento deportivo. "En nuestro estadio tienen prohibida la entrada entre 10 y 15 personas

aproximadamente", afirma Bernal. La cifra ronda las 150 personas en las dos categorías del fútbol profesional español.

Los ultras organizados se persiguen con mayor interés que antes. El pasado mayo una sentencia pionera abrió un nuevo camino. Once miembros de Indar Gorri, grupo radical vinculado a Osasuna, fueron condenados por asociación criminal y conspiración para cometer el delito de lesiones. Un nuevo paso para desarticular a estos colectivos, pero no el único: "La eliminación de su simbología de los estadios también ha tenido un efecto muy positivo. No solo porque anula en cierto modo su sentimiento de pertenencia y la exhibición de elementos radicales, sino porque les quita publicidad. Y si no se conocen sus marcas, nadie va a comprar sus productos, que es una de sus principales líneas de financiación", destaca Juan Carlos Privado.

Mayor vigilancia en los estadios con tecnología punta. 4K para identificar y biometría en los accesos

"Grabamos en audio y vídeo todo lo que pasa en las gradas con cámaras de alta resolución [4K]. Los cánticos ofensivos también quedan registrados gracias a las imágenes de la retransmisión deportiva, que pueden exponerse como evidencia ante las autoridades", asegura Juan Carlos Privado. Los accesos a los estadios también tienen cámaras. De esta forma se logró identificar y detener en pocos días al agresor de un guardia de seguridad del Wanda Metropolitano (que perdió un ojo a consecuencia de las heridas) a finales de 2017. "Los sistemas de detección de metales, las cámaras, la inversión en formación y contratación de personal… Hemos evolucionado muchísimo en muy poco tiempo. Nuestros estadios están mucho mejor dotados que los de nuestro entorno", señala Fernando Bernal del Sevilla FC, club pionero en usar perros para la detección de explosivos o material pirotécnico como bengalas. El responsable de seguridad del club sevillista señala que gracias a estas medidas el Pizjuán no ha vivido ningún episodio de violencia física, lanzamiento de objetos o uso de bengalas en los cuatro años que lleva en el cargo. En toda la temporada pasada, solo se denunció un episodio con bengalas y diez de lanzamiento de objetos en todos los partidos de La Liga.

"La innovación tecnológica, por razones obvias, es la principal línea de avance para los próximos años, ya que en España toda la labor de legislación, formación y concienciación lleva muy buen camino desde hace tiempo", analiza Bernal. La biometría controla, de momento, el acceso a las gradas de animación, pero en el futuro su uso se generalizará. "La idea del Sevilla FC es que lo que sirve para una parte de la grada sirve para todo el estadio. Queremos instalar el acceso por biometría en todo el Ramón Sánchez Pizjuán, remodelando todas las puertas de acceso y salida para lograr que a corto o medio plazo todo el público tenga esta posibilidad". El proyecto ya está en marcha, pero el club aún no ha decidido si la identificación será dactilar o facial. La Liga ya es segura, y lo será cada vez más.

Procesos judiciales contra los violentos. La Liga presente como acusación particular

La Liga presentó la pasada temporada 75 denuncias ante la Comisión Antiviolencia y el Comité de Competición, 51 de ellas por cánticos ofensivos registrados en los estadios. Cánticos de radicales son sistemáticamente denunciados con la mayor precisión. La Liga, con la ayuda del director de partido, se encarga de detectar de forma exhaustiva los comportamientos relacionados con la violencia, el racismo, la xenofobia y la intolerancia que se dan durante un partido de fútbol.

Este es un ejemplo real del tipo de denuncia que se suele presentar acompañada de pruebas documentales: "En el minuto 7 de partido, unos 500 aficionados locales, entonaron de forma coral y coordinada durante aproximadamente 12 segundos, el cántico 'XXXX bastardo". Se persiguen los insultos, las incitaciones a la violencia, el racismo o la homofobia; dirigidos contra jugadores, cuerpo técnico, árbitros o aficiones rivales.

La Liga también se presenta como acusación particular en algunas causas penales, como la de la muerte del propio Jimmy, para que en ciertos casos el proceso judicial pueda tener lugar. También se ha personado en el caso de la reyerta ocurrida en 2016 entre los grupos radicales de Getafe y Zaragoza en las inmediaciones del Coliseum Alfonso Pérez. O en la denuncia contra un aficionado del Real Oviedo por agredir a un guardia de seguridad en las puertas del Carlos Tartiere el pasado 20 de abril. El suceso, también en este caso, fue captado por las cámaras del estadio.

La labor pedagógica. Animar al equipo no significa insultar al rival

Los cánticos ofensivos han pasado a ser mal recibidos por buena parte de la grada. Los estadios recuerdan con megafonía o desde sus videomarcadores que animar a un equipo no significa insultar al rival. Instituciones y clubes fomentan la afición sana al fútbol y los hermanamientos entre peñas desde Aficiones Unidas. La Liga envía temporada tras temporada documentos informativos para todos los equipos con normas y recomendaciones. Recomiendan la puesta en marcha de "campañas institucionales de rechazo ante cualquier tipo de violencia" y "medidas preventivas", como la emisión de mensajes previos al encuentro o la organización de actos de confraternización con peñas rivales.

Los equipos y las instituciones que rodean al deporte español son los primeros interesados en acabar con la violencia física y verbal. "Una de las principales vías para terminar con esta lacra a medio o largo plazo es la concienciación y la pedagogía. El Sevilla lleva ya seis años con la campaña Cordiality, que a través de pancartas, vídeos, eventos o acciones en redes sociales fomenta la tolerancia y el respeto en el fútbol", expone Fernando Bernal, que asegura que la labor pedagógica es "probablemente la más difícil de realizar, pero la que mayores cambios ha provocado".

Santa Coloma de Gramanet y Premià de Dalt rescatan la figura del Sereno

Fuente: La Vanguardia
Fede Cedó

La medida busca paliar la falta de efectivos de seguridad

La sensación de inseguridad en las calles provocada por el incremento de la actividad delictiva, sumada a la falta de efectivos policiales, empuja a los municipios a buscar fórmulas para garantizar el sosiego de sus vecinos. Uno de estos recursos es la recuperación de la figura del sereno, el vigilante nocturno que desde finales del siglo XVIII hasta primeros del XX era una figura popular en la administración municipal. Ahora, dos municipios catalanes, Santa Coloma de Gramenet y Premià de Dalt, impulsan iniciativas en este sentido.

Núria Parlón, alcaldesa de Santa Coloma, presentó ayer el nuevo servicio de serenos de la ciudad que estará formado por 18 personas –dos encargados y 16 serenos- que patrullarán por parejas mixtas. La intención es crear entornos de confianza y mejorar la sensación de seguridad en el vecindario. "La seguridad no sólo está vinculada a la policía y a la prevención del delito, sino que se trata de generar entornos amables". Los serenos colomenses se identificarán con unos chalecos amarillos y pasearán por los barrios desde las once de la noche hasta las siete de la mañana En este proyecto, el Ayuntamiento invertirá 400.000 euros anuales.

El trabajo de los serenos en Santa Coloma será similar al de los agentes cívicos que recorren la ciudad durante el día. Entre sus labores estará inspeccionar el mobiliario urbano, el alumbrado, los vehículos estacionados, el estado de edificios y comercios, para detectar desperfectos y alteraciones. Otra de sus funciones será asistir a personas que necesiten ayuda, si se han perdido, si tienen miedo a bajar la basura o ciudadanos con movilidad reducida que necesiten ir a la farmacia. Los serenos estarán formados para informar sobre los medios públicos de transporte, equipamientos y servicios locales. Para ello, recibirán una formación específica y trabajarán en coordinación con la policía local y los Mossos d'Esquadra, a quienes deberán reportar cualquier incidencia de seguridad. Nunca podrán realizar funciones propias de los cuerpos de seguridad.

Además, el proyecto tiene una clara vocación social, ya que se trata de un programa experimental de ocupación para personas en situación de desempleo. Preferentemente mayores de 45 años parados de larga duración.

En Premià de Dalt, una de las poblaciones del Maresme más castigadas por los robos en el interior de los domicilios, el sereno sí complementará la acción de la policía local. Desde hace más de un año trabajan en el proyecto, analizando todos los flecos legales, hasta lograr que la comisión que depende del Departament d'Interior de la Generalitat les dé el visto bueno. El sereno, comenzará a patrullar por las calles premianenses en marzo como prueba piloto. "Después decidiremos cuál es la mejor época para reforzar la vigilancia policial" detalla Josep Triadó, alcalde del municipio, posiblemente entre octubre y marzo, los meses en los que se producen más incidentes.

Según Triadó, los vigilantes "reforzarán la labor policial en horario nocturno" como antaño hacían los serenos tradicionales. Un mínimo de un sereno patrullará a pie cada noche en cada uno de los cuatro barrios de la población. "Pensamos en el sereno del siglo XXI" ya que será un vigilante jurado profesional, equipado con defensas, esposas, medidas para reducir a los delincuentes y una emisora que le conectará con la central de la policía local, que a su vez mantendrá las patrullas habituales. "La finalidad es que siempre sea el mismo sereno", dice el alcalde, para que se establezca una relación de confianza con los vecinos. El Ayuntamiento dispondrá de una bolsa de horas para acceder a los vigilantes que considere necesarios, hasta un máximo de cuatro en cada barrio.

La alerta 4 antiterrorista obliga a los agentes policiales a patrullar de dos en dos, lo que también reduce el número de efectivos. Además, la ley de Racionalización y Sostenibilidad de la Administración Local (LRSAL) popularmente conocida como ley Montoro, impide que los entes locales aumenten la masa salarial aunque estén saneados y con remanente positivo, como el caso de Premià de Dalt. En este municipio de 10.350 habitantes "contratar a los vigilantes privados es un gasto contabilizado en el capítulo dos", que ascenderá a unos 100.000 euros anuales.

En la ciudad de Barcelona, el cuerpo de serenos se disolvió en 1976. El Ayuntamiento integró los cerca de 300 agentes de aquella plantilla en el servicio de funcionarios de vigilancia nocturno y en 1981 pasaron a formar parte de la Guardia Urbana.

Más presión que nunca para el director de seguridad de la información

Fuente: Cinco Días

El año 2019 comenzó con varias de las mayores filtraciones de seguridad de los últimos años, con permiso de Facebook. Una brecha en Fortnite dejó al descubierto hace apenas una semana datos personales y números de tarjetas de crédito de millones de usuarios. Otra, en Amadeus, dejó al aire los datos de millones de pasajeros de avión que volaban con clientes de la proveedora de soluciones tecnológicas. Son solo dos ejemplos recientes de una larga lista que no hace más que aumentar y que pone en peligro la reputación de las organizaciones.

A las empresas les preocupa más que nunca la seguridad y confidencialidad de su información. Así lo refleja un estudio de Capgemini, elaborado junto a IDC, que se presenta este jueves. En términos generales, la mayoría de los directivos a los que ha preguntado la consultora, en un 68% de los casos, coincide en que la importancia de la seguridad de la información ha crecido de forma significativa en los últimos tres años.

Además, se observa que el rol del conocido como director de la seguridad de la información (CISO, por sus siglas en inglés) empieza a concebirse de manera más amplia. Atendiendo a los beneficios que aporta la seguridad de los datos confidenciales al negocio, "entre los directivos pesan más los criterios vinculados a la competitividad que a la protección en sí de los activos", explica Carmen Dufur, directora de estrategia de ciberseguridad de Capgemini España.

Así, el 46% de los más de 1.000 ejecutivos encuestados a nivel mundial considera que la seguridad de la información es determinante para la competitividad de los productos y servicios. Para un 31%, la misión principal es la protección de los intereses del consumidor, seguido de la mejora de la eficiencia (13%). Solo un 10% destaca su papel como mero guardián de los activos corporativos, el papel tradicional de este perfil.

Esto hace suponer que con cada vez más frecuencia las compañías exijan a sus profesionales de la seguridad que vayan más allá, haciendo que estén más presionados que nunca para jugar un papel preponderante en el cambio y la innovación de los negocios. "Esto significa que el CISO moderno debe seguir adaptándose o arriesgarse a ser reemplazado. La empresa ya no se conforma con que siga las decisiones tomadas. Quiere que participe en ese proceso", prosigue Dufur.

Pese a este apremio y presión extra, hay algunos datos que corroboran que la situación no es tan empinada para estos profesionales, según apunta el informe. Como primer apunte, los altos ejecutivos han mejorado su punto de vista sobre esta área, y la mayoría de ellos, en un 86%, "ha dejado de percibirla como el departamento del no". Hace años era muy común que se conociese a esta división con estos términos, ya que estaba muy extendida la idea de que al afán de protección ponía freno a la innovación y al lanzamiento de medidas originales o arriesgadas. Hoy, la visibilidad e influencia del CISO en las empresas ha mejorado con respecto a los últimos tres años: un 77% de los directivos así lo considera, frente al 22% que piensa que su rol sigue siendo el mismo.

"Esto se debe a que hay una mayor concienciación hacia la seguridad. Todas las brechas y fugas de información que estamos viendo han ayudado mucho a ello", esgrime Dufur. En este cambio también han puesto su grano de arena los propios directores de seguridad, "que han optado por acercarse más al negocio y no estar solo pendientes de la seguridad de los activos".

Falta, no obstante, mucho por hacer. Es necesario, explica Dufur, que la labor del CISO siga evolucionando y se transforme a sí mismo y a sus equipos para ser conductor del cambio y de la innovación en vez de tener un papel reactivo. Esto requiere de nuevas formas de pensar y nuevas competencias. Para mantener o incrementar su relevancia, estos profesionales deben convertirse en habilitadores de negocios más que en responsables de seguridad. Deben adoptar una mentalidad empresarial e impulsar la transformación digital, no reaccionar ante ella. También deben tener más "presencia en la organización, tejer una red de contactos y evolucionar hacia finanzas, marketing, comunicación y otras habilidades más ligadas al día a día de una empresa".

No hay que olvidar, señala la experta, el papel que puede jugar este perfil a la hora de encontrar oportunidades para el negocio dada su posición y su conocimiento privilegiado. "Debe posicionarse como visionario o experto, así como invertir en añadir valor a las iniciativas de negocio procurando objetivos, asesoramiento y perspectiva imparcial". Por ahora lo tiene todo a su favor. Según los datos de Capgemini, a día de hoy más del 90% de los directivos considera que la influencia del CISO en los comités de dirección es entre media y alta.

Buch resalta la "cooperación" entre policías y vigilantes en el Dia Català de la Seguretat Privada

Fuente: Europa Press

Buch resalta la *"cooperación"* entre policías y vigilantes en el Día de la Seguridad Privada.

El conseller de Interior de la Generalitat, Miquel Buch, ha destacado este jueves en el VI Dia Català de la Seguretat Privada que *"la colaboración y cooperación entre los diferentes colectivos de la seguridad de Catalunya es muy importante"* y que Mossos d'Esquadra, policías locales y vigilantes y profesionales del sector forman parte del modelo catalán de seguridad.

Acompañado del alcalde de Terrassa (Barcelona), Alfredo Vega, Buch ha presidido el evento y la entrega de menciones, y ha agradecido la colaboración del sector de seguridad privada *"en la elaboración del protocolo contra las violencias sexuales en entornos de ocio"*, ha informado el Departamento en un comunicado.

Buch resalta la *"cooperación"* entre policías y vigilantes en el Día de la Seguridad Privada.

Y ha añadido que *"si la libertad de las mujeres está en peligro, la libertad del país está en peligro"*.

Ha defendido que *"el modelo de seguridad en Catalunya ha demostrado ser un modelo de éxito con la colaboración, la información y la corresponsabilidad del sector de la seguridad privada"* y ha terminado agradeciendo a sus profesionales la cooperación con cuerpos policiales y la labor que realizaron tras los atentados del 17 de agosto de 2017 en Barcelona y Cambrils (Tarragona).

Buch resalta la *"cooperación"* entre policías y vigilantes en el Día de la Seguridad Privada.

JARDÍ Y ESQUIUS

El director general de Administración de Seguridad, Jordi Jardí, ha celebrado la *"cooperación público-privada"* que enriquece la seguridad y ha puesto como ejemplo que el Departamento de Interior facilite que municipios sin Policía Local tengan videovigilancia o la puesta en marcha del protocolo contra violencias sexuales en entornos de ocio. Buch resalta la *"cooperación"* entre policías y vigilantes en el Día de la Seguridad Privada.

El comisario jefe de los Mossos, Miquel Esquius, ha destacado que *"las amenazas de los nuevos retos"* sociales obligan a optimizar y coordinar recursos y que todos los actores implicados son necesarios.

Buch resalta la *"cooperación"* entre policías y vigilantes en el Día de la Seguridad Privada

Al acto han asistido, entre otros, el secretario general de Interior, Brauli Duart; el director general de Mossos, Andreu Joan Martínez; la directora del Institut de Seguretat Pública de Catalunya, Montserrat Royes, y el presidente en Catalunya de la Asociación Profesional de Compañías Privadas de Servicios de Seguridad (Aproser), Juan Montero, que ha hablado en nombre de los galardonados.

En el acto se han repartido 124 menciones de Seguridad Privada de Catalunya, entre ellas 66 reconocimientos y 10 distinciones honoríficas por actuaciones con motivo del 17-A.

¿Quienes han de contar con un Delegado de Protección de Datos?

Fuente: click datos

El Delegado de Protección de Datos (DPO por sus siglas en inglés) es una figura que viene creada por el Reglamento General de Protección de Datos (RGPD). Por esta razón, aún hay muchas dudas acerca de este profesional y en este texto, vamos a hablar sobre qué es este profesionalidad y quiénes un Delegado de Protección de Datos necesitan.

¿Qué es el Delegado de Protección de Datos (DPO)?

El DPO es el encargado de garantizar que la nueva normativa de protección de datos se cumpla en la empresa que lo tiene contratado. Lo principal que has de tener claro es que esta persona debe haberse formado para obtener conocimientos especializados de legislación y práctica en materia de protección de datos. Aunque no es necesario que cuente con una titulación específica, tiene que acreditar la tenencia y manejo de estos conocimientos.

Otro dato interesante es que este puede ser una persona externa a la empresa o que trabaje en ella. No obstante, si se opta por designar a un trabajador, este deberá dejar sus otras tareas y centrarse en la gestión de la recogida, almacenamiento y tratamiento de los datos.

Para entender mejor el papel de este profesional en una empresa debemos tener en cuenta sus funciones que son las siguientes:

- Informar y asesorar a los que se ocupen del tratamiento de los datos.
- Supervisión de los protocolos para adaptarlos a la nueva normativa europea y asegurarse que esta se cumple.
- Asesorar acerca de la evaluación del impacto relativa a la protección de datos y supervisión de su aplicación.
- Cooperación con las autoridades pertinentes y nexo de comunicación entre ellos y la entidad para la que trabaje.

Por último, debes tener claro que estas funciones están reguladas en el artículo 39 del RGPD al igual que la obligatoriedad o no de contratar a este profesional.

¿Cuándo es obligatorio contratar a este profesional según el RGPD?

A pesar de que se trata de una figura clave a la hora de mantener bajo control todo lo relacionado con la protección de datos, hay empresas que no están obligadas a tener esta figura. Así pues, vamos a exponer en qué casos sí es obligatorio contar con un DPO.

Artículo 37

Lo primero que has de tener en cuenta son los propios artículos del reglamento. En el número 37 se expone que contratar a este responsable de los datos es obligatorio en tres casos diferentes.

- Cuando se trata de un organismo o entidad pública.
- Cuando las actividades principales del tratamiento sean operaciones que necesiten un seguimiento continuo y sistemático de los interesados.
- Cuando la principal actividad se base en el tratamiento de los datos a gran escala de categorías especiales de datos o de aquellas informaciones relacionadas con condenas y delitos.

Pues bien, en estos supuestos hay que tener muy en cuenta tres factores en los que profundizaremos a continuación.

Actividades principales

Cuando en el artículo 37 del reglamento se habla de actividades principales, se hace referencia a que la recogida, almacenamiento y tratamiento de los datos ha de ser la función principal de la empresa en cuestión. Es decir, que si estos se recogen pero de ello no depende la función de la empresa, no existiría, en principio, necesidad de contratar un DPO. Aunque siempre es positivo contar con asesoramiento profesional.

De esta manera, una empresa que administrara perfiles de personas tendría la obligación de contratar un DPO. Ejemplos de ello son Facebook, 21Buttons, Twitter, Instagram…

Otra cuestión que se pone de manifiesto es el hecho de aquellas empresas en las que la recogida de datos fuese algo primordial. Esto es, sin necesidad de que sea la actividad principal, el desarrollo de la misma necesitase de la recogida

de los mismos. Por ejemplo, los hospitales cumplirían con esta condición ya que, aunque su actividad principal es la de tratar a los pacientes, sin manejar sus datos les sería imposible.

A gran escala

Este es otro de los factores que hay que tener en cuenta. Ciertamente, "a gran escala" es un principio algo confuso. Por ello, ante la confusión se está esperando a que se enumeren momentos en los que se establezcan parámetros más caros.

Hasta ahora, hay que basarse en cuatro puntos clave:

- Número de personas afectadas.
- Volumen de datos o índole de los mismos.
- Duración o permanencia de la actividad de tratamiento.
- Alcance geográfico del tratamiento.

Seguimiento regular y sistemático

Este es el último factor a tener en cuenta. Pero en esta condición encontramos tres factores diferentes.

Seguimiento hace referencia a la monitorización de los datos. Ya sea por la creación de perfiles o para la inclusión de publicidad.

Cuando se hace referencia a "regular", lo que se establece es que este tratamiento se haga de forma continuada o que se produzca en Intervalos concretos de forma recurrente o repetitiva. Es decir, que haya una periodicidad en el tratamiento y recogida de datos.

Por último, la palabra "sistemático" hace referencia a que exista el establecimiento de un sistema preestablecido con una organización o método concreto. Pero además, esta organización debe estar realizada como parte de un plan general de recogida de datos o como una estrategia de la propia empresa.

De esta manera, todas las compañías que cumplan todas o alguna de estas características han de tener claro que tienen que contratar un Delegado de Protección de Datos obligatoriamente.

Más datos interesantes sobre el DPO

Antes de acabar este artículo, no podemos dejar de mencionarte dos cuestiones interesantes sobre este profesional. La primera de ellas es que no puede ser despedido y la segunda que no puede recibir instrucciones por parte de la empresa.

La figura del DPO está completamente blindada para que verdaderamente pueda convertirse en un enclave de control interno. Si la empresa pudiera despedirlo o mandar sobre él, su control se vería coartado por las represalias de la empresa.

Por este motivo, el reglamento deja muy claro la imposibilidad de darle instrucciones sobre su trabajo y, obviamente, de despedirlo. En cualquier caso, lo más importante es contar con verdaderos profesionales.

Ahora que sabes quiénes un Delegado de Protección de Datos necesitan y en qué consiste su labor, te será mucho más sencillo entender quién ha de encargarse de tus datos dentro de las grandes empresas.

¿Cuáles son los elementos fundamentales de la prevención según el Reglamento de los servicios de prevención?

Fuente: IMF Bussines School
Josefina Del Prado

Si hay una normativa de referencia en cuanto a la prevención de riesgos laborales, es el RD 39/1997 por el que se aprueba el Reglamento de los servicios de prevención.

Este ha dado un nuevo enfoque a la prevención de riesgos laborales que debe integrase en el conjunto de actividades y decisiones de la empresa.

El Capítulo I del Reglamento, artículo 1 establece que la integración de la prevención es la primera obligación de la empresa. Además establece como primera actividad de asesoramiento y apoyo, el deber de facilitarle un servicio de prevención. Este servicio debe evitar cumplimientos meramente formales y no eficientes de la normativa.

En el artículo 2 del mencionado capítulo, señala que esa integración se realiza a través del Plan de prevención de riesgos laborales. El cual integra la actividad preventiva de la empresa en su sistema general de gestión. Logrando establecer una política de prevención de riesgos laborales que debe ser aprobado por la dirección de la empresa. Para que posteriormente ser asumido por toda su estructura organizativa.

Plan de prevención y los elementos fundamentales de la prevención

El plan de prevención de riesgos laborales habrá de reflejarse en un documento que incluirá los siguientes elementos:

- La identificación de la empresa, de su actividad productiva. A eso agregarle el número y características de los centros de trabajo y el número y característica relevantes de los trabajadores.
- La estructura organizativa de la empresa, identificando las funciones y responsabilidades que asume cada uno de sus niveles jerárquicos. Igualmente señalar los cauces de comunicación entre ellos, en relación con la prevención de riesgos laborales.
- La organización de la producción en cuanto a la identificación de los distintos procesos técnicos, las prácticas y los procedimientos organizativos existentes en la empresa. Siempre que estén relacionados con la prevención de riesgos laborales.
- La organización de la prevención en la empresa, indicando la modalidad preventiva elegida y los órganos de representación existentes.
- La política, los objetivos y metas que en materia preventiva pretende alcanzar la empresa. Así como los recursos humanos, técnicos, materiales y económicos de los que va a disponer al efecto.

En el Capítulo II se establecen los dos elementos básicos de actuación preventiva: la evaluación de riesgos y la planificación de la acción preventiva.

Evaluación de los riesgos laborales

Según el artículo 3 del RD 39/1997, es el proceso dirigido a estimar la magnitud de aquellos riesgos que no hayan podido evitarse. Gracias a la cual se obtiene la información necesaria para analizar las condiciones actuales y poder tomar una decisión apropiada sobre la necesidad de adoptar medidas preventivas y sobre el tipo de medidas que deben adoptarse.

Así, la evaluación pondrá de manifiesto las situaciones para:

- Eliminar o reducir el riesgo, mediante medidas de tipo:
  - De prevención en el origen.
  - Organizativas.
  - Protección colectiva, de protección individual.
  - De formación e información a los trabajadores.

- Controlar periódicamente:
  - Las condiciones.
  - La organización y los métodos de trabajo.
  - El estado de salud de los trabajadores.

Planificación de la actividad preventiva

¿Cuándo planificar la actividad preventiva?

El artículo 8 del Reglamento de los Servicios de Prevención expone que el empresario planificará la actividad preventiva que proceda con objeto de eliminar o controlar y reducir dichos riesgos. Siempre y cuando el resultado de la evaluación pusiera de manifiesto situaciones de riesgo. Conforme a un orden de prioridades en función de su magnitud y número de trabajadores expuestos a los mismos.

El artículo 9 del citado Reglamento continúa diciendo:

1. La planificación de la actividad preventiva incluirá, en todo caso, los medios humanos y materiales necesarios. Así como la asignación de los recursos económicos

precisos para la consecución de los objetivos propuestos.
2. Igualmente, habrán de ser objeto de integración en la planificación de la actividad preventiva de emergencia y la vigilancia de la salud.
3. La actividad preventiva deberá planificarse para un período determinado. Logrando establecer las fases y prioridades de su desarrollo en función de la magnitud de los riesgos y del número de trabajadores expuestos.

Como organizar la prevención según el Reglamento

La organización de los recursos para las actividades preventivas está regulada en el CAPÍTULO III del Real Decreto 39/1997. La organización de los recursos necesarios para el desarrollo de las actividades de prevención se realizará por el empresario de acuerdo con algunas de las siguientes modalidades:

Asunción personal por el empresario

El empresario podrá desarrollar personalmente la actividad preventiva, con excepción de las actividades relativas a la vigilancia de la salud de los trabajadores, cuando concurran las siguientes circunstancias:

- Que se trate de una empresa hasta 10 trabajadores.

La ley 14/2013 introduce una reforma en este sentido y modifica el artículo 30.5, que queda redactado del siguiente modo:

"En las empresas de hasta diez trabajadores, el empresario podrá asumir personalmente las funciones señaladas en el apartado 1, siempre que desarrolle de forma habitual su actividad en el centro de trabajo y tenga la capacidad necesaria, en función de los riesgos a que estén expuestos los trabajadores y la peligrosidad de las actividades, con el alcance que se determine en las disposiciones a que se refiere el artículo 6.1.e) de esta Ley. La misma posibilidad se reconoce al empresario que, cumpliendo tales requisitos, ocupe hasta 25 trabajadores, siempre y cuando la empresa disponga de un único centro de trabajo.» siempre que:

- Las actividades desarrolladas por la empresa no estén incluidas en el Anexo I del Real Decreto 39/97. (Este anexo I recoge un determinado número de actividades laborales consideradas peligrosas).
- Que desarrolle de forma habitual su actividad profesional en el centro de trabajo.
- Que tenga la capacidad correspondiente a las funciones preventivas que va a desarrollar, de acuerdo con el capítulo VI del Real Decreto 39/97.

La vigilancia de la salud de los trabajadores, así como aquellas otras actividades preventivas no asumidas personalmente por el empresario, deberán cubrirse mediante el recurso a alguna de las distintas modalidades de organización preventiva.

Designación de los trabajadores, capacidad y medios de éstos

El empresario designará a uno o varios trabajadores para ocuparse de la actividad preventiva en la empresa.

Las actividades de prevención, para cuya realización no resulte suficiente la designación de uno o varios trabajadores. Estas actividades deberán ser desarrolladas a través de uno o más servicios de prevención, propios o ajenos.

Servicios de Prevención Propios (SPP)

El empresario deberá constituir un SPP cuando concurra alguno de los siguientes supuestos:

- Sea una empresa de más de 500 trabajadores.
- Que, tratándose de empresas de entre 250 y 500 trabajadores, desarrollen alguna de las actividades de especial peligrosidad, incluidas en el Anexo I.
- Que, tratándose de empresas no incluidas en los apartados anteriores, si así lo decide la autoridad laboral.

Actividad preventiva en manos de un servicio de prevención ajeno

Cuando el empresario no cuente con suficientes recursos propios para el desarrollo de la actividad preventiva. Deberá desarrollarla a través de uno o varios servicios de prevención ajenos a la empresa. Lo que deberá concertar por escrito.

Son más las indicaciones que se hacen en esta normativa, todas de gran repercusión. Una de ellas es el referido al contenido mínimo de la formación a nivel básico y superior y las funciones que pueden desempeñar cada nivel formativo, o la referida a las auditorias del sistema de gestión de la prevención.

El Reglamento desde su aparición ha sufrido diversas modificaciones entre ellas destacan la introducida por el RD 337/2010 y el RD 604/2006.

¿Sabes cómo mejorar la ciberseguridad de tu organización? Implanta un Plan Director de Seguridad

Instituto Nacional de Ciberseguridad

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Cuando hablamos de ciberseguridad, dar el primer paso puede resultar algo complejo ya que seguramente serán varios los aspectos que se puedan y deban mejorar. Entonces, ¿por dónde empezar? Si queremos llevar a buen puerto la ciberseguridad de nuestra organización, será necesario crear en primer lugar una hoja de ruta. Además, será muy importante no salirse de ella, ya que esta nos ayudará implementar las mejoras que realmente son importantes. A esta hoja de ruta se la conoce como Plan Director de Seguridad.

¿Qué es un Plan Director de Seguridad?

Aunque os hemos hablado de él en unas cuantas ocasiones, os recordamos que un Plan Director de Seguridad es una estrategia con la que abordar los aspectos técnicos, legales y organizativos que ayudarán a mejorar la ciberseguridad de la organización. Para empezar con este plan será imprescindible contar con el compromiso de la dirección e identificar las prioridades, responsables y recursos que se destinarán.

¿Por dónde comienzo?

La primera etapa de un Plan Director de Seguridad consistirá en recolectar información con la que determinar cómo está la situación actual en la empresa y dónde se quiere llegar en materia de ciberseguridad, marcando siempre unos objetivos razonables y sobre todo, realistas. Puesto que las organizaciones pueden ser muy diferentes, cada una contará con unos activos, procesos de negocio, así como responsables de los mismos, ya que no existe una fórmula magistral que sirva para todas las empresas.

Para realizar una valoración inicial sobre la ciberseguridad de la organización se suele utilizar como referencia el estándar internacional ISO/IEC 27002:2017, el cuál reúne un Código de Buenas Prácticas para la Gestión de la Seguridad de la Información. Desde INCIBE, hemos desarrollado una herramienta de autodiagnóstico para ayudar a las pymes a realizar esta tarea de evaluación sobre la ciberseguridad de la organización. Mediante un sencillo y breve cuestionario se determinará el estado actual de la seguridad de la información, indicando los riesgos existentes y los aspectos a mejorar.

Una vez realizada la valoración inicial en base al estándar ISO se ha de crear un nuevo documento denominado «Declaración de Aplicabilidad» o «SOA - Statement of Applicability» que recogerá los controles o medidas de seguridad que se deberán aplicar. En este documento también se deberá incluir su grado de madurez, es decir, si están implantados y en su caso, en qué nivel se encuentran.

Mantener reuniones con el personal de la organización será imprescindible, ya que el punto de vista de las personas que realizan las tareas diarias puede ser muy esclarecedor sobre el tipo de información que se gestiona, cómo es tratada y que medidas de seguridad sería recomendable aplicar para protegerla.

Una vez se cuenta con la información sobre las deficiencias detectadas se han de analizar y establecer una escala de madurez, por ejemplo estableciendo un valor numérico como de 0 a 5, siendo el primero la ausencia total de control y el segundo valor, la optimización total del control.

También habrá que realizar un análisis de riesgos donde se identifiquen las principales amenazas que afectan a la organización y el riesgo asociado a cada una de ellas, en función de la probabilidad y el impacto que tengan de materializarse. Desde INCIBE facilitamos una plantilla ejemplo para esta tarea.

El último paso dentro de esta fase inicial será determinar cuáles son los objetivos a cumplir en materia de seguridad, siempre en base a la estrategia marcada por la organización, para mitigar los riesgos a los que están expuestos los activos críticos.

Determinar los objetivos y puesta en marcha

En la medida de lo posible, deberemos estimar el coste de las iniciativas propuestas en términos temporales y económicos, contemplando los recursos materiales y humanos, tanto a nivel interno como externo. Una vez identificadas hemos de clasificarlas y priorizarlas. Puede darse el caso que las acciones a tomar sean de índole variada, por lo que ante esta situación, es recomendable realizar grupos que homogeneicen el conjunto de proyectos definidos.

Para realizar esta clasificación, se pueden considerar varios criterios, pero con independencia de ellos, será conveniente agrupar los proyectos atendiendo al esfuerzo que requieren, tanto a nivel humano como económico y en función de su coste temporal. De este modo, se establecerán proyectos a corto, medio y largo plazo.

Una vez se haya elaborado el Plan Director de Seguridad, tendrá que ser revisado y aprobado por la dirección de la organización. Superado este trámite, llega el momento de poner en marcha todas las medidas tomadas en consideración, siendo recomendable realizar una presentación ante los miembros de la organización que se verán afectados por las mismas. También es recomendable asignar responsables y coordinadores de proyecto y establecer la periodicidad con la que se llevará a cabo las acciones de seguimiento por medio de hitos.

Siempre debemos tener presente que un Plan Director de Seguridad, se basa en la mejora continua. Por tanto, cuando hayamos finalizado el plan actual debemos comenzar de nuevo el ciclo, ya siempre existe margen de mejora.

Un Plan Director de Seguridad es una estrategia fundamental que toda organización debe tener presente, ya que la supervivencia de la misma puede depender de las acciones que se hayan llevado a cabo o no. Ponte manos a la obra y comienza con tu Plan Director de Seguridad.

twitter

Queremos recordarte nuestra nueva herramienta de información inmediata y constante del sector, y para todos nuestros Socios y Amigos, a través del Twitter; nos encontrareis aquí: http://twitter.com/ADSI_ES

Asociación de Directivos de Seguridad Integral
ADSI

@ADSI_ES

Primeros pasos para mejorar la seguridad de nuestros datos

Fuente: Oficina de Seguridad del Internauta

Las formas de ataque que pueden utilizar los ciberdelincuentes son muy variadas. En muchas ocasiones se aprovechan de nuestro desconocimiento para perpetrar sus ataques a nuestros dispositivos sirviéndose de técnicas de ingeniería social. Es por ello que debemos estar siempre atentos mientras navegamos o utilizamos dispositivos o servicios en Internet.

A pesar de esto, no hay que preocuparse en exceso ni dejar de utilizar Internet, siempre que utilices tu sentido común y tengas en mente una serie de pautas y buenas prácticas en materia de ciberseguridad que te aconsejamos:

Analiza las descargas y dispositivos que conectes a tus equipos con un antivirus

Las descargas desde páginas web o plataformas no oficiales pueden contener una gran variedad de tipos de virus y malware. Para evitarlo, además de usar siempre repositorios de confianza y sitios web legítimos, es muy recomendable que todas las descargas que realices las analices con un antivirus actualizado y oficial.

Evidentemente el mismo consejo aplica a descargarse un antivirus de un sitio no confiable ya que podría estar infectado y ser realmente un virus. Hay varias versiones gratuitas de antivirus oficiales por lo que, al menos, puedes usar una de ellas.

Estos consejos de análisis de archivos también se aplican a los que introducimos por otros medios, como puede ser el correo electrónico o un dispositivo conectado como un USB o un disco duro. Incluso si el USB es tuyo, debes tener especial cuidado si se los dejas a un conocido o familiar ya que puede tener su equipo infectado y transmitir la infección al tuyo.

Comprueba las páginas y los correos antes de dar información confidencial

Existen multitud de tácticas con las que los ciberdelincuentes buscan hacernos caer en la trampa y conseguir nuestros datos. Podemos encontrar desde correos falsos simulando ser bancos (phishing), hasta páginas web falsas que aparentan ser redes sociales u otro tipo de servicios conocidos.

El objetivo en la mayoría de los casos es lograr que el usuario proporcione su información confidencial, como datos bancarios, nombre de usuario o contraseñas, y después venderla o aprovecharla para cometer un delito. Para evitar este tipo de ataques debemos fijarnos en los siguientes puntos que los delatan:

1. **Faltas de ortografía:** Errores gramaticales o de ortografía en el contenido de las páginas web o de los correos pueden delatar al ciberdelincuente que intenta hacernos caer en su trampa. Algunos ejemplos son:
   - Frases mal construidas o con prisas: “Usted le damos las bienvenids por participar el concurso…”
   - Símbolos extraños incluidos en el texto: “Haga clic en el enlace incluido en la descripciÃ?n…”
   - Errores semánticos: “La agradecemos su interés…”

2. **Remitente o dirección web:** El remitente no se corresponde con la entidad a la que hace alusión el cuerpo del email. Por ejemplo, si se trata de un email oficial de nuestro banco, esperamos que la dirección sea “@tubanco.com” y no algo como “@xxtubanco.com”. Por

otro lado, lo mismo debemos comprobar en el enlace a una dirección web que no sea de confianza.

3. **HTTPS:** El sitio web no soporta HTTPS o el certificado no es de confianza. Esto es especialmente importante para sitios donde se autoriza un pago o páginas que recojan nuestros datos bancarios, ya que de no utilizar HTTPS sabremos con seguridad que no son fiables.

4. **Irregularidades:** Ausencia del contenido habitual de la página web o cambios sospechosos. Puede que un email de nuestro banco se refiera a nosotros como "Querido usuario" a pesar de que en el resto de los emails recibidos se refieran a nosotros por nuestro nombre y apellidos, o que el aspecto gráfico de la dirección web a la que nos enlazan parezca hecho con prisas.

Mejora la seguridad en tus contraseñas

Contraseña segura: C0ntr4sena_S3GuR4

Contraseña no segura: contraseña

Es muy probable que tus contraseñas puedan ser un poco más seguras de lo que son actualmente. Tu contraseña debe ser robusta ya que algunos ataques se basan en probar, mediante programas informáticos, miles de combinaciones por minuto.

Lo ideal si tienes varias y te cuesta recordarlas es utilizar un gestor de contraseñas. Además, cada vez más servicios por Internet ofrecen la posibilidad de emplear un doble factor de autenticación. Si consideras que la información o el uso que das a ese servicio es importante para ti, te recomendamos utilizarlos.

Por último, no te olvides de cambiar las contraseñas cada cierto tiempo. Esto se hace especialmente importante si sale alguna noticia donde se informa de que se han comprometido determinadas cuentas de un servicio que estés usando.

Tus dispositivos que estén actualizados

Las actualizaciones de los programas/aplicaciones y del sistema operativo suelen aparecer por varias razones: incluir nuevas funcionalidades, solventar fallos o resolver vulnerabilidades de seguridad. Por este motivo es recomendable instalar las actualizaciones lo antes posible para poder disfrutar de las funcionalidades de los programas y servicios que utilizamos gozando siempre de la máxima seguridad posible.

Cuidado con las modas

Dado que el objetivo de los ciberdelincuentes suele ser causar el mayor impacto posible, es importante prestar algo más de atención cuando vemos, descargamos o utilizamos contenido novedoso. Por ejemplo, una nueva aplicación que esté siendo muy descargada o un portal web 'trending-topic' serán lo primero que intenten imitar y falsificar para tratar de infectar a los usuarios.

Por ejemplo, durante el mundial de Rusia de 2018, se enviaron emails de phishing donde anunciaban a sus víctimas que habían sido los ganadores de viajes gratis a Moscú para poder ver a su selección. En plena fiebre por el fútbol, los ciberdelincuentes se aprovechaban del evento más popular del momento para sustraer toda la información personal posible de sus víctimas.

Como usuarios debemos contrastar toda esta información con fuentes de confianza y sobre todo, no hacer nada sin estar 100% seguros de su fiabilidad.

Mantente al día con las noticias de ciberseguridad

Desde la OSI trabajamos día a día para que el ciudadano tenga toda la información necesaria con la que mantenerse actualizado en materia de ciberseguridad. Puedes acceder a nuestro sitio web para conocer casos reales, noticias de actualidad e información básica que te ayudará a estar protegido frente a las ciberamenazas.

Nosotros, como usuarios, también debemos participar de forma activa en la lucha contra los ciberdelincuentes. Sigue estas pautas para mejorar la seguridad en tus dispositivos.

Noticias

El Govern pone en marcha un protocolo para dar criterios operativos a los profesionales de la seguridad para establecer las pautas de actuación contra las violencias sexuales en entornos de ocio.

La consejera de la Presidencia y portavoz del Gobierno, Elsa Artadi, y el consejero de Interior, Miquel Buch, acompañados de la presidenta del Instituto Català de les Dones, Nuria Balada; y el director general de la Administración de Seguridad, Jordi Jardí, presentaron ayer las actuaciones que se llevarán a cabo una vez el protocolo de seguridad contra las violencias sexuales en entornos de ocio ha sido validado por todos los sectores implicados con un amplio consenso.

El objetivo de este protocolo es hacer constar que todas las violencias sexuales es necesario erradicarlas y dar criterios operativos a los profesionales de la seguridad para establecer las pautas de actuación ante estas conductas infractoras.

El mencionado protocolo coordina todos los actores en seguridad (Policía de Cataluña, formada por el cuerpo de Mossos d'Esquadra y las policías locales; policías portuarias y profesionales de la seguridad privada) con otros actores que tienen incidencia en el ámbito de la seguridad y del ocio (cargos electos, técnicos municipales), junto con otros profesionales y personas que prestan sus servicios en el ámbito del ocio (personal de sala, camareras y camareros, personal de control de acceso, auxiliares de servicios, etc.), para que ningún hecho se escape de su conocimiento y se establezca cuál es el papel que cada una de estas personas tiene que tener a la hora de prevenir, pero también a la hora de reaccionar ante este tipo de violencias.

La formación de los cuerpos policiales y de los cargos electos tendrá lugar en el Instituto de Seguridad Pública de Cataluña y en el caso del personal de los locales de ocio irá a cargo del departamento de Interior, encargado de impulsar esta formación, en coordinación y colaboración con las entidades y organismos que corresponda, especialmente el Instituto Català de les Dones.

La formación será obligatoria para el personal al servicio de las diferentes entidades, públicas o privadas, que quieran adherirse al protocolo. Los profesionales que tienen que recibir esta formación serán tanto los que prestan sus servicios en el marco de la seguridad, como las diferentes categorías de personal que trabaja en las actividades de ocio.

En el enlace siguiente donde encontraran todos los detalles de la noticia así como el redactado del protocolo (documento PDF):

Presentación del Protocolo contra las violencias sexuales en entornos de ocio.

Formación

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

Más Información en el siguiente enlace

Oferta formativa de la Escuela de Prevención y Seguridad Integral

La **Escola de Prevenció i Seguretat Integral (EPSI)**, adscrita a la Universitat Autònoma de Barcelona, ofrece estudios universitarios en el ámbito de la prevención y la seguridad integral.

Programa en el siguiente enlace

Legislación

RESOLUCIÓN DE 21 DE NOVIEMBRE DE 2018, DE LA SECRETARÍA DE ESTADO DE SEGURIDAD, POR LA QUE SE APRUEBAN LAS BASES DE LAS CONVOCATORIAS DE PRUEBAS DE SELECCIÓN PARA VIGILANTE DE SEGURIDAD Y SU ESPECIALIDAD DE VIGILANTE DE EXPLOSIVOS Y ESCOLTA PRIVADO, PARA EL AÑO 2019.

PDF de la disposición en el siguiente enlace

CÓDIGO DE DERECHO DE LA CIBERSEGURIDAD.

PDF de la disposición en el siguiente enlace

Revistas

Seguritecnia Nº 460. Enero

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

- **Editorial:** Incertidumbre
- **Seguripress**
- **Especial:** Ciberseguridad
- **Entrevista:** Fernando Sánchez. Director del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC)

Enlace: ver revista digital

Cuadernos de Seguridad Nº 339. Diciembre

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:** «Un año para el avance y la innovación».
- **En Portada:** «Seguridad bancaria: una visión integral».
- **Entrevistas:** «Álvaro Echevarría Arévalo. Director de Seguridad y Servicios Corporativos Banc Sabadell».
- **Artículos:** «En la senda de la digitalización... con reparos, por Juan Manuel Zarco».

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.

La opinión manifestada por los autores de los artículos publicados a título personal que se publican en este medio informativo no necesariamente se corresponde con la de ADSI como Asociación.

Esta comunicación se le envía a partir de los datos de contacto que nos ha facilitado. Si desea cambiar su dirección de correo electrónico dirija su petición por correo postal a "ADSI - Asociación de Directivos de Seguridad Integral", Gran Via de Les Corts Catalanes, 373 – 385, 4ª planta, local B2, Centro Comercial "Arenas de Barcelona", 08015 - Barcelona, *o mediante e-mail a* secretario@adsi.pro .

Si o no desea recibir nuestros mensajes informativos utilice los mismos medios, haciendo constar como asunto "DAR DE BAJA". Su petición será efectiva en un máximo de diez días hábiles.