REVISTA

SEGURIDAD PROFESIONAL

Septiembre 2021 Edición Nº6

CIBERSEGURIDAD

Secretos empresariales, la clave para gestionar la seguridad de la información

NOTICIAS

Las redes sociales no son un juego – Canal prioritario

ENTREVISTA

Daniel Oliva, Director de Seguridad de Ferrocarrils de la Generalitat de Catalunya

PSICOLOGÍA

Características del Trastorno Límite de La Personalidad.

JPETER KÜRTEN, EL VAMPIRO DE DÜSSELDORF

CRÉDITOS

DIRECCIÓN
Antonio Cedenilla

EQUIPO DE DESARROLLO
Social Media
www.socialmediaspain.es

EDITOR
Sergi Tarrida

DISEÑO Y MAQUETACIÓN
Katherine Balliache

¿Que es AJDSE?

AJDSE, es una asociación Nacional e Internacional, es un centro de formación, es un centro Nacional de ciberseguridad, es una entidad asociada a una patronal, es una revista de seguridad y ahora a partir de octubre un programa de radio, denominado

AJDSE también es un sello de calidad en los servicios de Seguridad. AJDSE también es un sello de reconocimiento de profesionalidad

Visita Nuestra Página web www.ajse.es

AJSE-ISCA FIRMA UN CONVENIO CON LA UNIVERSIDAD EUROPEA DE ANDORRA

UNIVERSITAT EUROPEA
UNIVERSIDAD EUROPEA
EUROPEAN UNIVERSITY
Principat d'Andorra

Peter kürten, el vampiro de düsseldorf

Este oscuro personaje pasó más de veinte años perpetrando los más horrendos crímenes, hasta que finalmente fue juzgado y hallado culpable de nueve asesinatos y de otros siete en grado de tentativa, por lo que fue guillotinado en 1931 y su cerebro estudiado por la ciencia.

Imagen de Peter Kürten, el vampiro de Düsseldorf, tomada para la ficha policial tras su detención en 1931.

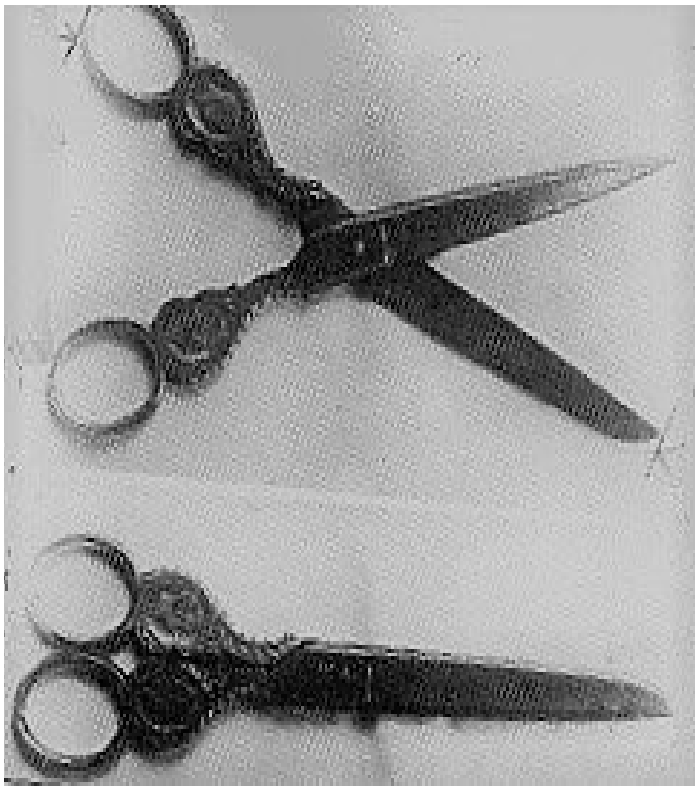
mayo del año 1930. La esposa de Peter Kürten pensó que su marido le estaba gastando una pesada broma cuando, mientras estaban sentados en el salón de su casa, éste le confesó que era la personificación del mal, la "Bestia de Dusseldorf". La mujer amagó con levantarse con una sonrisa en los labios, pero Peter la contuvo con un ademán de su mano y continuó con su historia. Erguido, serio y con las amarillentas mejillas maquilladas, Peter contó a su esposa el inmenso placer que le proporcionaba (prácticamente desde el año 1913) el hecho de apuñalar con un cuchillo o unas tijeras o apretar con sus manos desnudas las gargantas de mujeres jóvenes. Incluso se ha llegado a decir que Kürten pidió a su esposa que lo entregase ella misma a la policía para así poder cobrar la recompensa que se ofrecía por él.

UNA INFANCIA DESGRACIADA

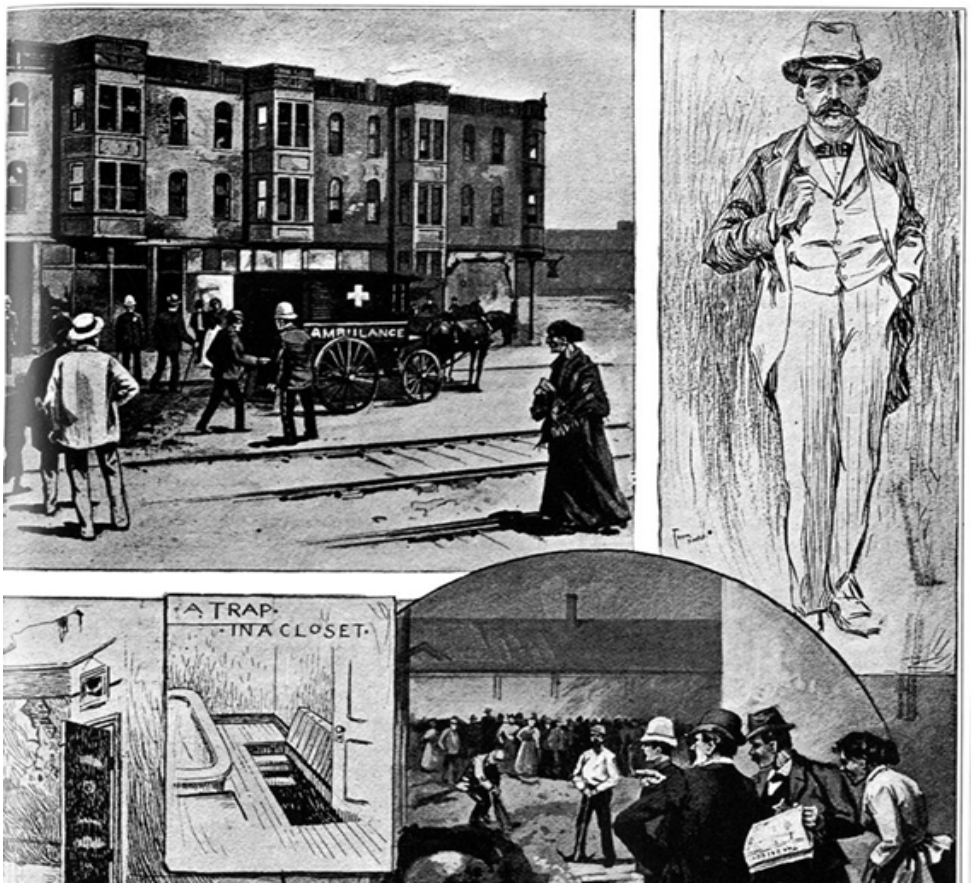
Nacido el 26 de mayo de 1883 en Mulheim, Peter Kürten era el tercero de trece hermanos. Al igual que éstos, Peter no fue bien recibido por sus padres. Su familia vivía en la miseria más absoluta y cada día era un desafío contra el hambre. En medio de la violencia física y psicológica, Peter vio como su padre, un alcohólico, daba palizas a su madre y no dudaba en abusar de sus hermanas. Con sólo nueve años, el niño decidió escapar de su casa de Düsseldorf, donde la familia se había mudado, para huir del dolor, la tristeza y la violencia extrema que habían convertido su vida en algo insoportable. Aunque sabía que lo que sucedía en su casa no era normal, en su interior fue arraigando un sentimiento que parecía empujar al joven hacia una vida marcada por la delincuencia y la violencia. Parece ser que al poco tiempo de abandonar su hogar asesinó a dos amigos ahogándolos en el río (aunque se carecen de registros policiales que puedan corroborar estos hechos). Tuvieron que transcurrir algunos años más para que Peter volviera a matar.

Con nueve años, Peter decidió escapar de su casa de Düsseldorf para huir del dolor, la tristeza y la violencia extrema que habían convertido su vida en algo insoportable.

El 25 de mayo de 1913, Peter Kürten, un hombre de treinta años, vivía de lo que robaba. Un día, estaba vigilando una casa presuntamente vacía para entrar a robar. Pero cuando entró para desvalijarla, se dio cuenta que en su interior se encontraba una niña de trece años llamada Khristine Klein, que estaba durmiendo en su habitación. Tras comprobar que no había nadie más en la casa, la estranguló y degolló. En palabras del propio asesino: "Entre en una casa de Wolfstrasse, cuyo inquilino erra de apellido Klein, fui hasta la primera planta. Abrí varias puertas y no encontré nada digno de robar, pero en la cama vi a una muchacha durmiendo de aproximadamente diez años cubierta con una cobija gruesa de plumas. Tenía un pequeño cuchillo en el bolsillo con el cual corté su garganta. Oí los chorros y el goteo de la sangre en la estera al lado de la cama...". El padre de la niña, Peter Klein, fue acusado del asesinato de su propia hija ya que Kürten (quien ya desde un primer momento mostró señales inequívocas de un trastorno narcisista) dejó en la escena del crimen un pañuelo con sus iniciales, PK, que casualmente coincidían con las del padre.



Estas fueron las tijeras que peter kürten utilizó para perpetrar varios de los asesinatos que cometió.



frente a los agentes, Kürten les envió un mapa donde indicaba el lugar en el que había arrojado el cadáver de una niña llamada Gertrude Albermann. En aquellos momentos, las comisarías alemanas se encontraban colapsadas por la enorme cantidad de denuncias que llegaban con los nombres de posibles sospechosos.

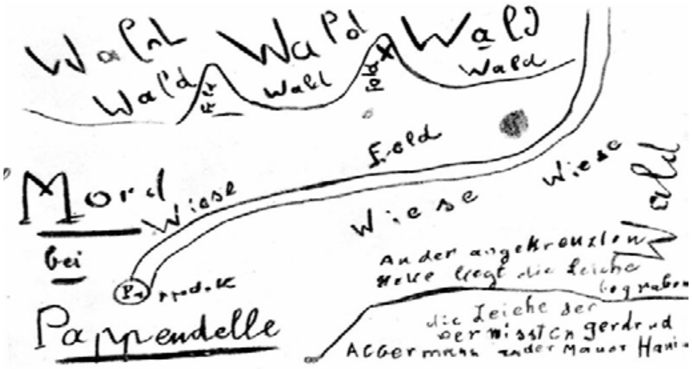
Las siguientes víctimas serían dos hermanas a las que mutiló y a partir de este entonces empezaría a experimentar bebiendo la sangre de sus víctimas.

EGO DESMESURADO

Dos meses después, Kürten encontró a su siguiente víctima. En un nuevo asalto domiciliario, el asesino se topó con la joven Gertrud Franken, de 17 años, a la que estranguló con sus propias manos. Aquel fue el punto de inflexión que marcaría el inicio de una serie de asesinatos que aterrorizarían a la ciudad de Düsseldorf. Kürten (que anteriormente había disfrutado matando y torturando animales) empezó a asesinar seres humanos. Las siguientes víctimas serían dos hermanas a las que mutiló, y a partir de entonces dio un paso más en su locura criminal: empezó a beber la sangre de sus víctimas.

Entre los meses de febrero y noviembre de 1929, Kürten, con el ego desatado (algo muy habitual entre los asesinos en serie), empezó a poner en jaque a la policía, burlándose de ella. En su afán por reafirmar su superioridad

Pero en 1930, un error fatal conduciría al brutal asesino ante un tribunal. Kürten se había fijado en María Büdleick una joven de veinte años que acaba de bajar del tren justamente en la estación de la ciudad donde él "actuaba". Irónicamente, Kürten salvó a Büdleick de un acosador que la estaba molestando y se ofreció a acompañarla hasta la residencia de estudiantes. Sin embargo, Kürten se las ingenió para llevarla hasta su casa, donde se insinuó a la joven y fue rechazado. Kürten entonces se ofreció a llevarla, esta vez sí, hasta la residencia de estudiantes, pero, en lugar de eso, la condujo hasta un bosque a las afueras de la ciudad, donde la violó y la estranguló, dándola por muerta. La fortuna acompañó a la joven, que sobrevivió a la agresión y acudió a la policía a denunciar los hechos. Pocos días después, Kürten era detenido.



Sketch enclosed by Kürten in the "murder letter", indicating where the body of Gertrude Albermann would be found

Tras el asesinato de una niña llamada gertrude albermann, el vampiro de düsseldorf dejó este mapa indicando dónde se podía encontrar el cadáver de su víctima.
Foto: cordon press

Los pecados capitales del padre Hans Schmidt

EL CAZADOR CAZADO

Los interrogatorios dieron a Kürten la oportunidad de satisfacer de nuevo su enorme ego. Durante las sesiones, confesó alrededor de setenta actos criminales entre los que se incluían agresiones sexuales, asesinatos y actos de piromanía. Decía que a veces prendía fuego a edificios abandonados "con la esperanza de ver salir ardiendo del interior a vagabundos que pernoctasen dentro". Entre sus fetiches se encontraba la sangre: decía que le proporcionaba un gran placer estar en contacto con ella y que a veces la bebía. Este trastorno se denomina hematodipsia o vampirismo clínico, y ha sido frecuente diagnosticado en otros personajes históricos y asesinos en serie como la condesa húngara del siglo XVI Elizabeth Bathory.

Tras escuchar las terribles declaraciones del acusado, el jurado no dudó en condenarlo a muerte al considerarlo culpable de nueve asesinatos. Kürten no protestó ni intentó apelar, aceptando la pena en silencio. Su ejecución por guillotina se fijo para el 2 de julio de 1931, en Colonia. Su estado de enajenación mental y el grado de trastorno del personaje quedó en evidencia tras sus últimas palabras antes de morir. Visiblemente intrigado preguntó a su verdugo: "¿Después de que me cortéis la cabeza… podré oír como brota la sangre de mi cuello?".

Entre los fetiches de Kürten se encontraba la sangre: decía que le proporcionaba un gran placer estar en contacto con ella y que a veces la bebía.

Todos los psiquiatras del país se mostraron muy intrigados con el caso, y el análisis clínico de las actividades del que fue bautizado como el "vampiro de Düsseldorf" servirían para poner las bases de numerosos estudios en el campo de la psiquiatría que tenían el objetivo de explicar la psicología de un asesino en serie y elaborar diversos perfiles criminales. Los psiquiatras, profundamente intrigados por la psicopatía y la anatomía del cerebro de Kürten, no dudaron en solicitar a las autoridades la cabeza cercenada del asesino para estudiar su cerebro, a lo que la justicia alemana no puso inconvenientes. A día de hoy, la cabeza del "vampiro de Düsseldorf se exhibe en el Museo Ripley's de Wisconsin Dells, en Estados Unidos, como una curiosidad histórica, dentro de una caja de cristal. Un cartel explica su caso a todos aquellos interesados en su vida y en su perfil criminal.

Secretos empresariales, la clave para gestionar la seguridad de la información

Jose María del Valle, Director de CLARKE MODET

Seguro que a muchos de vosotros, cuando os preguntan qué es la propiedad industrial e intelectual, os vienen a la mente conceptos como el de patente o incluso la marca.

Efectivamente, esas son formas muy habituales de protección del conocimiento y, más concretamente, herramientas de protección de propiedad industrial que otorgan una exclusiva a su titular, lo que le permite poder actuar contra los terceros que infrinjan su derecho de patente o marca. Eso es lo que las hace especialmente importantes e interesantes para las empresas.

Sin embargo, si os preguntasen por otro tipo de herramientas de protección del conocimiento, estoy convencido de que, aunque os sonase el secreto empresarial, pocos serían capaces de decir en qué consiste esa figura y qué es lo que tengo que hacer para protegerlos en mi empresa.

Muchos recordaréis el clásico ejemplo de la fórmula de la Coca-Cola, secreto empresarial por antonomasia y sobre el que circulan más leyendas urbanas que realidades.

Pero el número de ejemplos conocidos de secretos empresariales es incalculable, y entre ellos podemos mencionar también el caso del algoritmo de Google o la receta del Kentucky Fried Chicken, que seguro también os resultarán familiares.

Lo importante es que el secreto empresarial podemos encontrarlo en cualquier sector o ámbito de la economía. Se da en el mundo de las tecnologías de información y la comunicación con algoritmos o software, en el mundo de la alimentación con recetas o fórmulas alimenticias o en el sector de la automoción o la industria con procedimientos de fabricación, por solo poner unos ejemplos. Pero, además, el secreto empresarial es muy transversal, puesto que puede abarcar cualquier tipo de información dentro de la empresa, siempre y cuando genere una ventaja competitiva para la misma. Así, también podría constituir secreto empresarial un listado de clientes, un plan de negocio, unas tarifas de la empresa, una base de datos, un informe de ventas o un proceso o sistema interno de fabricación.

También os puede venir a la cabeza el tema del espionaje industrial, que en muchos de los casos implica una vulneración de un secreto empresarial y, por lo tanto, perseguible según esa figura.

Desde el punto de vista de la seguridad, es muy importante regular las condiciones de seguridad en el acceso a lo que consideramos que es nuestro secreto empresarial.

Para ello, tanto los tribunales como la nueva Ley de Secretos Empresariales -que entró en vigor en España en marzo de 2019 como

trasposición de una Directiva comunitaria de 2016-, establecen las condiciones del tratamiento seguro de la información que consideramos que es secreto empresarial. Si no cumplimos esas condiciones de seguridad en nuestra empresa, es muy probable que ningún Juez nos dé la razón respecto a esa vulneración de nuestro secreto y a ese presunto espionaje industrial.

Por otro lado, nadie está completamente a salvo de sufrir un ciberataque y, en negocios basados en la venta online, cada vez más habituales, se deberá tener en cuenta este riesgo y gestionarlo adecuadamente, ya que en muchos casos la supervivencia del negocio puede depender totalmente de ello.

En este sentido y como es lógico, se deberán implementar medidas técnicas para evitarlos, sin ninguna duda, pero también contar, desde una perspectiva legal, con plan adecuado que permita identificar y gestionar la información confidencial estratégica o secretos empresariales, como comentábamos antes. En este ámbito, es importantísima la concienciación y formación de los empleados tanto en materia de ciberseguridad como en la gestión de este tipo de información, ya que en muchas ocasiones los ciberataques o el filtrado de información sensible provienen de descuidos o desconocimiento de los empleados.

Tan importante como contar con las medidas técnicas para evitar un ciberataque y proteger los datos personales frente a los mismos es contar con plan adecuado para identificar y gestionar la información confidencial estratégica de la organización. Por ello, como comentaba, es fundamental la concienciación y formación de los empleados, no sólo en materia de ciberseguridad y protección de datos, sino también en la identificación y gestión de secretos empresariales. Guiar a los empleados para que conozcan qué información o activos son objeto de secreto y formarles para que puedan identificarlos desde el momento en el que ellos mismos puedan producirlos es esencial.

Por supuesto, también es fundamental establecer todas las medidas técnicas y legales para evitar su divulgación, como una adecuada rotulación de la documentación, sistemas restringidos de acceso y compartición de archivos, sistema de registro de evidencias, firma de acuerdos de confidencialidad con empleados y proveedores, etc.

Así, en la Ley anteriormente comentada de Secretos Empresariales se define el secreto empresarial como cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero, que reúna las siguientes condiciones:

- Ser secreto, en el sentido de que, no es generalmente conocido por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesible para ellas.

- Tener un valor empresarial, ya sea real o potencial, precisamente por ser secreto.

- Y haber sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto.

La protección que otorga un secreto empresarial que cumpla con estas condiciones permitirá impedir la revelación de la información constitutiva como secreto empresarial, permitiendo el ejercicio de acciones judiciales ante quienes revelen ilícitamente los secretos empresariales.

Por tanto, las medidas, tanto técnicas como jurídicas, son elementos básicos para que los secretos empresariales puedan tener esta consideración. Las medidas técnicas que serían razonables, generalmente se referirán al almacenamiento físico o digital de los secretos, de manera que estos no sean accesibles por quienes no participen ni en su elaboración desarrollo o comercialización. La empresa que pretenda proteger un secreto empresarial deberá establecer dichas medidas de control, almacenamiento o acceso.

Respecto a las medidas jurídicas, estas deben afectar a cualquier persona física o jurídica, ya sea de la propia empresa titular del secreto empresarial o tercero que participe en el desarrollo o explotación del secreto. Dichas relaciones contractuales deben fijar la confidencialidad mediante la que deben realizar su actividad estos terceros, teniendo claro en todo momento que están trabajando con los secretos empresariales protegidos por la empresa.

En este sentido, los acuerdos de confidencialidad, cuyo uso es muy extendido, podría no considerarse suficiente, dado que el tercero debe ser plenamente consciente de que esta ante secretos empresariales.

La pregunta aquí es clara, ¿cómo se pueden identificar esos secretos empresariales?, ¿cómo podemos además certificar su existencia ante una supuesta revelación de los mismos?

Tradicionalmente para identificar estos secretos empresariales se acudía al Notario y se depositaban ante él.

Sin embargo, estas acciones someten al secreto empresarial a riesgos técnicos, ya que su almacenamiento se produce fuera de las instalaciones del titular del secreto y dificulta mucho la protección de las versiones de los secretos, que en ocasiones son constantes, por ejemplo, cuando estamos ante un algoritmo considerado secreto, un código fuente, una base de datos de clientes, cuyas versiones se van actualizando asiduamente.

Es en esta parte en la que es posible utilizar la tecnología blockchain para identificar y certificar la existencia de los secretos empresariales, sin someterlos a riesgo en su envío o al salir de nuestra empresa.

Y es que blockchain permite certificar el contenido de los secretos empresariales mediante el “hash” del archivo digital que certificará que dicho archivo digital es exactamente ese y mediante el “timestamp” de blockchain se certificará que dicho archivo digital existe en una fecha determinada.

Con la combinación de estas dos tecnologías se puede evidenciar la existencia de estos archivos digitales, que previamente han sido considerados secretos empresariales, de manera segura, dado que a la red de blockchain únicamente se remiten los hashes correspondientes a los archivos digitales, por lo que en ningún momento se publican o hacen accesibles los contenidos de los secretos, que permanecerán en todo momento controlados por la empresa que previamente los identificó y le incorporó las medidas jurídicas y técnicas correspondientes para que estos puedan considerarse secretos empresariales.

SEGURITEC PERU

3RA. FERIA VIRTUAL DE SEGURIDAD

Octubre 25 - 30 2021

MegaFip
Mega Feria Internacional del Perú

Pabellón N° 1

El Registro de Visitante ya está Abierto Sin Costo

www.megafip.pe/seguritec

FÍSICA

INCENDIO

PERSONAL

VIAL

RESCATE

POLICÍA

Informes:

THAIS CORPORATION

gdelatorre@thaiscorp.com

+51 987-421-834

+51 982-508-607

Oficialización:

Prensa Acreditada:

Estas son las señales que indican que tienes **un virus en el móvil**

Troyanos, adwares, malwares, ransomware... Sus nombres ya suenan a peligro y ponen en alerta a cualquiera. Hoy en día existen miles de virus que amenazan a nuestros smartphones o móviles. Las consecuencias de un ciberataque pueden ser irreparables, ya que los dispositivos móviles poseen información muy sensible sobre nosotros, desde teléfonos de contacto hasta cuentas bancarias, contraseñas, imágenes, vídeos privados y una lista interminable de información personal. Por eso, es muy importante conocer nuestro dispositivo para saber si está infectado por un virus, y si lo está, como eliminarlo rápidamente para evitar deños irreparables.

Te contamos qué comportamientos en tu dispositivo móvil pueden indicarte que tienes algún tipo de virus instalado. También te damos algún consejo para eliminar el malware.

Cómo saber si tienes un virus en el móvil

En general, la principal vía por la que entran los virus en nuestros dispositivos móviles es descargando una aplicación fraudulenta. Normalmente nos llegan a través de servicios de mensajería como WhatsApp, Facebook Messenger, Twitter, el chat de Instagram... Si un contacto tuyo te envía un enlace

sospechoso, ten cuidado porque quizás es un virus.

Una de las primeras señales que indican que tienes un virus es un rendimiento anómalo en tu dispositivo. Por ejemplo, que aplicaciones y menús se cierren solos o que cada vez que visitas una página web aparezca más publicidad de lo normal. En este sentido, también es importante detectar si se instalan apps o se cambian ajustes sin tu permiso.

Si detectas que las aplicaciones nativas -aquellas que encontramos en el escritorio de nuestro smartphone y a la que accedemos a través de un icono propio- son sustituidas por otras, es porque tu móvil ha sido infectado por un virus. Este es un tipo de comportamiento bastante característico de algunos malwares extremadamente dañinos como el FluBot, que puede robarte dinero y tomar el control de tu dispositivo.
El gasto desmesurado de batería y datos móviles es otra señal de que quizás tengas un virus instalado en tu dispositivo. Eso debería ponernos en alerta. En este sentido, es conveniente que revises qué proceso está provocando ese elevado consumo.

Una señal inequívoca de que está pasando algo extraño es si mientras navegamos se nos redirige a páginas raras. Igual de sospechoso es que nos aparezca publicidad no deseada y en páginas que no se espera. En este caso, te recomendamos no hacer clic nunca en la publicidad.

Cómo eliminar un virus

Cuando tu dispositivo está infectado por un virus, lo primero que tienes que hacer es reiniciar el dispositivo en modo seguro.

En Android, basta con pulsar el botó de encendido/apagado. Se te abrirá un menú en el que deberás presionar 'apagar'. Tras apagarlo, al encender el móvil, no funcionará ninguna aplicación, el virus tampoco.

Tras reiniciar el móvil en modo seguro, te recomendamos desinstalar aplicaciones que consideres sospechosas. En caso de no poder desinstalarlas, ve a ajustes, a la sección 'seguridad'. Una vez dentro, ve a 'aplicaciones con acceso de uso' y quita estos accesos al virus.

Herramientas para detectar aplicaciones dañinas

Si tienes un dispositivo Android, debes saber que puedes buscar aplicaciones dañinas a través de la herramienta Play Protect. Solo tienes que entrar en Google Play, abrir el menú y buscar en la sección Play Protect. Esta herramienta analizará tu móvil móvil en busca de aplicaciones que puedan ser peligrosas.

iOS no tiene un sistema nativo de detección de amenazas o aplicaciones fraudulentas. En estos casos, Apple aconseja que actualices todas tus apps y el propio móvil.

Teoría de la Asociación Diferencial en el delito de Cuello Blanco.

El 27 de diciembre de 1939 Edwin H. Sutherland pronunció la conferencia inaugural de la reunión anual de la American Sociology Society, de la que era presidente, dedicándola a un tipo de delitos que hasta ese momento no había recibido la suficiente atención por parte de los estudiosos de la criminalidad. Hasta entonces, el comportamiento delictivo se relacionaba principalmente con cuestiones como la pobreza, la desestructuración social o los desórdenes mentales. Sin embargo, Sutherland acuña el término "delito de cuello blanco" para referirse al delito cometido por un individuo profesional o de los negocios con un alto estatus social y económico, el cual aprovecha la confianza que le otorga su estatus y la oportunidad que le brinda el puesto que ocupa. Detrás de este tipo de delitos suele estar también el beneficio económico, aunque aquí, el matiz estriba en que el delincuente ya posee un nivel social y económico que, en principio, no debería presionarlo mucho para buscar dinero, cuanto menos hacerlo por medios fraudulentos.

Son grandes directivos, financieros del alto standing o profesionales muy valorados y reconocidos que generalmente suelen disfrutar de buenas condiciones de vida, con una economía personal muy solvente y con todas las comodidades y lujos que le otorgan, en mayor o menor medida, su condición de profesional de "éxito". Sin embargo parece que, o esto no le es suficiente, o el tener mucho le presiona para querer tener más, siguiendo aquel refrán que dice: "el corazón del avaro se parece al fondo del mar, ya pueden llover riquezas que no se llenará".

Para tratar de explicar esta tipología delictiva, Sutherland crea la Teoría de la Asociación Diferencial, en donde explica que las conductas delictivas no son innatas sino aprendidas. El ser humano, al vivir en sociedad, se relaciona continuamente con otras personas, entre las cuales puede haber personas que no respeten la ley, de las cuales aprende que el delito tiene sus ventajas y sus justificaciones. Esta relación con personas o con un contexto que ofrecer una visión positiva del comportamiento delictivo, haría que el sujeto también acabe asumiendo estos comportamientos como lícitos. La asociación diferencial se produce al vivir inmerso en un mundo, el de los negocios "a toda costa", en donde se produce una organización social diferencial regida por unos

códigos de comportamiento enmarcados en la ilegalidad, que son transmitidos por aprendizaje y reforzados mediante claras técnicas de neutralización de las que hablábamos en un post anterior.
Este autor nos habla de que la organización puede estimular el fraude, erradicarlo o mantener una posición ambivalente. El primer tipo de organización favorece la aparición de delincuentes de cuello blanco a través de la convivencia con un contexto asociativo en el que prevalece una opinión favorable respecto a la violación de la ley. Si la organización se asienta además en un entorno social, político y legal que es permisivo, el fraude se convierte es un elemento estructural y cultural que queda fuertemente arraigado. Esto puede verse en diversos países, donde el fraude y la corrupción infectan todos los estratos sociales, desde el trabajador, al funcionario, desde el empresario al político.
Evidentemente, esta teoría tiene sus limitaciones explicativas y ha recibido enormes críticas respecto a su simplicidad y falta de profundidad. Sin embargo, aporta algunos elementos de interés para los que analizamos el comportamiento del fraude.

Uno de ellos es la visión distorsionada que el defraudador va generando de su comportamiento, pues el delincuente de cuello blanco generalmente no tiene una visión negativa o egodistónica de sí mismo, sino todo lo contrario. Éste se percibe en un estatus de superioridad y en un contexto de actuación donde sus actos no solo no son fraudulentos, sino que son los adecuados y ajustados a sus circunstancias. Esto en parte se ve apoyado por un contexto social y, en muchas ocasiones también legal, que no desaprueba o no lo considera un criminal. Esta visión general positiva, junto con elementos de justificación, le permiten evitar el proceso estigmatizador de sentirse y ser visto como “un delincuente”.
Otro elemento clave que participa en la comisión de este tipo de delitos es el abuso de la confianza. El delincuente de cuello blanco goza generalmente de un estatus de prestigio, a veces conseguido de forma lícita y profesional, lo que le genera una imagen de confianza entre subordinados y superiores. El éxito profesional le lleva a una posición de responsabilidad, pero también de privilegio, maneja grandes presupuestos o/y equipos. Delante de él se toman las grandes decisiones y fluye el dinero, los beneficios y las comisiones. Es una zona donde incluso lo objetivo, lo cuantificable y los balances debe-haber se tornan abstractos mediante el maquillaje financiero, la ingeniería contable o la optimización fiscal. En este contexto, el delincuente de cuello blanco utiliza su posición, sin la cual no podría estar en el lugar adecuado, y la confianza que otros han depositado en él para llevar a cabo el fraude. Desde esta posición, el engaño es más fácil y cómodo porque las víctimas se dejan llevar, creen u obedecen las indicaciones del defraudador. Víctimas que pueden ser en estos casos clientes o subordinados, pero también sus propios jefes o los accionistas para los que trabaja. Esta situación le permite conseguir sus fines sin apenas resistencia y sin mucho esfuerzo por su parte, lo que facilita el condicionamiento y repetición de la conducta fraudulenta.

Amazon entra en el negocio de la seguridad y lanzando un dron de vigilancia

Ring, la compañía de Amazon especializada en productos inteligentes de seguridad, ha lanzado su dron de seguridad Always Home Cam, un producto de vigilancia para el hogar que ya ha llegado a EEUU

Always Home Cam de Ring, que se había dado a conocer desde hace un año y apareció de nuevo en la presentación de hardware de Amazon de este martes, supone un nuevo formato de cámara de seguridad doméstica que se desplaza volando.

Este dron emplea una combinación de sensores activos y de algoritmos avanzados de navegación para volar en rutas personalizadas configuradas por el usuario dentro del hogar. Su función principal, según ha descrito su fabricante, es investigar cuando otro de las alarmas de Ring detecta movimiento inusual y emite una alerta, revisando la zona y la vivienda.

Ahora, como ha anunciado la marca de Amazon en un comunicado, este dispositivo ya puede reservarse desde este martes, aunque solo por invitación y únicamente para los usuarios de Estados Unidos.

AJSE
Asociación de Jefes de Seguridad de España

Nuevo Presidente Autonómico de AJDSE Valencia. D. Vicente Peris Cursa

Nuevo presidente autonómico de Madrid, de AJDSE. D. Jorge Salgueiro Rodríguez

Las redes sociales no son un juego – Canal prioritario

El Canal Prioritario de la Agencia Española de Protección de Datos ofrece una vía rápida y gratuita para denunciar la publicación ilegítima en Internet de contenidos sensibles, sexuales o violentos, incluso sin ser la persona afectada.

'Las redes sociales no son un juego – Si compartes contenido sexual o violento perdemos todos' es una iniciativa con la que la Agencia quiere poner el foco en la publicación en redes sociales de este tipo de contenidos y transmitir que todos podemos denunciar en el Canal prioritario su publicación.

Los casos más frecuentes planteados ante la Agencia están relacionados con la publicación en redes sociales y otros sitios web de contenidos de carácter sexual grabados con o sin el consentimiento de la mujer que aparece en ellos pero publicados sin su permiso, la publicación de grabaciones con agresiones a menores de edad y personas LGTBIQ+ y la publicación de perfiles falsos en páginas pornográficas.

La denuncia realizada en el Canal prioritario es independiente de la que pueda plantearse ante las Fuerzas y Cuerpos de Seguridad del Estado o la Fiscalía.

Cómo funciona el Canal prioritario

La Agencia, como autoridad independiente, puede adoptar medidas urgentes para limitar la difusión y el acceso a los datos personales. Tras el análisis de la denuncia (que puede ser realizada tanto por la víctima como por un tercero), la Agencia puede determinar la adopción de medidas cautelares para evitar la continuidad del tratamiento ilegítimo en casos particularmente graves. Al tiempo, la Agencia también valora la apertura de un procedimiento sancionador contra las personas responsables de haber realizado el tratamiento ilegítimo.

La denuncia de fotografías, vídeos o audios de contenido sexual o violento difundidos en Internet sin el consentimiento de las personas afectadas puede realizarse a través de este enlace

aepd agencia española protección datos

Denuncia la difusión de estos contenidos en el Canal prioritario

aepd.es/canalprioritario

NEGRA EN MI COCHE INTELIGENTE? EN QUE ME PUEDE AFECTAR LA CAJA NEGRA AUTOMOTRIZ EN MI VEHÍCULO PARTICULAR.

Paco con su coche nuevo de alta gama, circulaba por la N II, de madrugada, prácticamente sólo en la carretera, a una velocidad algo elevada, cruzando poblaciones, pero sin reducir velocidad a sabiendas que en esa zona no hay radares fijos ni móviles, por eso estaba muy tranquilo, ya que era prácticamente imposible que fuera detectado su exceso de velocidad.

Al girar una rotonda, ve un destello azul y le da el alto una patrulla de la Guardia Civil de Tráfico, en el alto policial, le solicitan la realización de test de detección de alcohol y sustancias psicotrópicas y drogas, después de unos segundos tensos, el resultado de las pruebas de detección da negativo en consumos prohibidos. Paco se siente a salvo, pero el agente se conecta mediante IoT con la caja negra del vehículo nuevo de Paco, y una vez realizada la lectura…nuestro amigo Paco acaba detenido por un presunto delito contra la seguridad del Tráfico, de los tipificados en el Código Penal… ¿Qué ha pasado?

Pues muy sencillo, la tecnología de grabación de datos de actividad de los automóviles ha ido evolucionando del muy básico EDR (Event Data Recorder) donde sólo se captan elementos básico de consumos y datos técnicos de motor, tales como presiones, temperaturas, pero las nuevas capacidades y necesidades del coche autónomo no ha llevado al DSSAD (Sistema de almacenamiento de datos para conducción automatizada) donde se recogen trayectorias, motores, etc o en futuras versiones avanzadas donde ya se permite incorporar cajas negras

automotrices en todos los vehículos privados e interconectarse mediante tecnología IoT, mediante IP e incluso mediante RFID, pudiéndose realizar en tiempo real lecturas de velocidades, trayectorias GPS, datos de actividad de motor, etc.

En la actualidad sólo los talleres tienen acceso a la CPU o unidad de procesamiento o al EDR, mediante el conector de enlace de diagnóstico (DLC), estas conexiones limitadas y verticales exclusivas del taller, es previsible que en muy breve puedan ser on line mediante tecnología IoT vía IP y conexión 5G, sin necesitar contacto físico con el vehículo.
En este sentido y dado el cariz que tienen las diferentes autoridades de control en materia de Seguridad Vial y las líneas maestras marcada por la UE, esta claro que se quiere accidentes cero, y una de las herramientas que van a dotar a los agentes encargados de regulación y control del tráfico será sin duda alguna es el acceso directo a la DSSAD, tanto para investigación de accidentes como para supervisión y vigilancia del tráfico.

El paso del acceso del taller a la unidad policial en carretera es sumamente sencillo dado el estado de la técnica de IoT vinculada al 4G y 5G.

En materia de protección de datos, este dispositivo DSSAD o las versiones futuras más avanzadas, pueden tener repercusiones muy severas en materia de protección de datos de carácter personal, ya que los datos de actividad del vehículo pueden ser vinculados a una persona física identificada e identificable, y esos datos pueden incluir excesos de velocidad, salidas de vía, etc, y en algunos casos más extremos pudieran tener severas repercusiones penales, e incluso nos puede indicar la existencia de un accidente grave (p.e. reducción instantánea de la velocidad del vehículo, por ejemplo por un impacto contra un árbol por una salida de vía en una autopista…)

La Dirección General de Tráfico, esta buscando hace tiempo la reducción de la velocidad de los vehículos en la vía como la mejor herramienta para bajar los accidentes graves. La existencia de una “caja negra” en nuestros vehículos puede comportar que las autoridades puedan acceder a nuestra actividad como conductores, siendo nuestro propio vehículo el principal testigo de cargo en el caso de infracción administrativa o penal por exceso de velocidad.

También hay que tener en cuenta, que Internet of Things, o Internet de las cosas (IoT) , puede hacer que el vehículo, la vía , los fabricantes, las autoridades y otros operadores estén interconectados en tiempo real. Es evidente que estas interconexiones comportan un gran volumen de datos, de sumo interés para los diferentes operadores de la movilidad, ya que la aplicación de la Inteligencia Artificial (IA) puede aportar predicciones y prospectivas de sumo interés, tanto para fabricantes, autoridades de control de movilidad, compañías de seguros, etc. como para las autoridades de control del tráfico, tanto locales, autonómicas y estatales.

Sin duda la “caja negra” interconectada mediante IoT, puede ser un elemento de ayuda y soporte tanto en la investigación de accidentes como para el análisis y regulación de la movilidad, pero es evidente que estas acciones de supervisión y control tendrán que ser tamizadas y ajustadas a la normativa de privacidad aplicable en cada momento, especialmente el RGPD y la LOPDGDD.
.Lo veremos en un tiempo, estaremos a la espera y os tendremos informados.
Un saludo.

Daniel Oliva, Director de Seguridad de Ferrocarrils de la Generalitat de Catalunya

Daniel Oliva de actualmente 44 años ejerce como Responsable del Departamento de Producción-Seguridad en Ferrocarrils de la Generalitat de Catalunya desde el año 2013.

Graduado en Criminología y con la titulación de Detective Privado, lleva más de 22 años ejerciendo profesionalmente en el mundo de la Seguridad (entre pública y privada).

Dispone de diferente formación en materia de Seguridad, como el Máster en Operaciones de Inteligencia y Contrainteligencia o el Máster Contraterrorismo y Fenomenología Terrorista, entre otros.

Reside en Sabadell, es un apasionado de la música y el deporte, y le encanta pasar su tiempo libre en familia con su mujer, su hija y su hijo.

1º ¿Que ha supuesto para su carrera profesional su incorporación a FGC?

Después del privilegio de haber podido estar más de 14 años en el Cuerpo de Mossos d'Esquadra, habiendo tenido la posibilidad de trabajar en múltiples destinos, realizar diferentes especialidades y de haber aprendido de tantas y tantas personas; me surgió la posibilidad de liderar un Departamento de Seguridad en fase de construcción y con un gran potencial de crecimiento en FGC.

En ese momento, y con 37 años, me apetecía iniciar un nuevo reto profesional, el poder

realizar una tarea diferente a todo lo vivido hasta ese momento; salir de mi zona de confort, explorar otra visión de la seguridad y adaptarme a una nueva cultura corporativa. Además, el hecho de tener la oportunidad de formar parte también de una organización tan importante, bien valorada por la sociedad catalana y que siempre busca la excelencia, le añadía un plus de motivación a ese reto.

2º ¿Con que problemas se encuentra a diario en su trabajo con la inseguridad y la delincuencia?

Podríamos decir que las tipologías más habituales que padecemos en FGC van muy en la línea del resto de operadores del transporte y están sobre todo relacionadas a ataques de grupos estructurados u organizaciones vinculadas al fenómeno grafitero, pequeños hurtos, apedreamientos de trenes y daños patrimoniales en instalaciones o trenes.

En nuestro Departamento, diariamente y mediante un mapa de conflictividad, recogemos y analizamos todos los hechos vinculados a conductas antisociales. Clasificamos esa información en base a unos datos teniendo en cuenta la naturaleza del incidente, el lugar del hecho, la temporalidad, franja horaria, día determinado o época del año, u otra información relevante. A partir de ese momento y de manera global, obtenemos unos indicadores que nos ayudan a determinar conclusiones. Además, estos resultados facilitan el análisis para, por un

lado, poder identificar tendencias (cuándo, cómo y dónde se están produciendo); y, por otro, nos permiten analizar de manera pormenorizada y objetivada cada una de estas problemáticas y adaptar nuestras operativas de seguridad en función de cada necesidad.

No es menos cierto que paralelamente siempre van apareciendo nuevas conductas antisociales que requieren un plan de choque específico y una readaptación de nuestras medidas de seguridad y recursos con su correspondiente seguimiento hasta paliar esas posibles amenazas.

En un mundo totalmente globalizado resulta inevitable la aparición de nuevas conductas delictivas e incluso de mutaciones/ transformaciones en los modus operandi de posibles infractores y, por tanto, una vez analizada la situación, resulta vital asegurar una adecuada respuesta.

3º Debido a la pandemia del COVID 19, ¿qué medidas han impuesto para la seguridad de los viajeros en su empresa?

Como se pueden imaginar, en el marco de la pandemia nos hemos encontrado con distintos escenarios según cada momento. Los cambios vividos en la sociedad también han tenido una afectación en las conductas antisociales.
A modo genérico podríamos hablar de dos realidades evidentes: por un lado, una realidad delictiva antes de la situación más restrictiva y mientras estábamos en régimen de confinamiento domiciliario, municipal, etc., donde absolutamente todas las incidencias antisociales habían disminuido y algunas casi desaparecido; y una segunda realidad a partir de la desaparición de estas medidas más restrictivas, donde se ha notado una reactivación delictiva acorde con la normalización progresiva de la actividad social.

Por otro lado, y si nos centramos en el momento actual, vemos como han aparecido nuevas problemáticas inexistentes antes de la pandemia y que, hoy en día, conviven en nuestro ecosistema de protección y pueden influir en la percepción de inseguridad que algunas personas puedan tener en momentos puntuales. Como ejemplo, si analizamos los actuales indicadores, es evidente que la aparición en escena de “la mascarilla” ha aflorado 2 nuevas problemáticas que nos han repercutido significativamente en nuestros indicadores:

1- La obligación de llevar puesta o de llevarla correctamente puesta dentro de los trenes o estaciones ha incrementado el nivel de conflictividad en algunos ámbitos, generando en ocasiones disputas entre los mismos clientes o encontronazos con nuestros trabajadores cuando estos han actuado para corregir hechos. En este sentido, cabe recordar que nuestra plantilla de agentes, así como nuestros vigilantes de seguridad han tenido y tienen la misión de velar para que los usuarios respeten esta medida y fruto de estas intervenciones se han generado en ocasiones determinadas problemáticas
2- Por otro lado, el solo hecho de llevar mascarilla, ha podido generar sensación de

cierta impunidad desde el punto de vista de los infractores ya que, sabiendo que todos los trenes y estaciones están controlados por cámaras de CCTV, el hecho de estar con parte del rostro cubierto les ha hecho pensar que no es posible su identificación. Esta circunstancia ha sido aprovechada por algunas personas para cometer hechos punibles e incluso contribuir a que haya personas que se planteen delinquir o realizar infracciones en estas condiciones.

4º Que le motivó a dar el paso de la seguridad pública a la seguridad privada?

Ya estando en la seguridad pública, y aun sin tener demasiado conocimiento en la materia desde fuera, la seguridad privada siempre me llamó la atención. Lo veía como un mundo muy interesante y totalmente complementario a la seguridad pública (al final Seguridad es Seguridad).

Recuerdo que, en el año 2007, me matriculé en la UAB y me saqué la TIP de Director de Seguridad, porque realmente me apetecía ampliar mi formación y profundizar en este ámbito, aunque en ese momento no me planteaba ningún cambio profesional.

Una vez realizado el curso y el proyecto final, recuerdo sentir una grata sensación y positiva percepción del mundo de la seguridad privada.
Al final, tal y como he comentado anteriormente, 6 años después apareció la posibilidad de cambiar y aquí estoy.

5º ¿Qué medidas han dispuesto en FGC, al respecto de los grafitis y sabotajes?

Como vemos diariamente, el mundo está cambiando, están apareciendo nuevas amenazas, determinadas conductas antisociales están aflorando y no debemos olvidar que continuamos en un nivel de alerta terrorista 4 sobre 5 permanente en el contexto actual y, por tanto, la manera de protegernos también debe adaptarse a estas circunstancias.

En FGC no queremos ser vulnerables. No queremos ir “detrás de la pelota” y por este motivo de manera constante trabajamos para garantizar que todos nuestros trenes e instalaciones estén protegidos.

El Departamento de Seguridad de FGC orienta, entre otros, a garantizar 3 objetivos nucleares:

- Garantizar los servicios esenciales de movilidad y su normal actividad.

- Proteger la integridad física de sus trabajadores y clientes.

- Proteger sus infraestructuras y trenes (bienes y activos).

En este contexto, FGC continúa avanzando por el camino de la seguridad física inteligente, para asegurar una mayor eficiencia de sus actuaciones, mejorar su capacidad de respuesta y garantizar la protección de las personas y activos bajo su responsabilidad.
Las medidas diferenciales aplicadas no tan solo hacia el fenómeno grafitero sino en relación con cualquier intrusión no autorizada (independientemente de su finalidad) van encaminadas a:

- Garantizar un modelo de seguridad física 360º. Es decir, asegurar un modelo de seguridad global que contemple todo el ciclo vital ante cualquier incidente de seguridad: Proteger, detectar, identificar y responder ante cualquier amenaza.

- Disponer de una protección activa. Mediante unos procedimientos orientados a la prevención, anticipación de los hechos y actuación inmediata que permitan obtener una mejor respuesta ante situaciones de riesgo que se puedan producir.

- Apostar por una tecnología innovadora e inteligente. Con capacidad para reaccionar y ayudar al modelo de seguridad implantado con procesos y personas implicadas y centrando gran parte de sus recursos en la pre-detección de posibles ataques o acciones en sus instalaciones o trenes.

6º En licitaciones concursales sobre sistemas y personal de seguridad, ¿qué es lo que mayormente valoran a la hora de elegir una empresa?

En cuestión de licitaciones concursales nos regimos a la normativa de subcontratación que nos marca la administración pública.

Evidentemente en toda licitación pública, marcamos unos requerimientos técnicos específicos y de calidad como operador ferroviario, y que para nosotros son imprescindibles para asegurar un adecuado servicio.

Resulta esencial al final del proceso asegurar que la empresa adjudicada está en disposición de garantizar el normal funcionamiento de FGC y cumplir con los índices cualitativos acorde a nuestro modelo de producción.

7º ¿Actualmente su departamento de Seguridad en FGC, trabaja con sistemas y métodos de Ciberseguridad?

Efectivamente, y teniendo en cuenta que en todo el mundo actualmente se está produciendo también un incremento exponencial de la ciberdelincuencia, FGC intenta estar preparado para todo tipo de nuevas amenazas globales y ciberseguridad, la evolución y transformación tecnológica ha creado nuevos riesgos intrínsecos y extrínsecos que requieren una serie de medidas de seguridad en este sentido.

Resulta clave disponer de personas con formación específica en la materia pluridisciplinar y con una suficiente experiencia y conocimientos capaces de hacer frente a estas nuevas amenazas y que soporten a unos medios tecnológicos capaces de contrarrestar y detectar posibles ataques cibernéticos.
Cabe recordar que hoy en día algunos de los diferentes modus operandi de muchas organizaciones delincuenciales, criminales y/o de terrorismo internacional operan, trabajan y generan sus procesos mediante computadoras, aplicaciones, servidores, redes, sistemas electrónicos, dispositivos móviles o similares.
Por tanto, el Departamento de Seguridad de FGC trabaja transversalmente en base a una política de seguridad conectada a la tecnología de la información para garantizar la protección de datos, evitando el robo de estos, los ataques cibernéticos o usurpaciones de identidad, entre otras cosas.

8º Por último, ¿cuál cree Vd. que será el futuro del tren y en su caso también cuál será el de FGC?

Mi opinión al respecto es que los operadores ferroviarios que garantizan una movilidad sostenible y eléctrica representarán un elemento vital en la movilidad del futuro.
El crecimiento urbano previsto en los próximos años obliga a una reconversión de la movilidad entre las diferentes ciudades de una manera cada vez más respetuosa con el medio ambiente, que permita el fácil acceso a las diferentes poblaciones y grandes ciudades del futuro y mejorando la experiencia de los usuarios y usuarias.

En el caso de FGC la tendencia es la de continuar creciendo y se está trabajando en múltiples proyectos de presente y de futuro. Como reto más inminente, por ejemplo, hay que decir que estamos en proceso de prolongación y conexión de la estación de Plaza Espanya con la estación de Gràcia, lo que permitirá conectar el metro Llobregat-Anoia con el metro del Vallès y construir tres nuevas estaciones: Hospital Clínic, Francesc Macià y Gràcia.

Esta mejora prevista en 6 años permitirá ampliar la zona de influencia directa en casco urbano, mejorar la conectividad e incrementar en más de 60 millones de usuarios por año la capacidad de plazas.

Además, en FGC también trabajamos en otros proyectos como la nueva línea R-Aeroport que enlazará la ciudad de Barcelona con el Aeropuerto del Prat, con 10 millones más de oferta de transporte público; el nuevo servicio de Cercanías de Lleida, con 1 millón de viajes al año ofertados, y el Tren-tranvía del Camp de Tarragona, que tendrá una capacidad de entre 2 y 5 millones de viajeros al año.

Por lo tanto, nos esperan años de muchísimo trabajo y retos apasionantes también en materia de seguridad y protección.

RADIO STAR 100.5 FM
www.radiostarterrassa.com

MOMENTOS DE SEGURIDAD

Nuevo programa de radio dónde se tratarán los temas más relevantes en seguridad

El primer y tercer miércoles de cada mes

Organizado por :

AJDSE
Asociación de Jefes y Directores de Seguridad de España

Presentado por:

- ✔ Mónica Roman
- ✔ Sergi Tarrida

Visita Nuestra Página web www.ajse.es

AJSE-ISCA centro de formación de DPD

AJDSE
Asociación de Jefes y Directores de Seguridad de España

Centro de formación (AJSE)
Delegados de Protección de Datos