ciber.gal

iVIGO BUSINESS SPACE

DEPUTACIÓN PONTEVEDRA

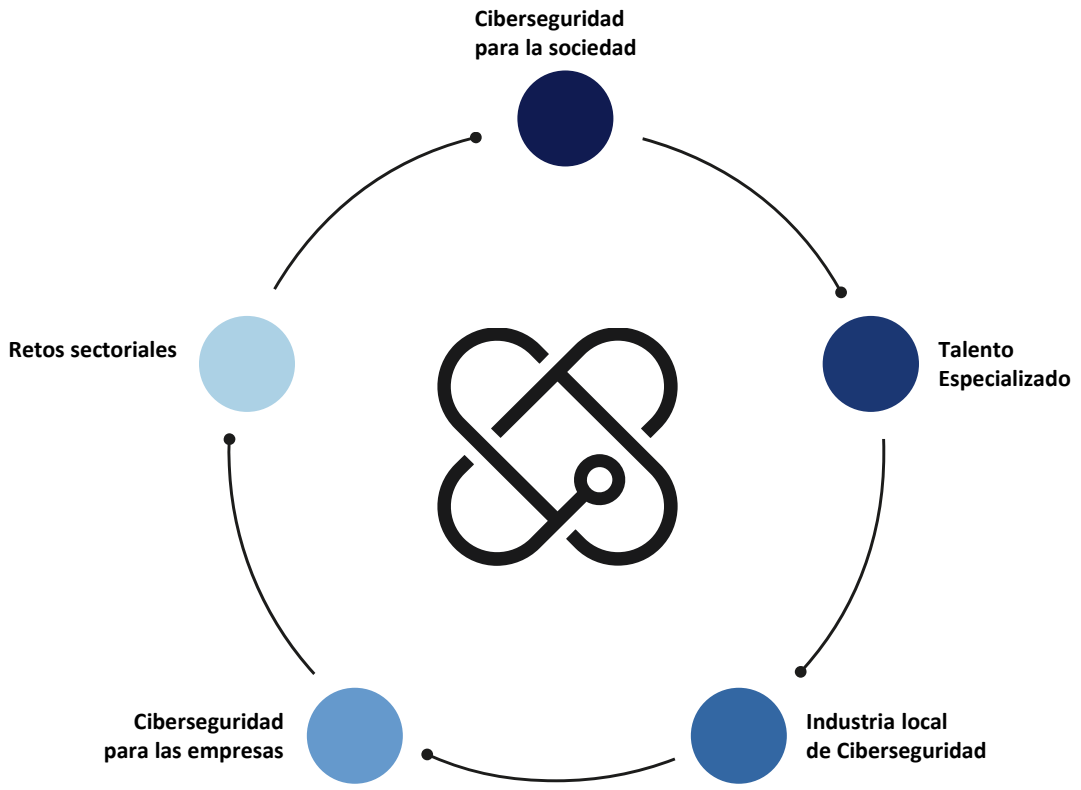
Ciberseguridad en el sector TURISMO y OCIO

Pontevedra 09/06/2022

https://ivigo.es/ciberseguridad-en-el-sector-turismo-y-ocio-nodo-cibergal/

Qué veremos hoy:

- *Qué hacer y qué no hacer para estar ciberseguros.*
- *Cómo detectar las ciberamenazas.*
- *Casos reales de ciber problemas reales.*
- *Medidas de ciber protección.*




0011010
0011010
0011010
1011000110
****
****

La Voz de Galicia

RED

Ramón Suárez: «En seguridad digital muchos siguen 'a velas vir'»

Es un «influencer» experto en la industria 4.0., un tipo de tecnología que conectará entre sí 50.000 millones de dispositivos de robotización, impresión 3D e Internet de las Cosas. Teme que en un mundo hiperconectado, los «hackers» hagan peligrar vidas.

M. MORALEJO

E. V. PITA
REDACCIÓN 02/07/2018 20:03 H

Ramón Suárez es un influencer y mentor digital a nivel europeo y especializado en la industria 4.0, y coordinador de la red gallega

FIREWALL HUMANO

FIREWALL HUMANO

El 95% de los ciberataques que logra su objetivo viene precedido de un error humano

Expertos de KPMG advierten de que para mejorar la seguridad informática de una compañía no basta con invertir en tecnología; es fundamental formar sobre los riesgos a los trabajadores

IRATXE BERNAL

Martes, 21 abril 2020, 02:01

ciber.gal

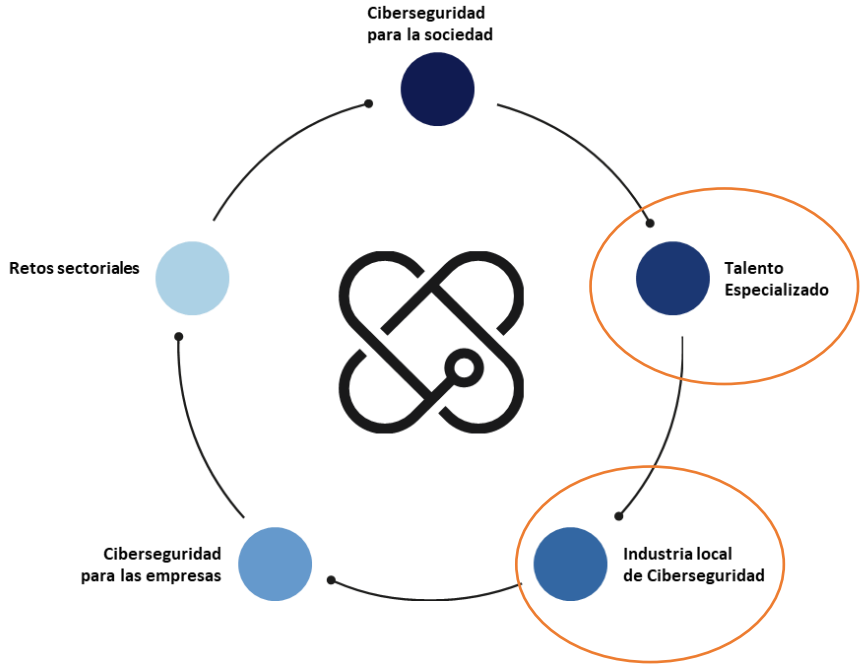
Nodos > CIBER.gal >

Colaboradores

CIBER.gal como estructura para la cooperación y promoción en el ámbito de la ciberseguridad, colabora con entidades tanto públicas como privadas para convertirse en el espacio gallego de referencia para el intercambio de conocimiento e ideas que permita dar respuesta tanto a la ciudadanía, pymes y administración como a las propias necesidades del sector para apoyar su desarrollo.

Actualmente CIBER.gal cuenta con la colaboración de entidades de diversos ámbitos y sectores, entre los que destacan el tecnológico, el jurídico y el de la investigación y conocimiento.

ciber.gal iVIGO BUSINESS SPACE DEPUTACIÓN PONTEVEDRA



17 de abril del 2022 • La Voz de Galicia

Vigo, pionero en negocios con NFT

Una asociación no admite el pago en euros y un artista negocia ventas de criptoarte

E. V. PITA
VIGO / LA VOZ

Antonino Comesaña, de Agalbit. X.C.GIL

Ramón Suárez, de iVigo, reconvertido en galerista de NFT. M. MORALEJO

Vigo es una de las ciudades pioneras que han adoptado el formato digital NFT. Estas obras de arte digital coleccionables, el llamado criptoarte, están de moda y los postores pujan miles de euros en las subastas pero los emprendedores vigueses ya están aplicando nuevos usos a esta tecnología de certificación de autenticidad. Por ejemplo, una asociación de Vigo ha renunciado al euro y va a cobrar las cuotas de sus socios obligando a comprar su propio logo coleccionable convertido en NFT. Una vez que uno es dueño de esa pegatina virtual, la web de la asociación lo reconocerá como miembro y le dará derecho a votar en las juntas.

Por otro lado, un emprendedor, Ramón Suárez, ha montado la primera galería de cuadros en NFT en la ciudad y está negociado ventas del autor Elohim con coleccionistas de arte digital y un fabricante internacional de metaversos que quiere añadirlos a su galería virtual.

La Asociación Galega de Blockchain e IoT (Agalbit) ha puesto en marcha su propio *Brexit* porque ya no aceptará los pagos de sus cuotas en dinero en metálico. Solo cobrará las mensualidades en NFT o, alternativamente, en *tokens* (fichas virtuales). Los socios tendrán que acceder a una billetera electrónica, pagar en un Market Place (portal de compraventas en criptomonedas) y comprar el logo en NFT de la asociación por una cuantía fija cada mes. Cuando Agalbit organice un evento *on line* en abierto, la máquina reconocerá automáticamente a los propietarios del NFT, los acreditará como miembros, y los autorizará a votar.

El presidente de Agalbit, Antonino Comesaña, explica este cambio: «Queremos demostrar que el *blockchain* no es una tecnología muerta, no puede ser que haya socios que nunca hayan comprado un *token*, les obligamos a surfear la ola y a monetizarse digitalmente. Servirá para introducir a la gente en esta tecnología; algunos no saben interactuar con los protocolos, es como aprenderlo todo sobre el ordenador y no haber encendido ninguno. Queremos dar a los socios perezosos un empujón, esta tecnología está viva».

El plan de cobrar las cuotas en NFT está listo pero la asociación se plantea otro pago alternativo: emitir su propia criptomoneda o *token* de utilidad para abonar las cuotas de los asociados.

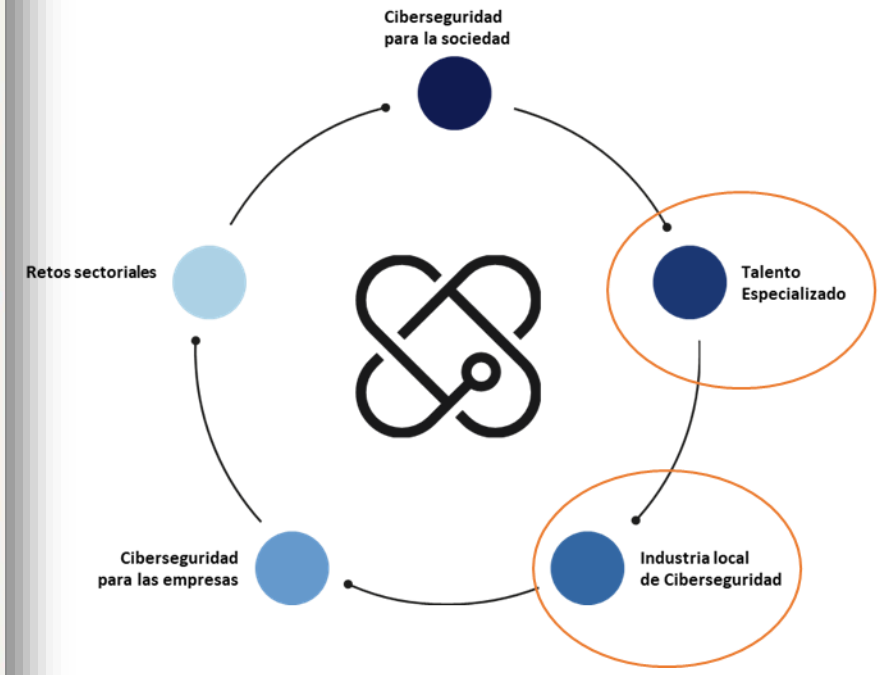
El presidente de Agalbit, Antonino Comesaña, prefiere las NFT porque la emisión de su propio *token* (el equivalente digital a un maravedí de la feria medieval de Ribadavia) atraería a los especuladores como si echasen carnaza a los tiburones. Al ser un *token* para socios, todos compran y nadie vende y, a ojos de un especulador, esa criptomoneda tiene liquidez, tomaría posiciones e inflaría su cotización. Si un socio pagase inicialmente dos *tokens* en un Market Place (mercado virtual) por una cuota mensual de 20 euros, podría toparse al poco tiempo con que el valor de cada *token* subió a cien euros por las presiones alcistas. Comesaña admite que todos temen a los especuladores aunque la idea sería viable si estabilizasen y ajustasen cada mes el número de *tokens* por pagar en función de su valor en el mercado. Admite que el procedimiento iba a ser engorroso.

Esta experiencia pionera de pagos exclusivos de cuotas en moneda digital en Galicia abrirá una brecha entre quienes se manejen con las nuevas tecnologías y los que aún piensan en billetes de euro. «Habrá una doble capa de socios. Por un lado, los profesionales del *blockchain* y, por otra, los colaboradores, por podrán acceder a servicios gratuitos o descuentos».

La diferencia se notará al hacer una votación en la plataforma, que no dejará votar a los que carezcan del token o el NFT. «La billetera queda registrada y te permite votar e interactuar, es como un contrato inteligente», añade Comesaña. Técnicamente, Agalbit no prohíbe el pago en euros pero ese socio se vería relegado a opinar sin derecho a tener voto electrónico.

Ramón Suárez: «La galería va genial. ¡Es un experiencia futurista!»

El autor Elohim ha replicado las 23 obras originales en pintura a más de 60 versiones digitales en formato multimedia con animaciones y sonidos totalmente digitales. Su colección de criptoarte *La iluminación del Ser* está expuesta en el espacio de *coworking* iVigo, en la calle Condesa Casa Bárcena. «La galería va genial. Ha venido mucha gente a visitar la exposición y se han sorprendido gratamente de las inmensas posibilidades que proporciona el formato NFT», dice el emprendedor Ramón Suárez, gerente de iVigo. «En cuanto a ventas, se están empezando a vender en estos últimos días, estamos negociando con varios compradores y con plataformas digitales interesadas en la colección en NFT. Incluso estamos negociando con un fabricante internacional de metaversos para incluir los NFTs en la galería virtual del metaverso, ¡Es toda una experiencia futurista !», recalca. Para pagar, el cliente «puede escoger pero prefiere en criptos».



La Voz de Galicia

R RED

Ramón Suárez: «En seguridad digital muchos siguen 'a velas vir'»

E. V. PITA
REDACCIÓN

M. MORALEJO

Es un «influencer» experto en la industria 4.0., un tipo de tecnología que conectará entre sí 50.000 millones de dispositivos de robotización, impresión 3D e Internet de las Cosas. Teme que en un mundo hiperconectado, los «hackers» hagan peligrar vidas.

02 jul 2018 . Actualizado a las 20:53 h.

Comentar · 0

Ramón Suárez es un influencer y mentor digital a nivel europeo y especializado en la industria 4.0, y coordinador de la red gallega de FabLabs. Ha participado hace poco en eventos como Hack & Beers de Vigo, las presentaciones de la Cátedra Telefónica y la Cátedra de Industria Conectada del ICAI-ICADE de Comillas, impartió charlas sobre industria 4.0 en Extremadura y estuvo en la mesa redonda sobre tendencias en el Encuentro Internacional de Ciberseguridad del Incibe en León. «Los expertos coinciden en que las claves para la ciberseguridad son la anticipación y predicción de ataques mediante analítica de datos e inteligencia artificial», señala.

La Generalitat recluta a un hácker vigués para «piratear» su red

Proyecto pionero para destapar fallos en las webs públicas

E. V. PITA
VIGO / LA VOZ

La Generalitat de Cataluña pidió ayuda a un hácker vigués para que reclutase a un grupo de informáticos cazarrecompensas y proponerles un reto: piratear la red de la Administración pública catalana para descubrir *bugs* (agujeros o errores de seguridad) y prevenir ataques de ciberdelincuentes y trolls. Estos ataques de fuego amigo son un clásico de la ciberseguridad denominado bugs bounty («fallos y recompensa»), pero esta esa la primera vez que se pone en marcha en España en una administración.

El hácker vigués es Antonio Fernandes, conocido experto en ciberseguridad y veterano cazarrecompensas, al que varios gobiernos extranjeros, como Estados Unidos y Holanda, le han agradecido sus servicios. Ahora suma el de Cataluña, que lo menciona en un comunicado oficial donde le da las gracias.

El encargo le llegó a Fernandes en diciembre a través de la Agencia de Ciberseguritat Catalana, perteneciente al departamento de Políticas Digitales y Administración Pública de Cataluña. Se trata del primer *bug bounty* (término en inglés por el que se conoce las recompensas por encontrar fallos de seguridad) organizado en la Administración Pública española.

Antonio Fernandes, hácker. X.C.GIL

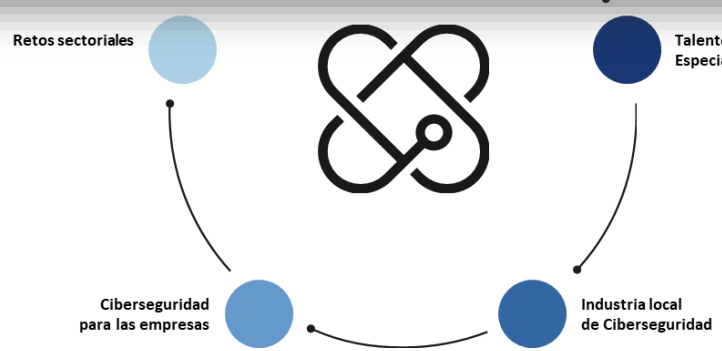
«Les ayudé a encontrar gente hácker y a definir cómo hacer para que encuentren fallos de seguridad y reportárselos a la agencia. Se trata de un proyecto pionero en España», explica Fernandes. Él mismo rastreó fallos.

Las conclusiones de la prueba piloto fueron publicadas ayer por la Agencia de Ciberseguritat. El test se hizo en coordinación con el departamento de Vicepresidencia de Economía y Hacienda de Cataluña. En su comunicado, la Agencia agradece la participación en el programa *bug bounty* a 15 cazarrecompensas, entre ellos al hácker vigués.

Según explica la agencia, el objetivo del programa fue reforzar los sistemas de información pública de Cataluña a la vez que promueven el talento en ciberseguridad. El equipo formado por Fernandes se centró en localizar cinco vulnerabilidades: dos en las webs de la Generalitat y tres en aplicaciones corporativas. Cuando los hackers avisaron de los fallos, los informáticos catalanes los repararon. El programa fue supervisado por el equipo de incidentes Catalonia-CERT.

La Agencia calificó el programa de pionero para blindar sus sistemas electrónicos y fomentar la participación del talento civil. Por ejemplo, en el 2016, el Pentágono (organismo de defensa de Estados Unidos) creó el programa *Hack the Pentagon*. Antonio Fernandes se ha especializado en este tipo de chequeos y en el 2019 el Gobierno de Holanda le envió una camiseta de regalo por los servicios prestados.

La ciberseguridad es estratégica para un mundo que se basará en las tecnologías del 5G y la Inteligencia Artificial, en los que un fallo en la red puede causar daños sistémicos.



ves, 26 de mayo del 2022 • La Voz de Galicia

«Los estafadores tenían mucha información sobre nosotros»

La comerciante señala que fueron a por «el empleado más joven»

NURIA GUILLERMO
A CORUÑA / LA VOZ

María Vázquez, encargada de la tienda que sufrió recientemente una estafa en A Coruña. EDUARDO PÉREZ

«Los estafadores tenían muchos datos nuestros. Sabían mi nombre, que ese día no había ido a trabajar, que había quedado dinero en la tienda... Es la primera vez en diez años que queda dinero en la tienda, y ellos lo sabían. Precisamente, el problema fue que a la persona que les estaba atendiendo en ese momento le cuadraba todo lo que decían porque tenían mucha información». Así explica lo sucedido María Vázquez, encargada de Arco Iris, la tienda de chucherías y papelería de A Coruña que sufrió una estafa el pasado día 12. Los delincuentes llamaron al establecimiento haciéndose pasar por una empresa de transporte con la que trabajan frecuentemente aprovechando que ese día ella no se encontraba allí.

«Desde la policía nos han dicho que no nos fiemos, que no demos números de cuenta y que comprobemos si lo que nos dicen es cierto, pero tal y como te lo exponen es muy difícil», añade. María es la más veterana entre los trabajadores de la tienda, pero, en sus propias palabras, el resto de sus compañeros son «chavales». «Fueron conscientemente a por uno de los compañeros, porque es el más joven, el que menos tiempo lleva en el comercio y el que menos sabe cómo funcionan ciertas cosas», afirma.

Este tipo de delitos se relacionan estrechamente con la gran cantidad de información personal que hay disponible en internet. «Estamos muy expuestos a innumerables filtraciones. Las bases de datos digitales se subastan inicialmente a través de la *dark web* [internet oscura, a la que solo se puede acceder desde navegadores especializados], pero luego se puede acceder a ellas de manera sencilla. En muchos casos, los ciberdelincuentes las compran y las cruzan con bases de otras filtraciones. Si coincide un único dato de una persona, como el correo electrónico, se pueden obtener muchos más», explica Víctor Salgado, abogado especialista en delitos cibernéticos.

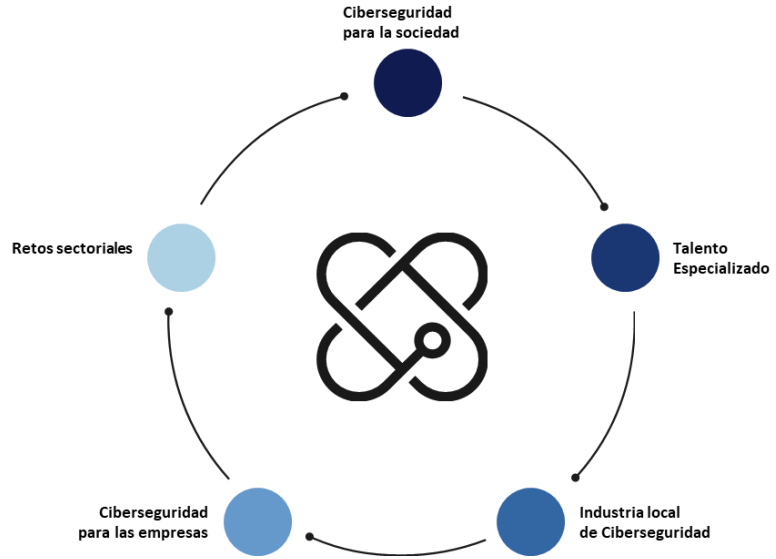
A través de esta técnica, los ciberdelincuentes obtienen mucha información sobre sus posibles víctimas antes de actuar. «Incluso pueden desarrollar un perfil de a quién les interesa dirigirse y a quién no, todo ello sin moverse de su mesa de trabajo», añade el experto. «A esto le añadimos las técnicas de ingeniería social: llamadas de teléfono, correos electrónicos..., que es lo que más daño hace ahora. A través de estas, se envían mensajes muy bien dirigidos y en los que, en muchos casos, nos demuestran que conocen datos que asumimos que solo tienen unas determinadas empresas con las que tenemos relación. En esas situaciones, estamos más inclinados a confiar en la persona que se dirige a nosotros y a dar a estos sujetos la información que les falta», relata Salgado.

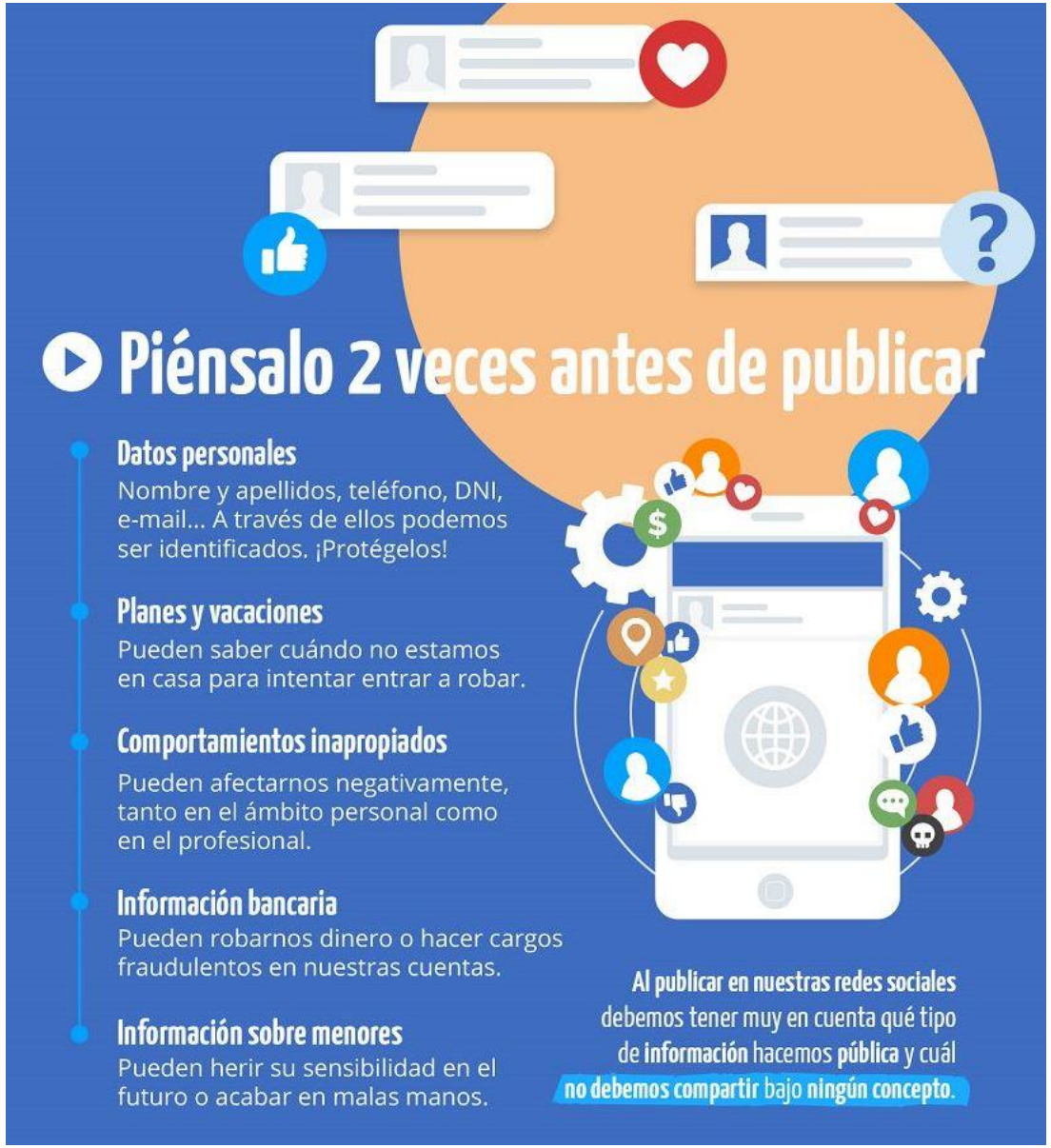
En el caso del establecimiento coruñés, su encargada cree que los delincuentes pudieron acceder a los datos de la empresa de transporte o incluso tener hackeadas las cámaras de la tienda, que van por wifi.

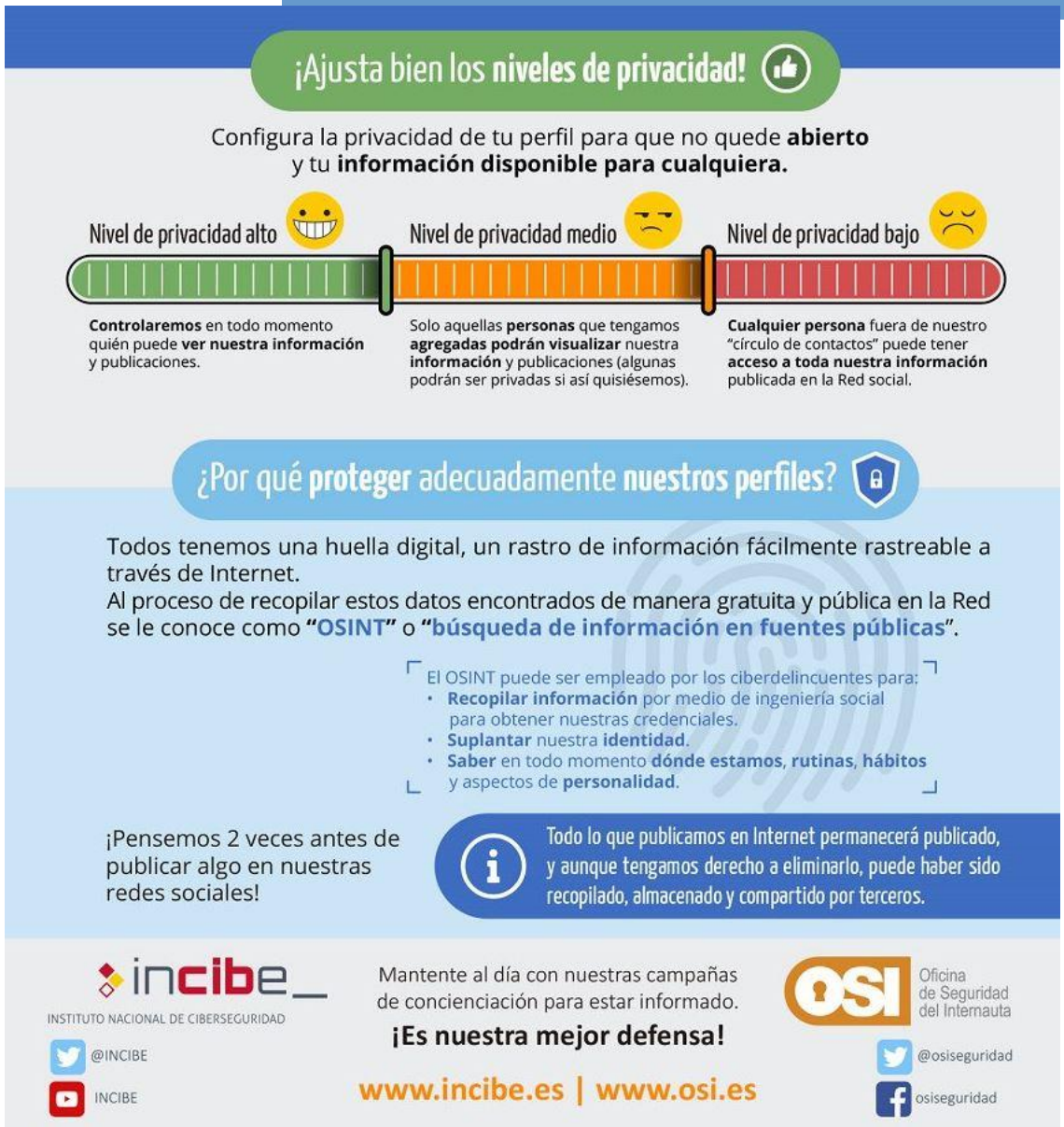
Para evitar ser víctima de este tipo de delitos, el experto insiste en la importancia de realizar periódicamente una comprobación de los datos personales que se encuentran disponibles en internet. «También es muy recomendable cambiar las contraseñas cada cierto tiempo, porque en muchos casos, las bases de datos las incluyen», explica. Y precisamente con esta información, un ciberdelincuente podría acceder, por ejemplo, al correo electrónico y a todos los mensajes que se acumulan en el servidor.

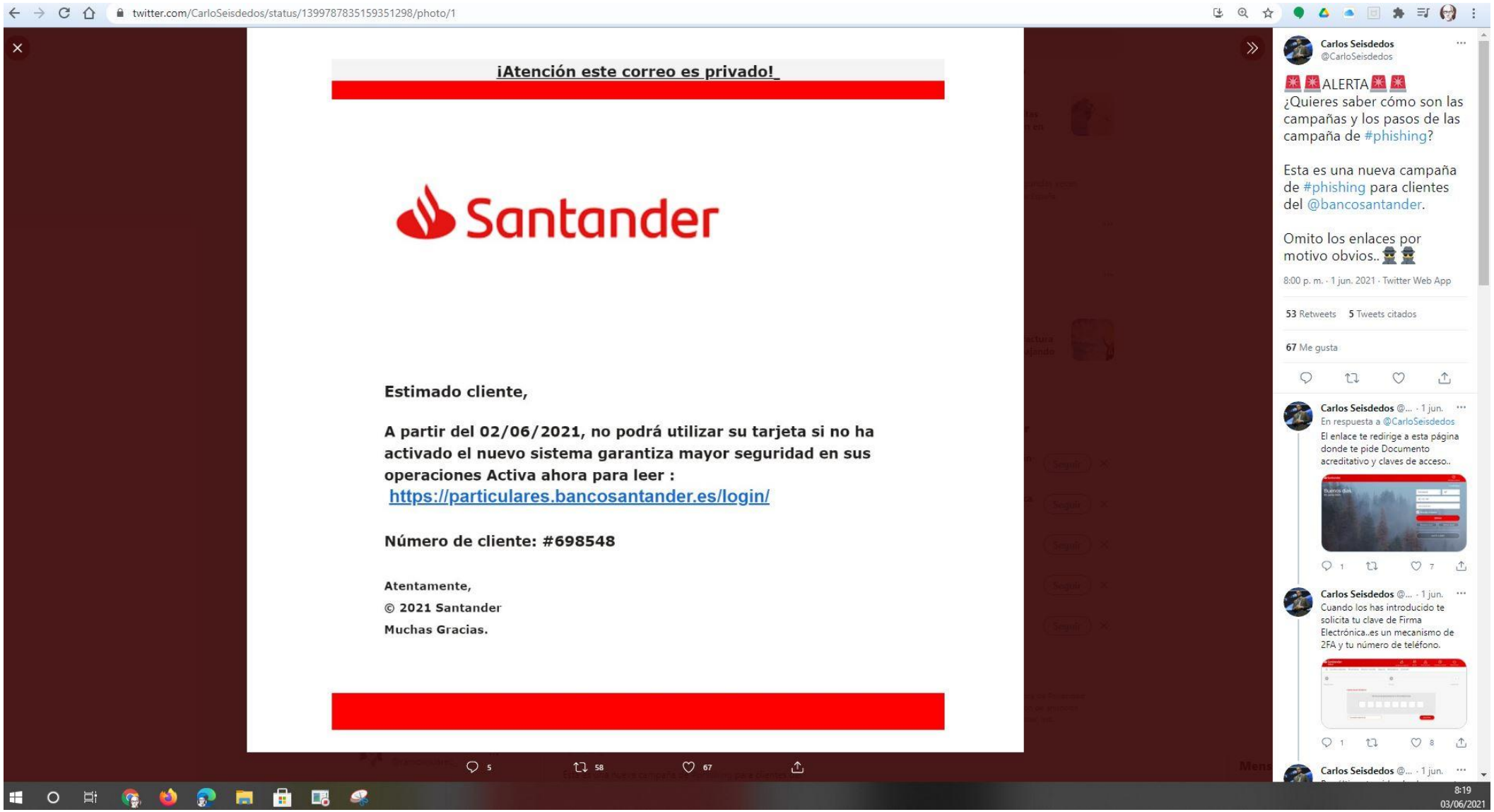
Aumento de las ciberestafas

Durante el 2021, las estafas cibernéticas aumentaron en Galicia un 53 %, con casi 20.000 fraudes a través de internet. A raíz de esto, las fuerzas de seguridad del Estado aumentaron sus actuaciones contra la delincuencia digital, incrementando el número de agentes especializados en este ámbito tanto en la Policía Nacional como en la Guardia Civil. Desde las instituciones creen que es necesario concienciar a la ciudadanía, puesto que se trata de casos difíciles de investigar.

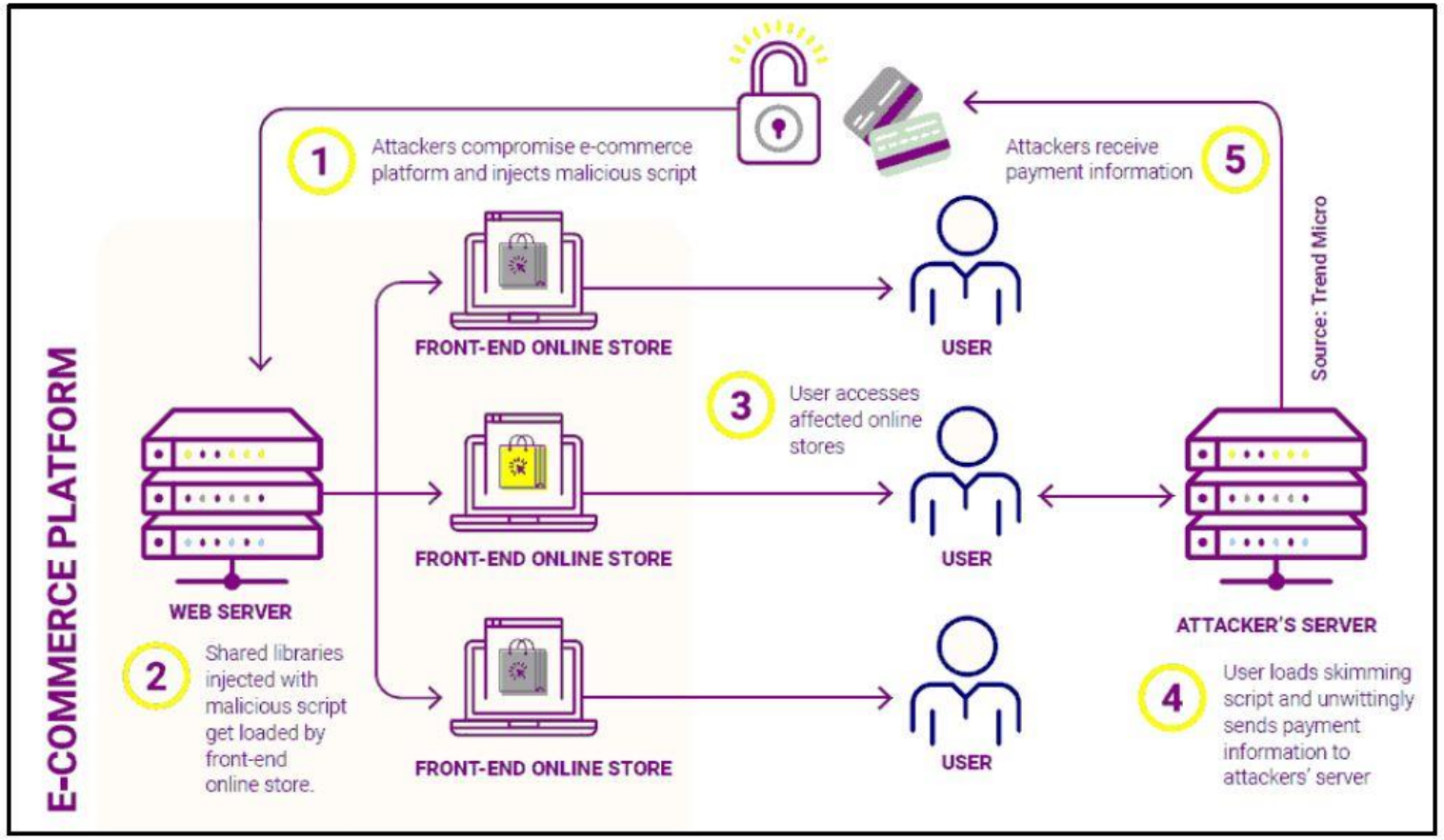



Piénsalo 2 veces antes de publicar
Datos personales
Nombre y apellidos, teléfono, DNI, e-mail... A través de ellos podemos ser identificados. ¡Protégelos!
Planes y vacaciones
Pueden saber cuándo no estamos en casa para intentar entrar a robar.
Comportamientos inapropiados
Pueden afectarnos negativamente, tanto en el ámbito personal como en el profesional.
Información bancaria
Pueden robarnos dinero o hacer cargos fraudulentos en nuestras cuentas.
Información sobre menores
Pueden herir su sensibilidad en el futuro o acabar en malas manos.
Al publicar en nuestras redes sociales debemos tener muy en cuenta qué tipo de información hacemos pública y cuál no debemos compartir bajo ningún concepto.


¡Ajusta bien los niveles de privacidad!
Configura la privacidad de tu perfil para que no quede abierto y tu información disponible para cualquiera.
Nivel de privacidad alto
Nivel de privacidad medio
Nivel de privacidad bajo
Controlaremos en todo momento quién puede ver nuestra información y publicaciones.
Solo aquellas personas que tengamos agregadas podrán visualizar nuestra información y publicaciones (algunas podrán ser privadas si así quisiésemos).
Cualquier persona fuera de nuestro "círculo de contactos" puede tener acceso a toda nuestra información publicada en la Red social.
¿Por qué proteger adecuadamente nuestros perfiles?
Todos tenemos una huella digital, un rastro de información fácilmente rastreable a través de Internet.
Al proceso de recopilar estos datos encontrados de manera gratuita y pública en la Red se le conoce como "OSINT" o "búsqueda de información en fuentes públicas".
El OSINT puede ser empleado por los ciberdelincuentes para:
Recopilar información por medio de ingeniería social para obtener nuestras credenciales.
Suplantar nuestra identidad.
Saber en todo momento dónde estamos, rutinas, hábitos y aspectos de personalidad.
¡Pensemos 2 veces antes de publicar algo en nuestras redes sociales!
Todo lo que publicamos en Internet permanecerá publicado, y aunque tengamos derecho a eliminarlo, puede haber sido recopilado, almacenado y compartido por terceros.
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
@INCIBE
INCIBE
Mantente al día con nuestras campañas de concienciación para estar informado.
¡Es nuestra mejor defensa!
www.incibe.es | www.osi.es
OSI
Oficina de Seguridad del Internauta
@osiseguridad
osiseguridad


twitter.com/CarloSeisdedos/status/1399787835159351298/photo/1
¡Atención este correo es privado!_
Santander
Estimado cliente,
A partir del 02/06/2021, no podrá utilizar su tarjeta si no ha activado el nuevo sistema garantiza mayor seguridad en sus operaciones Activa ahora para leer :
https://particulares.bancosantander.es/login/
Número de cliente: #698548
Atentamente,
© 2021 Santander
Muchas Gracias.
Carlos Seisdedos
@CarloSeisdedos
ALERTA
¿Quieres saber cómo son las campañas y los pasos de las campaña de #phishing?
Esta es una nueva campaña de #phishing para clientes del @bancosantander.
Omito los enlaces por motivo obvios..
8:00 p. m. · 1 jun. 2021 · Twitter Web App
53 Retweets 5 Tweets citados
67 Me gusta
Carlos Seisdedos @... · 1 jun.
En respuesta a @CarloSeisdedos
El enlace te redirige a esta página donde te pide Documento acreditativo y claves de acceso..
Carlos Seisdedos @... · 1 jun.
Cuando los has introducido te solicita tu clave de Firma Electrónica..es un mecanismo de 2FA y tu número de teléfono.
8:19
03/06/2021

ESTUDIO SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA | 2019



Infografía nº 3.- Esquema de EUROPOL donde se refleja el acceso por ciberdelincuentes a datos bancarios de clientes en plataformas de comercio electrónico.

Los #cibercriminales también hacen #OSINT.

Cada vez nos desinhibimos más en #RRSS y eso puede tener unas repercusiones nefastas en nuestras vidas.

Si no queremos ser víctima de los #cibercriminales hagamos caso a las recomendaciones del @dsn, @INCIBE y @osiseguridad.

Récord de ciberestafas en cinco meses en Vigo

E. V. PITA
VIGO / LA VOZ

CNP

Los ocho policías de Vigo están «saturados» con casi 1.400 denuncias desde enero en Vigo. Los casos se han disparado un 20 %

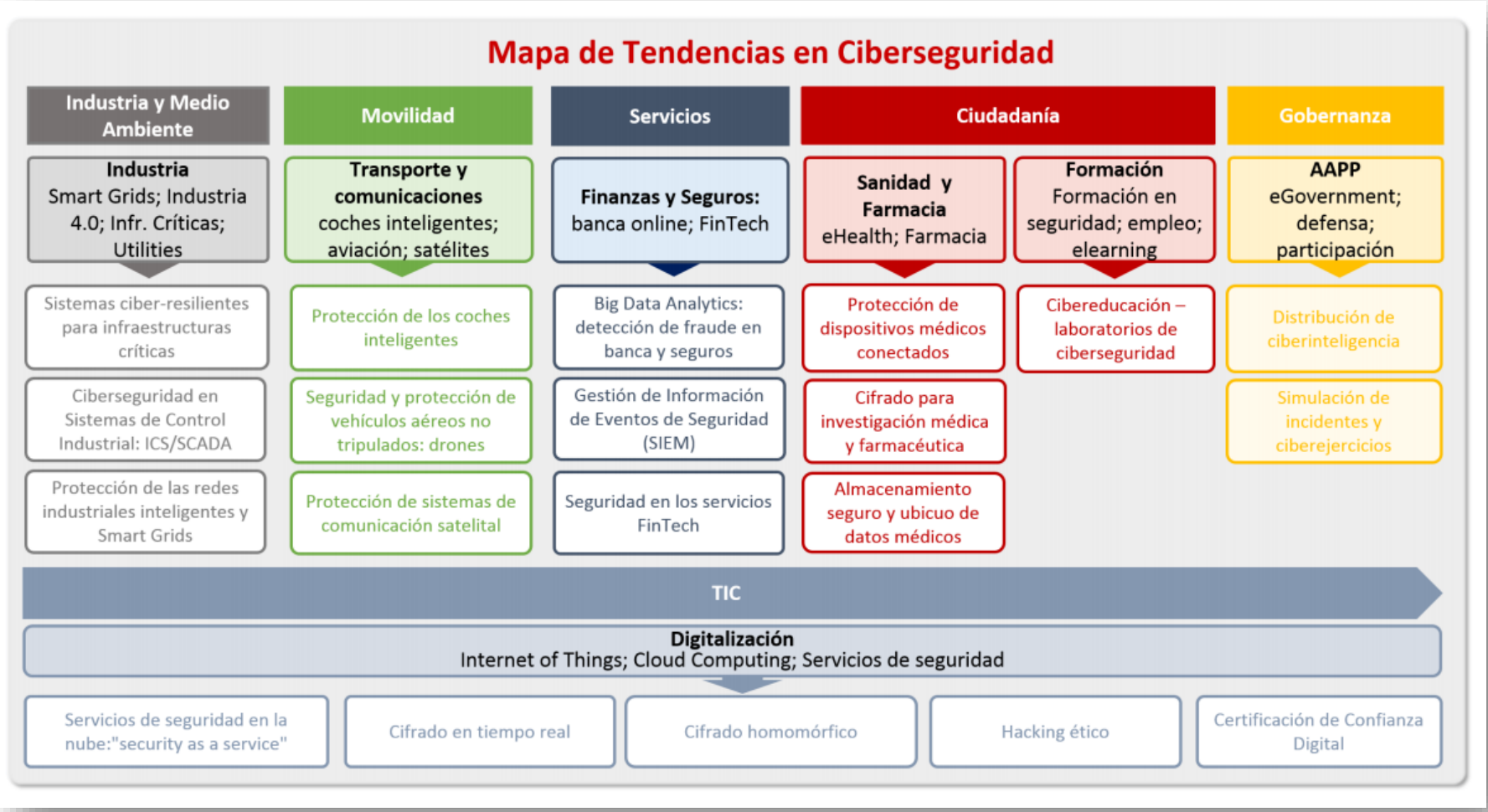
03 jun 2021 . Actualizado a las 05:00 h.

Hay tranquilidad en el juzgado de guardia de Vigo. Nada destacable salvo las denuncias por estafas por Internet, que ya son la rutina del día a día. «Están llegando varias denuncias al día, no aquí sino a todos los juzgados», dice un letrado judicial. En los últimos cinco meses, **Vigo ha registrado alrededor de 1.400 denuncias por estafas informáticas**, un auténtico récord. La **provincia de Pontevedra** acumuló entre enero y mayo, 2.200 casos. La ciberdelincuencia se ha disparado el 20 % respecto al último semestre del 2020, en plena segunda ola de la pandemia.

Esta avalancha se explica por varios motivos: los clientes de la banca tradicional están migrando a las aplicaciones on line. Por otro lado, la pandemia ha acelerado el uso de compras en tiendas por Internet. Y por donde nada el dinero, siempre hay pescadores al acecho. A ello se suman las recientes denuncias de ahorradores vigueses que perdieron hasta 70.000 euros en inversiones que

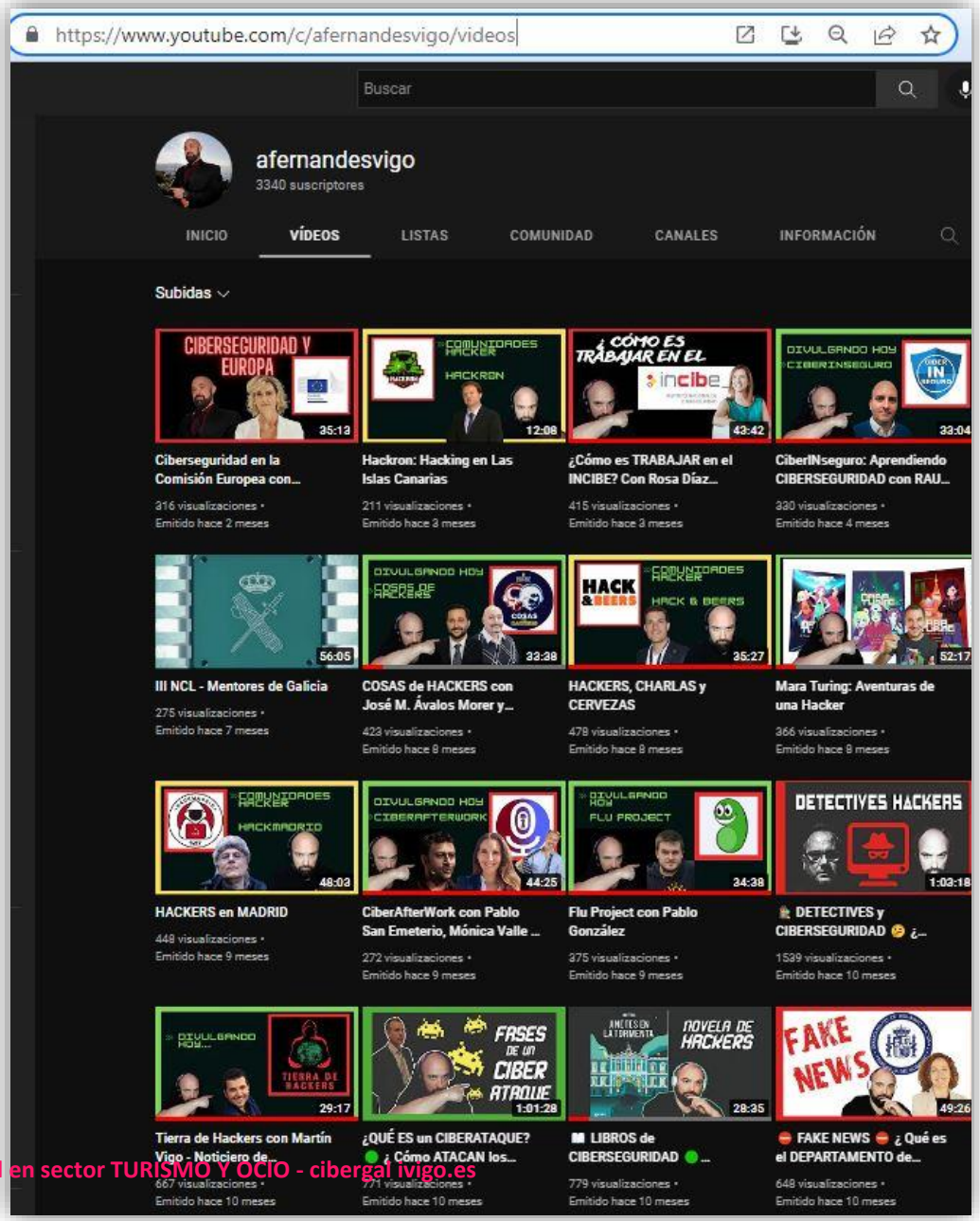
Roberto González
(Policía Nacional en activo, secretario general del SUP en Galicia y miembro del Consejo de Policía).

Entrevista en CRTVG con #SUPGalicia #PoliciaNacional sobre el inicio de nuestro CURSO DE CIBERSEGURIDAD
Hoy 14-06-2021 nos entrevistan con #SUPGalicia de la #PoliciaNacional sobre el inicio de nuestro CURSO DE CIBERSEGURIDAD para Fuerzas y Cuerpos de Seguridad del Estado.
En la Corporación Radio e Televisión de Galicia min: 01:05:00
https://lnkd.in/ehi5Fvj
#ciberseguridad #CyberSecurity #TransformacionDigital #Galicia #futuresociety


Mapa de Tendencias en Ciberseguridad
Industria y Medio Ambiente
Movilidad
Servicios
Ciudadanía
Gobernanza
Industria
Smart Grids; Industria 4.0; Infr. Críticas; Utilities
Transporte y comunicaciones
coches inteligentes; aviación; satélites
Finanzas y Seguros:
banca online; FinTech
Sanidad y Farmacia
eHealth; Farmacia
Formación
Formación en seguridad; empleo; elearning
AAPP
eGovernment; defensa; participación
Sistemas ciber-resilientes para infraestructuras críticas
Protección de los coches inteligentes
Big Data Analytics: detección de fraude en banca y seguros
Protección de dispositivos médicos conectados
Cibereducación – laboratorios de ciberseguridad
Distribución de ciberinteligencia
Ciberseguridad en Sistemas de Control Industrial: ICS/SCADA
Seguridad y protección de vehículos aéreos no tripulados: drones
Gestión de Información de Eventos de Seguridad (SIEM)
Cifrado para investigación médica y farmacéutica
Simulación de incidentes y ciberejercicios
Protección de las redes industriales inteligentes y Smart Grids
Protección de sistemas de comunicación satelital
Seguridad en los servicios FinTech
Almacenamiento seguro y ubicuo de datos médicos
TIC
Digitalización
Internet of Things; Cloud Computing; Servicios de seguridad
Servicios de seguridad en la nube:"security as a service"
Cifrado en tiempo real
Cifrado homomórfico
Hacking ético
Certificación de Confianza Digital


REAL ACADEMIA ESPAÑOLA
Diccionario de la lengua española
Edición del Tricentenario
Actualización 2020
Consulta posible gracias al compromiso con la cultura de la
Fundación "la Caixa"
por palabras
Escriba aquí la palabra
Consultar
jáquer
Del ingl. hacker.
1. m. y f. Inform. pirata informático.
2. m. y f. Inform. Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora.
Real Academia Española © Todos los derechos reservados


https://www.linkedin.com/in/afernandesvigo/
Buscar
Inicio
Mi red
Empleos
Mensaje
... el S-SDLC es el futuro!!
Antonio Fernandes · 1er
Hacker y Responsable de Ciberseguridad
Temas que suele tratar: #hacker, #hackers, #infosec, #cybersecurity y #ciberseguridad
Vigo, Galicia / Galiza, España · Información de contacto
7712 seguidores · Más de 500 contactos
Financiera Maderera S.A.
Massachusetts Institute of Technology - Sloan School of Management


https://www.youtube.com/c/afernandesvigo/videos
Buscar
afernandesvigo
3340 suscriptores
INICIO
VÍDEOS
LISTAS
COMUNIDAD
CANALES
INFORMACIÓN
Subidas
Ciberseguridad en la Comisión Europea con...
316 visualizaciones • Emitido hace 2 meses
Hackron: Hacking en Las Islas Canarias
211 visualizaciones • Emitido hace 3 meses
¿Cómo es TRABAJAR en el INCIBE? Con Rosa Díaz...
415 visualizaciones • Emitido hace 3 meses
CiberINseguro: Aprendiendo CIBERSEGURIDAD con RAU...
330 visualizaciones • Emitido hace 4 meses
III NCL - Mentores de Galicia
275 visualizaciones • Emitido hace 7 meses
COSAS de HACKERS con José M. Ávalos Morer y...
423 visualizaciones • Emitido hace 8 meses
HACKERS, CHARLAS y CERVEZAS
478 visualizaciones • Emitido hace 8 meses
Mara Turing: Aventuras de una Hacker
366 visualizaciones • Emitido hace 8 meses
HACKERS en MADRID
448 visualizaciones • Emitido hace 9 meses
CiberAfterWork con Pablo San Emeterio, Mónica Valle ...
272 visualizaciones • Emitido hace 9 meses
Flu Project con Pablo González
375 visualizaciones • Emitido hace 9 meses
DETECTIVES y CIBERSEGURIDAD
1539 visualizaciones • Emitido hace 10 meses
Tierra de Hackers con Martín Vigo - Noticiero de...
667 visualizaciones • Emitido hace 10 meses
¿QUÉ ES un CIBERATAQUE? ¿Cómo ATACAN los...
771 visualizaciones • Emitido hace 10 meses
LIBROS de CIBERSEGURIDAD
779 visualizaciones • Emitido hace 10 meses
FAKE NEWS ¿Qué es el DEPARTAMENTO de...
648 visualizaciones • Emitido hace 10 meses

VIGO
video iVigo 2020-09-19 PontUP HACKERS GALEGAS QUE DEFENDEN EL #CIBERESPACIO

19 visualizaciones • 19 oct 2020 2 0 COMPARTIR GUARDAR

ivigo Business Space
54 suscriptores
SUSCRITO

HACKERS GALLEGAS QUE DEFIENDEN EL #CIBERESPACIO
Mesa redonda entre hackers éticas y expertas en ciberseguridad, que debatirán sobre el presente y futuro del ciberespacio, las venturas y desventuras que encuentran en su profesión, así como, sobre el futuro de los perfiles profesionales y el emprendimiento en esta disciplina.

La RAE define «hacker» como persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora. La transformación digital es imparable en todos los países del mundo, por lo que se necesitan cada vez más profesionales expertos en ciberseguridad, ciberdefensa y uso ético de nuestros datos. Expertas gallegas contarán su experiencia desde dentro de la gran red de redes, y expondrán las situaciones con las que se encuentran y como las resuelven cada día.

Ponentes:
- Olalla Sánchez Suárez @OlallaSanchezs #Women4Cyber Ingeniera Teleco, Hacker ética, Consultora de Ciberseguridad, Cofundadora del Congreso de Ciberseguridad ViCON.gal

- Pilar Vila @PilarinaVilla #Women4Cyber Ingeniera Informática, CEO cofundadora de Forensic & Security y de DFTools Digital Forensics Analyst. CSE Chief Security Envoy en ElevenPaths. Emprendedora

- Susana Rey Baldomir, Ingeniera Teleco, Delegada de Protección de Datos (DPO) en Grupo Euskaltel, Virgin Telco, R y Telecable, Experta en Ciberseguridad

- Lilian Adkinson @lilian_adkinson, Ingeniera Teleco, Responsable de Analítica en Seguridad y Privacidad en Gradiant, Investigadora en Ciberseguridad

- Sara Suárez Gonzalo @SaraSuarezG Doctora en Comunicación, Científica Social, Investigadora #BigData #privacidad #InteligenciaArtificial y #algoritmia en la UPF

Organiza: iVigo Business Space (iVigo.es)

Presenta y modera Ramón Suárez @RamonSuarez_ CEO de iVigo Business Space (iVigo.es) y Cofundador del Congreso de Ciberseguridad ViCON.gal

video iVigo 2020-09-19 PontUP HACKERS GALEGA...

ivigo Business Space
54 suscriptores

HACKERS GALLEGAS QUE DEFIENDEN EL #CIBERESPACIO
Mesa redonda entre hackers éticas y expertas en ciberseguridad, que debatirán sobre el presente y futuro del ciberespacio, las venturas y desventuras que encuentran en su profesión, así como, sobre el futuro de los perfiles profesionales y el emprendimiento en esta disciplina.

La RAE define «hacker» como persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora. La transformación digital es imparable en todos los países del mundo, por lo que se necesitan cada vez más profesionales expertos en ciberseguridad, ciberdefensa y uso ético de nuestros datos. Expertas gallegas contarán su experiencia desde dentro de la gran red de redes, y expondrán las situaciones con las que se encuentran y como las resuelven cada día.

Ponentes:
- Olalla Sánchez Suárez @OlallaSanchezs #Women4Cyber Ingeniera Teleco, Hacker ética, Consultora de Ciberseguridad, Cofundadora del Congreso de Ciberseguridad ViCON.gal

- Pilar Vila @PilarinaVilla #Women4Cyber Ingeniera Informática, CEO cofundadora de Forensic & Security y de DFTools Digital Forensics Analyst. CSE Chief Security Envoy en ElevenPaths. Emprendedora

- Susana Rey Baldomir, Ingeniera Teleco, Delegada de Protección de Datos (DPO) en Grupo Euskaltel, Virgin Telco, R y Telecable, Experta en Ciberseguridad

- Lilian Adkinson @lilian_adkinson, Ingeniera Teleco, Responsable de Analítica en Seguridad y Privacidad en Gradiant, Investigadora en Ciberseguridad

- Sara Suárez Gonzalo @SaraSuarezG Doctora en Comunicación, Científica Social, Investigadora #BigData #privacidad #InteligenciaArtificial y #algoritmia en la UPF

Organiza: iVigo Business Space (iVigo.es)

Presenta y modera Ramón Suárez @RamonSuarez_ CEO de iVigo Business Space (iVigo.es) y Cofundador del Congreso de Ciberseguridad ViCON.gal

La Voz de Galicia

VIGO

La joven que vigila al Gran Hermano

E. V. PITA
VIGO / LA VOZ

La investigadora viguesa Sara Suárez-Gonzalo, experta en extracción masiva de datos (Big Data), recibe un premio europeo

29 ene 2019 . Actualizado a las 21:21 h.

Comentar · 0

¿Nuestro cepillo de dientes eléctrico, la tele y el robot aspiradora nos espían? ¿Un Gran Hermano nos vigila a través de nuestros datos? El *influencer* experto en la Industria 4.0 Ramón Suárez recalca que ahora mismo hay profesionales vigueses que están en primera línea mundial de investigación en la explotación masiva de datos (el Big Data) y algoritmos, como es el caso de Sara Suárez-Gonzalo, de 26 años.

Precisamente, el Big Data es el tema de la tesis doctoral que está redactando esta joven viguesa. Suárez-Gonzalo es investigadora predoctoral en la Universidad Pompeu Fabra de Barcelona y quiere terminar la tesis este mismo año. Dicho trabajo está vinculado al grupo de Investigación en Comunicación Política, Medios y Democracia (Polcom).

Su tesis se centra en el impacto social del fenómeno Big Data y en el valor de la privacidad para proteger los datos personales frente a su explotación masiva mediante técnicas algorítmicas de Inteligencia Artificial, *machine learning* (aprendizaje automatizado) o *deep learning* (aprendizaje profundo). Acaba de ser galardonada con el premio europeo de investigación que otorga la Young

Una viguesa experta en big data gana el premio a la investigación audiovisual

Sara Suárez es reconocida por el Consejo del Audiovisual de Cataluña por su tesis sobre el análisis masivo de datos en las redes

E. V. PITA
VIGO / LA VOZ

La doctora Sara Suárez obtuvo un premio a la investigación.

Cualquiera que haya navegado por Internet ha tenido la sensación de que los publicistas conocen demasiado bien sus gustos. ¿Nos están vigilando a través de nuestros móviles? Precisamente eso es lo que analizó la Sara Suárez Gonzalo (Vigo, 1992), experta en *big data* (análisis masivo de datos). Sus pesquisas le han valido el equivalente al Goya del audiovisual español por una investigación.

El Consejo del Audiovisual de Cataluña (CAC) la ha declarado ganadora de la XXI edición de su certamen y le ha otorgado el primer premio a la investigación, dotado con 5.000 euros. Le concede el galardón por los méritos logrados con su tesis doctoral titulada *Big data, poder y libertad. Sobre el impacto social y político de la vigilancia masiva.*

Se trata de un estudio que analiza la llamada sociedad de la vigilancia, en la que el ciudadano regala sus datos a cambio de acceso gratis a aplicaciones como Facebook, Instagram o el correo electrónico. La autora profundiza en la filosofía del todo gratis que se oculta tras estos contratos que ningún usuario lee al acceder a los servicios de una plataforma *on line*. Como dice un dicho de Silicon Valley: «Si te ofrecen algo gratis, es que el producto eres tú».

El premio concedido a Sara Suárez es único y lo decide un jurado compuesto por siete investigadores independientes de varias universidades. La entrega del galardón será en marzo.

«La comparación con los Oscar la veo exagerada pero es un premio muy bien valorado y un gran reconocimiento al trabajo que he hecho en los últimos años y eso, en el mundo de la investigación, se agradece mucho», dice la ganadora. Defendió su tesis en diciembre del 2019 en la Universitat Pompeu Fabra de Barcelona.

«Es un premio competitivo al que concurren todas las investigaciones sobre temáticas de comunicación, realizadas desde cualquier disciplina, como la comunicación, el derecho, la economía, la ciencia política o la sociología, entre otras», afirma.

La tesis examina las consecuencias sociales de la explotación de datos masivos. Se compone de cinco artículos publicados en revistas de investigación, y una memoria que liga todas las aportaciones. Analiza la idea de privacidad que subyace al reglamento europeo de protección de datos, y estudia casos como el Cambridge Analytica, o el del *chatbot* Tay de Microsoft.

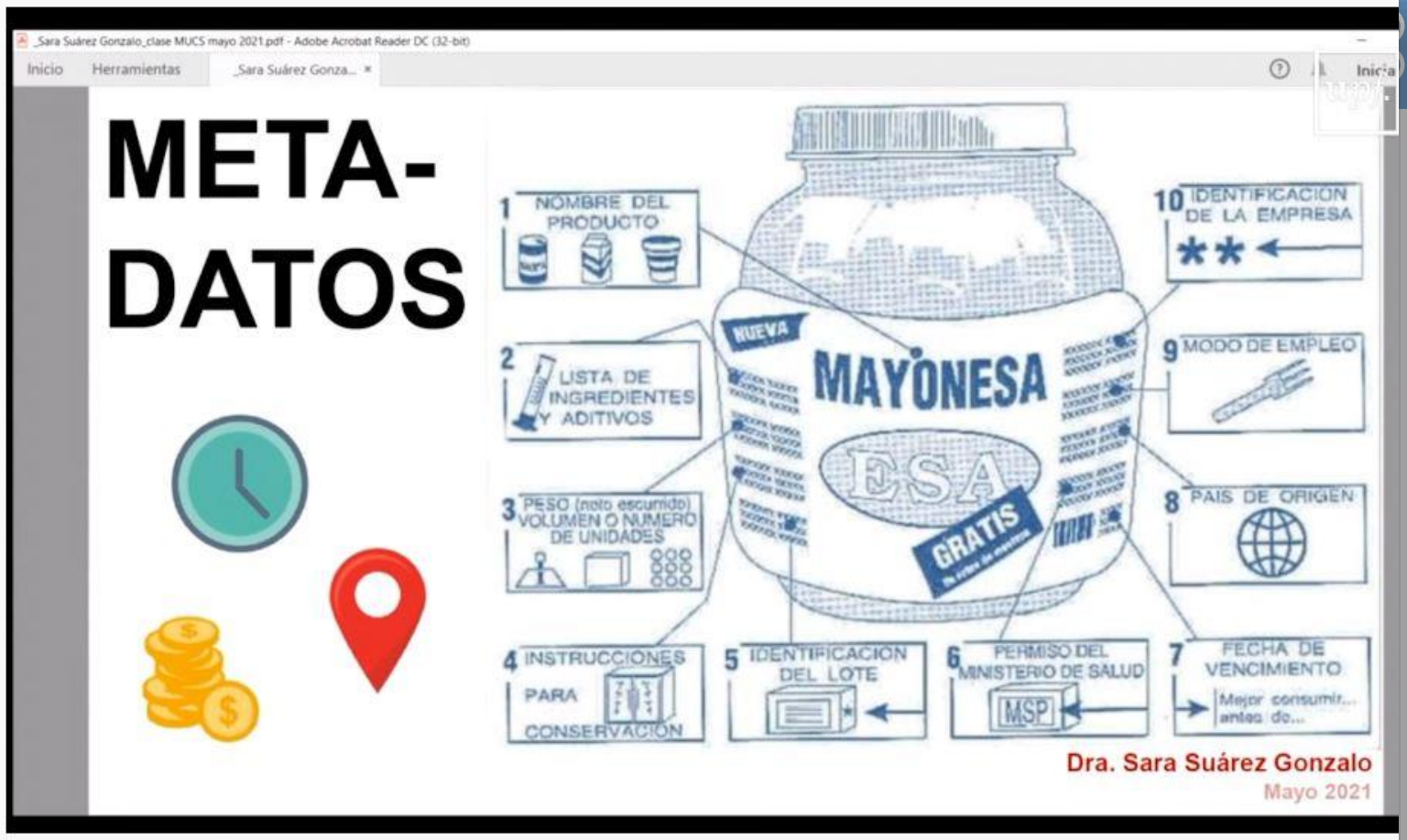
Sociedad de la vigilancia

La doctora señala que la «vigilancia» se entiende como una forma de espionaje, que implica que alguien actúa desde la sombra, mediante métodos dudosos, para obtener información sobre una persona y utilizarla en su contra. Pero en su tesis, la palabra *vigilancia* no tiene este significado. «La teoría republicana, en la que me baso, define la vigilancia como la consecuencia de una desigualdad de poder, que permite a alguien interferir en la vida de una o más personas, sin que estas puedan controlar esta interferencia por sus propios medios», explica.

Según Suárez, esto implica que la parte vigilante se sitúa en una posición de superioridad que le permitiría ejercer esta interferencia sobre la otra parte, si lo desea. «En nuestra sociedad, quienes se benefician de esta desigualdad de poder son, sobre todo, cinco grandes empresas tecnológicas: Google, Amazon, Facebook, Apple y Microsoft (GAFAM). ¿Qué les permite este privilegio? Estas empresas transnacionales comercializan productos y servicios necesarios para llevar una vida normal en las sociedades avanzadas», dice.

La autora sugiere reflexionar sobre el buscador de Google, el Whatsapp o el Microsoft Word. «Para utilizar estos productos, debemos consentir, individualmente, que estas empresas recopilen y utilicen nuestros datos. De lo contrario, ni podríamos usarlos ni podrían existir. Por eso, esquivar este poder, no es tan fácil como oponerse a darles los datos», dice. Añade que, además, la difusión de nuestros datos personales no es algo personal. «Por poner un ejemplo, tus amigos, los que sí usan Instagram, también le están proporcionando a la plataforma datos sobre ti. Esta desigualdad nos afecta a todas y todos, como individuos y como sociedad, y no podemos revertirlo individualmente. Se trata de un problema estructural», concluye.

El Consejo del Audiovisual de Cataluña es la autoridad independiente de regulación de la comunicación audiovisual de Cataluña. No hay un equivalente en otras comunidades autónomas (salvo en Andalucía), ni nada similar a nivel nacional.



Seminario / Taller: Métodos y recursos para la investigación y la comunicación académica

55 visualizaciones • 26 may 2021

4 0 COMPARTIR GUARDA

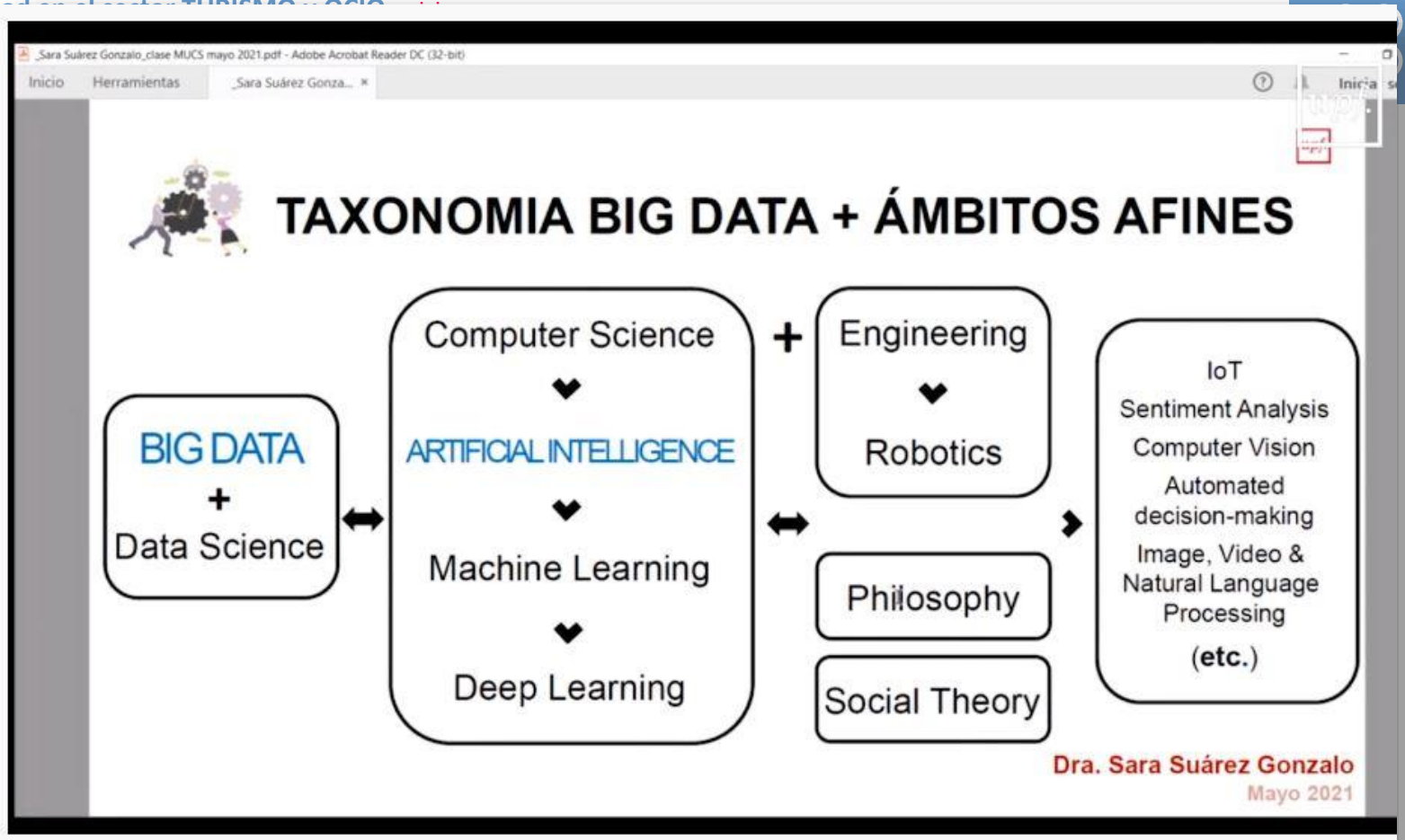
upf. Universitat Pompeu Fabra - Barcelona
6930 suscriptores

SUSCRI

Activitat organitzada pel Màster Universitari en Investigació en Comunicació Social.
Departament de Comunicació. Universitat Pompeu Fabra. 17 de maig del 2021

0 comentarios ORDENAR POR

Añade un comentario público...



Seminario / Taller: Métodos y recursos para la investigación y la comunicación académica

55 visualizaciones • 26 may 2021

4 0 COMPARTIR GUARDAR

upf. Universitat Pompeu Fabra - Barcelona
6930 suscriptores

SUSCRIBI

Activitat organitzada pel Màster Universitari en Investigació en Comunicació Social.
Departament de Comunicació. Universitat Pompeu Fabra. 17 de maig del 2021

0 comentarios ORDENAR POR

Añade un comentario público...

incibe.es

English | Contacto | Tu Ayuda en Ciberseguridad | Agenda | Sala de prensa | Encuestas | Mapa web

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Protege tu empresa | Eventos | Otras actividades | Conoce INCIBE

#AprendeCiberseguridad con INCIBE

Cada semana y de una manera muy sencilla, te explicaremos en nuestras redes sociales un concepto general o una tipología de incidente de seguridad habitual. ¿Nos sigues en @incibe?

#AprendeCiberseguridad

TU AYUDA EN CIBERSEGURIDAD

Guía de ciberataques

Todo lo que debes saber a nivel usuario

Índice

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Protege tu empresa · Eventos · Otras actividades · Conoce INCIBE

TU AYUDA EN
CIBERSEGURIDAD

Ver en YouTube

VICEPRESIDENCIA TERCERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Casos reales

Bulo COVID

Suplantación de identidad - RRSS

Estafa

Robo cuenta videojuego

Suplantación de identidad - SMS

Ciberacoso

Uso excesivo

Phishing

Publicaciones

El sector turístico se ha posicionado como una de las tres industrias target para el cibercrimen

Un proceso de transformación digital como palanca de crecimiento, junto al establecimiento de una adecuada estrategia de ciberseguridad, es la clave para la adaptación al ecosistema digital y al éxito en el sector turístico.

Expectativas de Turismo, informe elaborado por Deloitte, señala que la **ciberseguridad** es uno de los puntos protagonistas en la agenda del CEO de la industria turística. La preocupación por la amenaza del cibercrimen ha crecido considerablemente en los últimos años. Por ello, la Unión Europea anunció en 2016 el establecimiento de una estrategia público-privada en ciberseguridad con una inversión de 450 millones de euros.

El sector turístico se enfrenta a grandes amenazas en materia de ciberseguridad como son el robo de información (para venderlo en el mercado negro); ataques que provocan la disrupción del negocio (no permiten a las compañías prestar los servicios); y ataques que afectan a la calidad del servicio (degradan la experiencia del usuario). Los datos muestran que el 89% de los ciberataques tienen motivos financieros y de espionaje, lo que pone de manifiesto que cualquier información puede ser monetizable. Asimismo, El riesgo en el sector turístico se incrementa en su cadena de valor, en la que aparecen negocios de terceros que completan la propuesta, añadiendo nuevos riesgos sobre la seguridad de los datos de sus clientes y de la propia compañía.

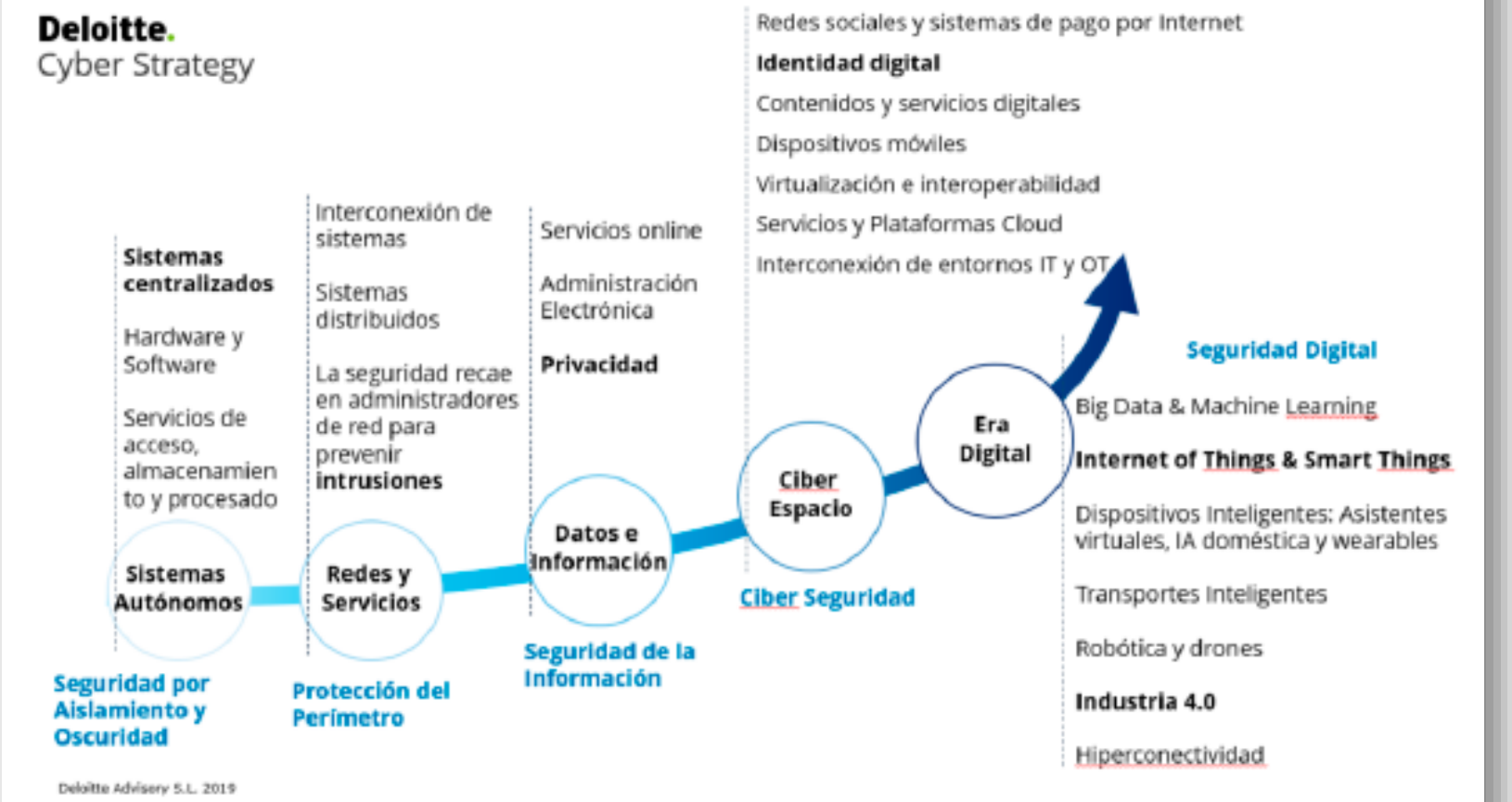
Pérdida de confianza de los clientes, daño a la reputación de la marca, pérdidas económicas y riesgos legales constituyen las principales **consecuencias** del ciberataque en la industria turística. Pese a que estos ataques crecen exponencialmente, muchos de estos riesgos pueden ser evitados, o al menos controlados, si aplicamos las siguientes **medidas de seguridad**:

1. Seguridad en los datos: debemos reunir la información necesaria y limitar su acceso a terceros (partners, agencias de marketing, etc.).
2. Control de accesos a los datos más sensibles: restringimos el acceso de datos

Descarga el informe Expectativas de Turismo 2017

https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/ciberseguridad-sector-turistico.html

Figura 1. Evolución de la transformación digital



Fuente: Deloitte Cyber Strategy.

Andalucía lab · itrem · FIT Canarias Factoría de Innovación Turística · Generalitat Valenciana · Invat·tur · ITH Instituto Tecnológico Hotelero · eurecat Centre Tecnològic de Catalunya · tecnalia Member of Basque Research & Technology Alliance · turistec · vicomtech Member of Basque Research & Technology Alliance · Segittur turismo e innovación · Gobierno de España Ministerio de Ciencia e Innovación · thinktur Plataforma Tecnológica del Turismo

ciber.gal · iVIGO Business Space · Deputación Pontevedra

ÍNDICE

Mitigar los riesgos de ciberseguridad *(Identificar, Proteger, Detectar, Responder y Recuperar - NIST Cybersecurity Framework)*: implantando un plan director en ciberseguridad, realizando diagnósticos de seguridad que nos alerten de posibles amenazas, haciendo auditorías de cumplimiento, analizando aplicaciones e infraestructuras (incluyendo WIFIs), implantando soluciones tecnológicas de ciberseguridad, disponer de un BIA y un Plan de Continuidad de Negocio...

Concienciación y Formación: analizando las probabilidades de éxito realizando ataques simulados de phishing, módulos en entrenamiento interactivos, herramientas de *reporting* de incidentes e informes de resultados.

El sector turístico como una de las industrias objetivo top para los ciberdelincuentes.

VULNERABILIDADES

Ejemplos de vulnerabilidades:

- **Diseño**
  - Debilidad en el diseño de los protocolos utilizados en las redes, políticas de seguridad deficientes e inexistentes...
- **Implementación**
  - Errores de programación, existencia de "puertas traseras", descuidos de los fabricantes...
- **Operación/Control**
  - Configuración inadecuada de los sistemas, desconocimiento y falta de sensibilización de los usuarios y de los responsables de los sistemas, disponibilidad de herramientas que facilitan los ataques...
- **Vulnerabilidades de día cero**

www.eurecat.org

ATAQUES/AMENAZAS

- La mayoría de ataques o amenazas **se pueden clasificar en una de estas categorías**:
  - Secuestro de datos (Ransomware),
  - Suplantación de identidad (spoofing),
  - Phishing,
  - Denegación de servicio (DoS),
  - Manipulación (tampering),
  - Espionaje (eavesdropping),
  - Puerta trasera,
  - Ingeniería social,
  - Ataque directo,
  - Escalada de privilegios.

www.eurecat.org

gal iVIGO BUSINESS SPACE DEPUTACIÓN PONTEVEDRA

La ciberseguridad, identificada como el

BRECHAS DE DATOS

SECUESTRO DE DATOS

Un ha
llaves

Los hotel
blancos d

Por Manu Con

Un hotel a
ransomwa
puertas de

Photo

Marriott says ... may have exposed ... guests. This marks Marriott's second data breach in

...base breach

...mers

...eal

...reach

MALWARE

RevengeHotels una c
para robar datos de la
los clientes de

5 diciembre, 2019 Por Fernando Ramíre

Una campaña de malware denomi
más de 20 hoteles en varios países
y poder hacer compras con ellas p

Home › News › Se

Hackers T

By Sergiu Gatlan

A malspam car
multiple entiti
NetWiredRC R

Malspam (shor
payloads via m

Hackers didn't waste any time and have ... service launched.

OTROS

El fraude del CEO, un timo millonario silenciado por las propias empresas

OFRECIDO POR ESET

Gettyimages

BrandLab
22/10/2019 - 09:05

Uno de los ciberdelitos más habituales es la suplantación de ... hacen pasar por otra persona para obtener un rendimiento ... directamente económico, de un usuario desprevenido.

hipertextual

SEGURIDAD

El Internet de las Cosas fue usado para el último gran ataque DDoS y no podemos hacer nada para impedirlo

Eduardo Arcos - Oct 13, 2016 - 17:02 (CET)

La situación de falta de seguridad en millones de dispositivos del internet de las cosas es tan grave que ... medio internet no solo es posible, sino ... amente tienen grandes conocimientos

SEGURIDAD

Hackean un casino a través de un termómetro de pecera conectado a Internet

By Jorge Quijije - Abr 16, 2018

ÍNDICE

INCIBE_PTE_AproxEmpresario_017_Turismo_Ocio-2021-v1

Cloud	» Soluciones para la gestión de clientes y recursos: CRM (Gestión de la Relación con Clientes), CRS (Sistema Central de Reservas), PMS (Sistema de Administración de Propiedades) y TPV (Terminal Punto de Venta). » Soluciones de comercio electrónico: web de venta online y pasarelas de pago. » Otras soluciones de alojamiento web y servicios de backup.
IoT *(Internet of Things)*	» Soluciones de comercio electrónico: aplicaciones de reserva online y pagos por móvil. » Soluciones para el control, conocimiento de afluencia y presentación de contenidos. » Soluciones para domotizar alojamientos u otros establecimientos turísticos. » Otras soluciones: pulseras inteligentes.
Big data	» Soluciones de gestión de recursos: RMS (Sistema de Gestión de Ingresos). » Soluciones para toma de decisiones estratégicas o marketing. » Soluciones para la mejora y/o personalización de la experiencia de usuario: motores de búsqueda avanzados, seguimiento, análisis de opiniones y materiales o sistemas de venta basados en realidad virtual.
Inteligencia artificial	» Soluciones de gestión de redes sociales (seguimiento y análisis). » Soluciones de soporte a la experiencia del viajero: asistentes virtuales y *chatbots*.
Infraestructura	» Soluciones para redes internas. » Soluciones para redes wifi (públicas/privadas). » Otras soluciones: portal cautivo.

Tabla 2. *Soluciones tecnológicas más habituales del sector*

Al listado anterior pueden incorporarse las principales tecnologías de ciberseguridad **[REF - 5]** que podrían ser utilizadas por las empresas del sector:

- Auditoría técnica.
- Seguridad en la nube.
- Seguridad en dispositivos móviles.
- Seguridad *e-commerce*.
- Protección *end-point*.
- Protección de las comunicaciones.
- Gestión de incidentes.
- Formación y concienciación.
- Cumplimiento legal.

No obstante, existen diversas herramientas y servicios en el mercado con el objetivo de que las empresas puedan evaluar su nivel de riesgo en ciberseguridad, y de esta forma, comenzar a mejorar su protección. Dentro de estos servicios INCIBE proporciona **la herramienta de autodiagnóstico** [REF - 6], que ofrece un primer punto de partida para conocer el estado actual de ciberseguridad de la organización.

Resumen

Su nivel de seguridad es adecuado pero mejorable. Ya es consciente de que sus empleados son uno de los elementos en los que más tiene que invertir en ciberseguridad y tiene algunas medidas. No obstante, aún le falta hacer un esfuerzo para organizar y controlar mejor algunos aspectos.

44.6%

Este porcentaje está considerado como RIESGO MEDIO

[REF - 6] Herramienta de autodiagnóstico - https://adl.incibe.es/

Herramienta de Autodiagnóstico

Reiniciar

Resumen del diagnóstico

Su nivel de seguridad es adecuado pero mejorable. Ya es consciente de que sus empleados son uno de los elementos en los que más tiene que invertir en ciberseguridad y tiene algunas medidas. No obstante, aún le falta hacer un esfuerzo para organizar y controlar mejor algunos aspectos.

- El Kit de concienciación puede ser muy útil para fortalecer este eslabón de la cadena.
- Aún le queda camino que recorrer para establecer unas políticas adecuadas, le recomendamos que intente establecer un Plan Director de Seguridad.
- Si la web es una parte esencial para su negocio, puede seguir los consejos de la sección Protege tu web.
- En caso de que los dispositivos móviles sean imprescindibles para su actividad, revise el apartado de Protección en movilidad y conexiones inalámbricas.

Ahora que ya conoce el nivel de riesgo de su empresa, ¿quiere conocer el estado de seguridad de sus datos? Puede hacerlo con la herramienta FACILITA de la Agencia Española del Protección de Datos.

¿Qué le ha parecido la Herramienta de Autodiagnóstico? Su opinión nos importa, ayúdenos a mejorarla completando la siguiente Encuesta de Valoración

El resultado de la encuesta concluye que el riesgo en su empresa es:

44.6%

Este porcentaje está considerado como RIESGO MEDIO

Niveles de riesgo

Personas	51.3%	Riesgo MEDIO
Procesos	36.4%	Riesgo MEDIO
Tecnología	46.1%	Riesgo MEDIO

Comparta esta herramienta en las redes sociales

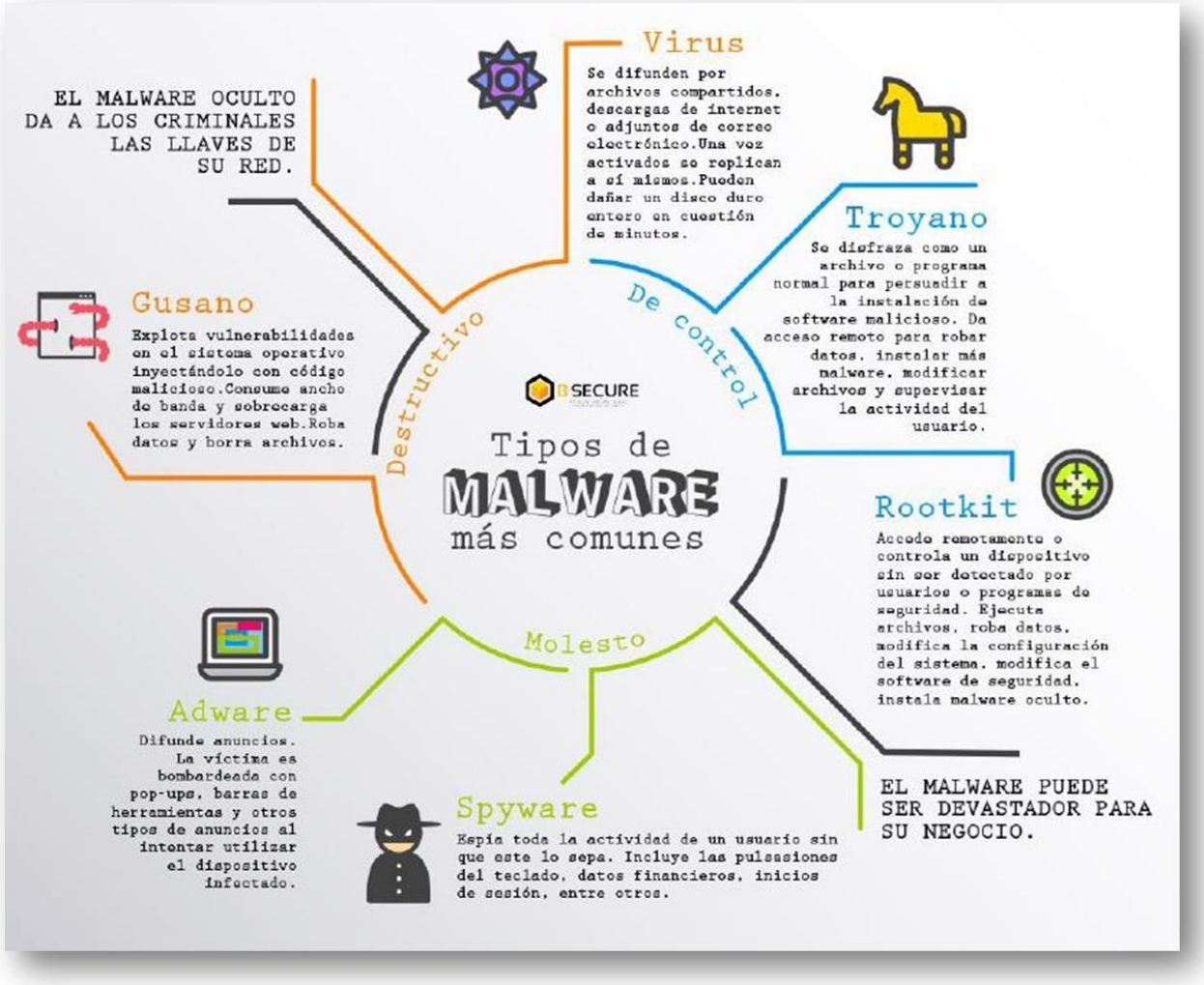
Permita que sus contactos y amigos evalúen los riesgos de seguridad de su negocio en tan solo cinco minutos.

Pulse para descargar el resultado en PDF

incibe_ 017 protege tu empresa SEGITTUR turismo e innovación

3 PRINCIPALES AMENAZAS DE CIBERSEGURIDAD EN EL SECTOR

Ser consciente de las amenazas y conocerlas a fondo es esencial para poder evitarlas, y así proteger nuestros sistemas e información **[REF - 7]**. Ciberataques de *ransomware* y *phishing* o contra la página web, fugas de información, uso de redes inalámbricas o acceso remoto a los sistemas, administración de perfiles en redes sociales o relaciones con proveedores tecnológicos, son solo algunas de las amenazas a las que constantemente están sometidas las empresas de este sector.



GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_

Ilustración 4: Elementos de la Gestión de la Seguridad de la Información

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD 017 protege tu empresa SEGITTUR turismo e innovación

4 MEDIDAS DE CIBERSEGURIDAD PARA EL SECTOR

El sector del turismo y ocio se enfrenta a grandes amenazas en materia de ciberseguridad. Una brecha de seguridad puede ocasionar una pérdida de confianza por parte de los clientes, daño a la reputación de la marca, pérdidas económicas y perjuicios legales. Pese a que estos ataques crecen exponencialmente, muchos de estos riesgos pueden ser evitados o al menos controlados, minimizando así su impacto, si aplicamos ciertas **medidas de ciberseguridad** y, sobre todo, el **sentido común**.

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

LA ESTRATEGIA 3-2-1 DE LAS COPIAS DE SEGURIDAD

Una buena práctica a la hora de realizar copias de seguridad es adoptar la estrategia 3-2-1 que se basa en diversificar las copias de seguridad para garantizar que siempre haya alguna recuperable. Sus **claves de actuación** son las siguientes [12]:

- **3**: Mantener 3 copias de cualquier fichero importante: el archivo original y 2 *backups*.
- **2**: Almacenar las copias en 2 soportes distintos de almacenamiento para protegerlas ante distintos riesgos. Si tuviéramos las dos copias en el mismo tipo de soporte, ambos pueden verse afectados por el mismo fallo de funcionamiento y por tanto poner en peligro las dos copias al mismo tiempo.
- **1**: Almacenar 1 copia de seguridad fuera de nuestra empresa, lo que también se conoce como *backup offsite*. La copia de seguridad en la nube es una clara opción de este tipo de copia.

Estrategia 3-2-1 de copias de seguridad

https://www.osi.es/es


OSI
Oficina de Seguridad del Internauta
¿Quiénes somos? Encuesta de valoración Contacto Boletines
Ponte al día Campañas Protégete Recursos Juegos educativos Iniciativas Ayuda
Buscar
Inicio » Guías de ciberseguridad
Guías de ciberseguridad
SPAM
DESCARGA
Guías de ciberseguridad
Navega seguro por Internet y protege tus dispositivos
Te presentamos una serie de guías para que aprendas a navegar seguro por Internet y a mantener tus dispositivos protegidos. No esperes más y échales un vistazo, evitarás riesgos y te mantendrás a salvo de los ciberdelincuentes, los fraudes y cualquier amenaza de Internet.


TU ROUTER
TU CASTILLO
Guía
Guía para configurar el router wifi
Con esta guía podrás configurar, paso a paso y de manera sencilla, el router de tu casa para mejorar la seguridad de tus conexiones. También aprenderás cuáles son las principales amenazas que pueden afectar a tu router. ¡Configúralo!
Guía de ciberataques
Guía
Guía de ciberataques
Esta guía está dividida en 4 grandes categorías en las que te explicamos hasta 30 tipos de ataques diferentes, como ataques a contraseñas, ataques por ingeniería social, ataques a las conexiones y ataques por malware, ¡conócelos todos!
EL CICLO DE VIDA SEGURO
OSI
DE LOS DISPOSITIVOS MÓVILES
Guía
Guía para configurar dispositivos móviles
Elige la guía que más se adapte a tu dispositivo según su sistema operativo (iOS o Android) y configúralo de manera segura con ayuda de estas 10 fichas. ¡Mantén a salvo toda tu información!
Guía
Aprendiendo a identificar fraudes online
Guía
Guía para aprender a identificar fraudes online
En esta guía repasamos los diferentes tipos de fraudes online que circulan por la Red. Te enseñamos cómo evitarlos y qué hacer si resultas víctima de alguno de ellos. ¡Que no te engañen!
PRIVACIDAD Y SEGURIDAD EN INTERNET
Guía
Guía de privacidad y seguridad en Internet
Esta guía recoge los principales riesgos a los que te expones al navegar por Internet y te explica las principales medidas de protección que debes aplicar para evitarlos. ¡Protégete!
Compra segura en INTERNET
GUÍA PRÁCTICA
Guía
Compra segura en Internet
Con esta guía aprenderás a realizar compras online de una manera mucho más segura. Sigue nuestros 10 consejos, descubre en qué te tienes que fijar para que no te engañen con "chollos". ¡Infórmate!

OSI Oficina de Seguridad del Internauta

¿Quiénes somos? Encuesta de valoración Contacto Boletines

Ponte al día Campañas Protégete Recursos Juegos educativos Iniciativas Ayuda

Buscar

Inicio » Recursos » Guías » Guía de privacidad y seguridad en Internet

Guía de privacidad y seguridad en Internet

¿Sabes por qué es tan importante tener contraseñas robustas? ¿Y de hacer copias de seguridad? ¿Te gustaría obtener unos consejos para comprar en línea o sobre cómo evitar los programas maliciosos? Pues has aterrizado en la página correcta. Te presentamos la guía de "Privacidad y seguridad en Internet" que la Agencia Española de Protección de Datos (AEPD) y la OSI hemos desarrollado para ti.

La guía está formada por 18 fichas que recogen los principales riesgos a los que nos exponemos al hacer uso de Internet así como las medidas de protección que debemos aplicar para evitarlos. En concreto, cada ficha plantea una situación que podría ocurrir a cualquier usuario que haga uso de dispositivos electrónicos y se conecte a Internet, con el objetivo de hacer reflexionar a éste sobre la problemática de hacer o no hacer una determinada acción. A continuación, se expone información general sobre la temática abordada. Finalmente, cada ficha facilita una serie de consejos y recomendaciones que ayudarán a evitar los riesgos planteados y mantenerse protegido.

DESCARGAR GUÍA

Además de las 18 fichas, hemos desarrollado varios videotutoriales que te permitirán configurar las opciones de privacidad de las principales redes sociales y aplicaciones de mensajería instantánea. En concreto para Facebook, Twitter, Instagram, Youtube, Whatsapp y Snapchat. ¡No te los pierdas!

Privacidad en Facebook

Ver videotutorial

Privacidad en Twitter

Ver videotutorial

Privacidad en Instagram

Ver videotutorial

Privacidad en Youtube

Ver videotutorial

Privacidad en Whatsapp

Ver videotutorial

Privacidad en Snapchat

Ver videotutorial

Si lo deseas, puedes descargar las distintas fichas de las que se compone la guía de manera individual. Elije la temática que más te interese, descárgate la ficha y sé el primero en compartirla con tus contactos.

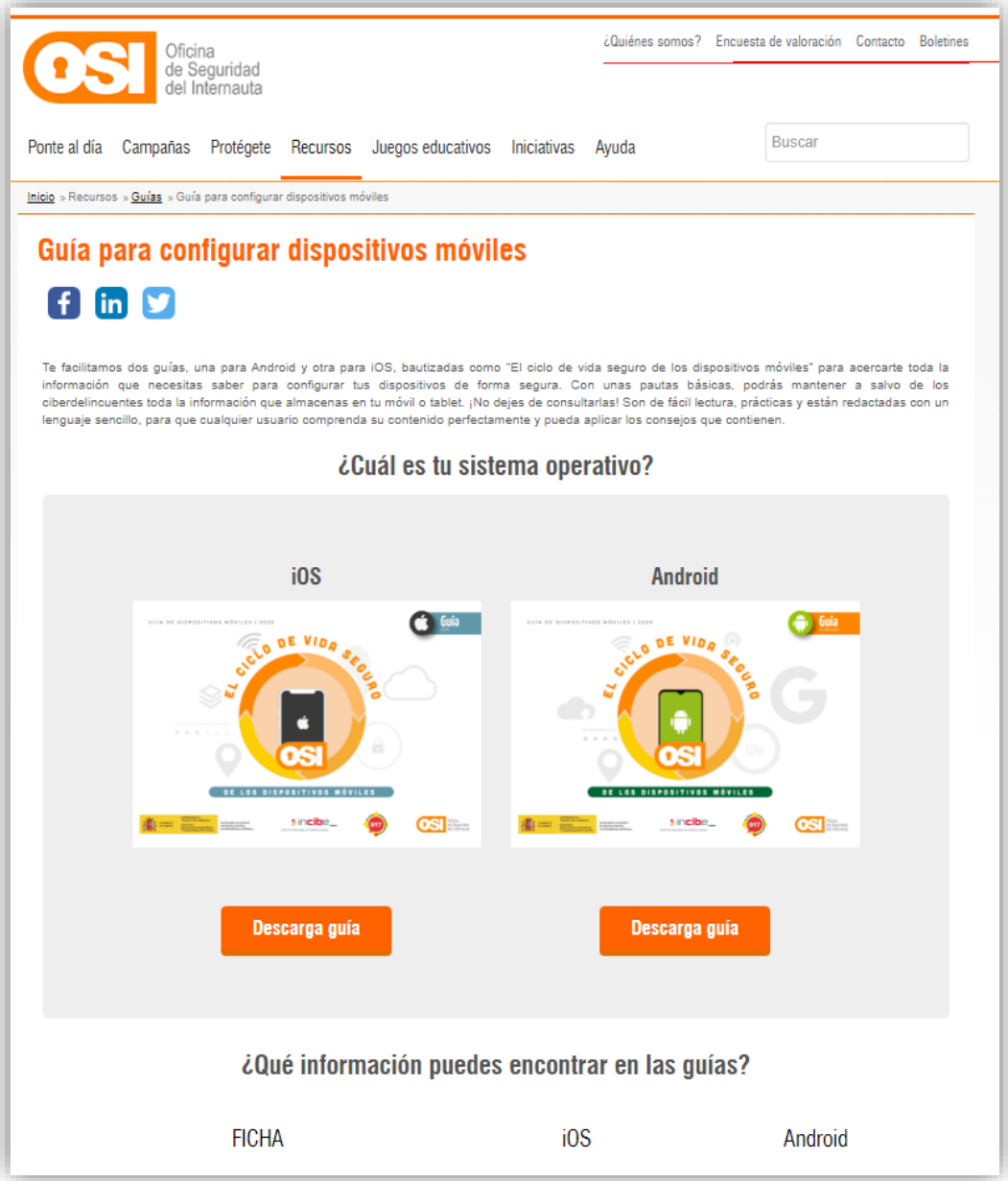
- FICHA 1: Tus dispositivos almacenan mucha información privada ¿Te habías parado a pensarlo?
- FICHA 2: ¿Por qué son tan importantes las contraseñas?
- FICHA 3: ¿Son suficientes las contraseñas?
- FICHA 4: No esperes a tener un problema para realizar copias de seguridad
- FICHA 5: ¿Será fiable esta página?
- FICHA 6: ¿Tengo obligación de dar mis datos cuando me los piden?
- FICHA 7: ¿Cómo puedo eliminar datos personales que aparecen en los resultados de un buscador?
- FICHA 8: ¿Cómo puedo usar el navegador para que no almacene todos los pasos que doy por Internet?
- FICHA 9: ¿Quién puede ver lo que publico en una red social?
- FICHA 10: Identificando timos y otros riesgos en servicios de mensajería instantánea
- FICHA 11: Toda la información que se publica en Internet ¿es cierta?
- FICHA 12: Phishing: el fraude que intenta robar nuestros datos personales y bancarios
- FICHA 13: ¡Qué le pasa a mi conexión de Internet!
- FICHA 14: Quiero proteger mi correo electrónico
- FICHA 15: ¿Qué tengo que tener en cuenta si guardo mi información personal en la nube?
- FICHA 16: ¿Puedo compartir ficheros por Internet de forma segura?
- FICHA 17: No tengo claro para qué está utilizando mi hijo Internet, ¿qué puedo hacer?
- FICHA 18: ¿Las pulseras y relojes que miden la actividad física son seguros?

Tanto la AEPD como la OSI esperamos que esta iniciativa sea de utilidad a todos los usuarios de Internet y permita un acercamiento práctico a los contenidos desarrollados con el fin último de capacitar, prevenir y ayudar en el uso seguro y responsable de Internet.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

OSI Oficina de Seguridad del Internauta

Además de las 18 fichas, hemos desarrollado varios videotutoriales que te permitirán configurar las opciones de privacidad de las principales redes sociales y aplicaciones de mensajería instantánea. En concreto para Facebook, Twitter, Instagram, Youtube, Whatsapp y Snapchat. ¡No te los pierdas!


Oficina de Seguridad del Internauta
¿Quiénes somos? Encuesta de valoración Contacto Boletines
Ponte al día Campañas Protégete Recursos Juegos educativos Iniciativas Ayuda
Buscar
Inicio » Recursos » Guías » Guía para configurar dispositivos móviles
Guía para configurar dispositivos móviles
Te facilitamos dos guías, una para Android y otra para iOS, bautizadas como "El ciclo de vida seguro de los dispositivos móviles" para acercarte toda la información que necesitas saber para configurar tus dispositivos de forma segura. Con unas pautas básicas, podrás mantener a salvo de los ciberdelincuentes toda la información que almacenas en tu móvil o tablet. ¡No dejes de consultarlas! Son de fácil lectura, prácticas y están redactadas con un lenguaje sencillo, para que cualquier usuario comprenda su contenido perfectamente y pueda aplicar los consejos que contienen.
¿Cuál es tu sistema operativo?
iOS
Android
Descarga guía
Descarga guía
¿Qué información puedes encontrar en las guías?
FICHA
iOS
Android


FICHA
iOS
Android
1. Móvil nuevo en la mano, ¿y ahora qué?
Elige un idioma | Conéctate a una red wifi | Vincula tu cuenta de Google | Actualiza el software
2. ¡Qué nadie lo use sin tu permiso!
Establece contraseñas seguras | Doble factor de autenticación
3. Conexiones siempre seguras
Configuraciones de redes inalámbricas
4. Protección contra virus y fraudes
Antivirus | Actualización de software
5. ¡No pierdas tu información y protégela!
Copias de seguridad | Cifrado
6. Personalización - ¡Hazlo tuyo!
Instalación de apps desde Play Store | Permisos de apps | Geolocalización
7. ¡Localiza tu dispositivo!
Desde web
8. Ya pasará a otra vida - Deshacernos del móvil
Borrado seguro
9. Consejos generales

PRIMEROS PASOS PARA MEJORAR LA SEGURIDAD

9 CONSEJOS GENERALES

1. Vincula tu dispositivo móvil a una cuenta Google en tu móvil Android.
2. Utiliza una clave de bloqueo para tu dispositivo. Si no es biométrica, recuerda usar una contraseña robusta.
3. Activa el sistema de actualizaciones automáticas de tu dispositivo y aplicaciones, pues con esto se corrigen los defectos en seguridad que puedan tener.
4. Usa aplicaciones de seguridad que añadan una capa extra de seguridad a tu dispositivo, como por ejemplo un antivirus.
5. Protege tu información mediante copias de seguridad. De este modo tendrás una copia de respaldo en caso de pérdida o borrado de tu dispositivo.

6. Desactiva las conexiones inalámbricas una vez hayas terminado de usarlas (wifi, Bluetooth, NFC).
7. Cuando instales aplicaciones, revisa siempre quién es el desarrollador así como las opiniones y valoraciones del resto de usuarios. ¡Y acuérdate de eliminar las que ya no uses!

Google Play

8. Otorga los permisos a las apps que sean imprescindibles para su correcto funcionamiento y revisa siempre que sean coherentes con la funcionalidad de la app.
9. Evita prácticas de riesgo con el rooting en Android.
10. Si vas a deshacerte de tu móvil, asegúrate de borrar toda la información que contiene para no dejar rastro.
11. Apóyate en herramientas de control parental si el dispositivo lo va a utilizar un menor.

18+

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · 017 · OSI Oficina de Seguridad del Internauta

GUÍA DE DISPOSITIVOS MÓVILES | 11/12

FIREWALL HUMANO

Contacto

ivigo.es

info@ivigo.es

Pontevedra 09/06/2022

https://ivigo.es/ciberseguridad-en-el-sector-turismo-y-ocio-nodo-cibergal/