

Perfiles de alto impacto en apuros:

Protección de la identidad
digital corporativa y
personal.
Cómo mitigar riesgos.





KINDLY REMINDER

El contenido de este documento es confidencial y está sometido a secreto profesional. onBRANDING, BRAND CARE y CELEBrandSEC tienen registrados todos sus contenidos y metodologías en el Registro de la Propiedad Intelectual archivo: B-3017-15.



EQUIPO



Coordinadora del proyecto, Selva Orejón

Perito judicial especializada en Identidad y Reputación digital y Ciberinvestigación. Licenciada en Ciencias de la Comunicación por la Universitat Ramon Llull, Diplomada en Business Organization and Environment, University of Cambridge y Diplomada en Inteligencia al Servicio del Estado y la Empresa. Profesora en la Universidad de Barcelona UB en el Máster de Ciberseguridad, impartiendo Ciberinteligencia – OSINT, y en la Escuela de Policía de Catalunya, (Ciberinvestigación y Protección de la identidad digital).





Cuidar la IDENTIDAD DIGITAL minimiza los riesgos de sufrir un CIBERATAQUE y una crisis de PRIVACIDAD, SEGURIDAD y su consecuencia en REPUTACIÓN.



¿QUÉ VEREMOS?



LA IMPORTANCIA
PROTEGER LA
IDENTIDAD
DIGITAL



CASOS EN
COVID-19



AUMENTO DEL CIBERCRIMEN



Los ataques cibernéticos a la privacidad personal y corporativa encabezan la lista de preocupaciones.

Robo - daño de secretos y propiedad intelectual

Fraudes en línea

Robo y suplantación de identidad

El coste de estos ciberdelitos suma 1 billón de dólares, Y podría triplicarse.





RIESGOS Y CONSECUENCIAS

**INTEGRIDAD PERSONAL
/
ENTORNO**

**REPUTACIÓN PERSONAL
/
ENTORNO**

**REPUTACIÓN PROFESIONAL
PROPIA**

**REPUTACIÓN PROFESIONAL DEL
ENTORNO**



ATAQUE DIRIGIDO A PERFIL DE ALTO IMPACTO

VÍA DE ENTRADA con un mínimo común: **FALTA DE SEGURIDAD / PRIVACIDAD**

1) DISPOSITIVOS



- Navegar y chatear con las cámaras destapadas
- No contar con una solución de seguridad en PC, móviles y tabletas

2) COMUNICACIONES



- Navegar con WIFI abiertas
- Compartir redes, bluetooth...
- Contraseña del router por defecto
- Navegar sin VPN

3) COMPORTAMIENTO HUMANO



- EXTIMIDAD** (deseada o no)
- Pseudo confianza: hablar de más
 - Falsas creencias (Apple)
 - No tengo nada que esconder
 - Comparto mis sesiones
 - No cambio contraseñas, ni 2FV



COVID-19 ATTACKS





LOS CUERPOS POLICIALES ALERTAN



ATAQUE ALEATORIO

 **Policía Nacional** @policia · 1h

Este #phishing suplantando a la DGT está circulando...
#NoPiques
Si tienes dudas  dirígete a la fuente oficial para comprobar.

#EsteVirusLoParamosUnidos

PAGA TU MULTA

[Sede Electrónica-sede.dgt.gob.es](https://sede.dgt.gob.es)



Ver en el navegador

Pago de sanciones:

Detectamos en nuestro sistema un registro de multa de tránsito no pagada. Debido a que usted no se notificó en el tribunal de faltas correspondiente le Reenviamos las Foto-multas vía internet.

4 84 87



Alertas de ataques durante la crisis del COVID-19:

 **Guardia Civil**   @guardiacivil · 8h

Los [#ciberdelincuentes](#) aprovechan la crisis del [#COVID19](#) para buscar víctimas. ¿Puedes ayudar a la [@guardiacivil](#) a identificarlos? ¡Colabora! 🌟

[#ciberestafas](#) y [#ciberfraudes](#)
ciberestafas@guardiacivil.org

[#ciberincidentes](#) graves
ciberataques@guardiacivil.org



 11  212  328 



Alertas de ataques durante la crisis del COVID-19:

 **Guardia Civil**   @guardiacivil · 23h

Los **#ciberdelinquentes** aprovechan la crisis actual para llevar a cabo sus **#estafas** y **#fraudes** online.

+  **@osiseguridad** ha creado una lista con los más relevantes: Top 10 fraudes que utilizan el **#COVID-19** para engañar.
 bit.ly/2wGLcRi



 4  117  190 



Alertas de ataques durante la crisis del COVID-19:



Guardia Civil 🇪🇸 @guardiacivil · 27 mar.

🚨 Detectadas aplicaciones maliciosas que aseguran facilitar un mapa para seguir la evolución del #COVID19. La difusión se realiza a través mensajes que contienen un link de descarga. #NoPiques

 + @osiseguridad 📢
bit.ly/39ISgzY
#EsteVirusLoParamosUnidos



4 254 261



Alertas de ataques durante la crisis del COVID-19:

mos SOS Mossos @mossos · 6h

Els casos de #phishing i #ransomware són dos dels ciberdelictes que més han augmentat aquests dies. Aquí t'expliquem en què consisteixen #coronavirus 🦠

Què és el RAMSONWARE?
Segrest de dades que s'obté a partir de la instal·lació d'un programa maliciós que restringeix l'accés total o parcial a les nostres dades i pel qual els ciberdelinqüents demanen un rescat econòmic

Què és el PHISHING?
Engany que consisteix en fer-se passar per empreses, persones de confiança o organitzacions i provocar que es realitzin accions com proporcionar dades o informació de caràcter confidencial

112 mossos d'esquadra Govern de Catalunya Departament d'Interior

1 38 45



Alertas de ataques durante la crisis del COVID-19:

mos sos Mossos @mossos · 8h

Sabies que durant el confinament hem detectat un augment dels delictes per internet? Pren mesures de seguretat i segueix aquests consells
[#coronavirus](#) bit.ly/2UrgDYN

ULL AMB LES CIBER ESTAFES!

No obriu **enllaços** de correu, ni missatgeria electrònica amb informació sobre el COVID-19 amb arxius adjunts

No obriu **enllaços** inesperats a webs o documents relacionats amb el COVID-19 amb arxius adjunts

No descarregueu **programari** ni aplicacions no oficials amb informació de l'abast del COVID-19



SI POU REGISTREU: EXAMINEU LES RECOMANACIONS DE SEGURETAT DE LA VOSTRA EMPRESA

SI TENEU DUBTES CONSULTA AMB LA NOSTRA BRUITA A MOSSOS CIBERSEGURETAT@MOSSOS.CAT

112 mossos d'esquadra  Generalitat de Catalunya Departament d'Interior

4 66 76



Alertas de ataques durante la crisis del COVID-19:

 **Mossos** @mossos · 26 mar.

⚠️ Si aquests dies reps un correu relacionat amb una compra en línia que no has fet i per anul·lar-la et demanen les dades de la teva targeta bancària, no ho facis. Es tracta d'una estafa #Nopiquis



Obtén ayuda con suscripciones y compras. [Visita la página de Cancelar y gestionar compra](#)

Obtén información sobre cómo [administrar las preferencias de tu contraseña](#)

para compras hechas en iTunes, Apple Books y App Store.

Resumen del Apple ID · Condiciones de venta · Política de privacidad

Copyright © 2020 Apple Inc.
Todos los derechos reservados

1 146 137



Alertas de ataques durante la crisis del COVID-19:

 **Mossos** @mossos · 25 mar.

⚠ Detectem anuncis falsos en portals en línia de material de protecció contra el #coronavirus. Uiii Són estafes o t'adrecen a webs malicioses. Recorda que tens el portal bit.ly/3ajVvJE per resoldre dubtes.

MASCARILLAS DE TRES CAPAS

Est. 3000000000 OFFERTA - Útils en billao 100

Mascarillas 3 capas tipo de 50 unidades

COMPRALO CON GARANTIA



MASCARILLAS FARMACÉUTICAS PREVENCIÓN COV

Ref. 344510701 OFFERTA - Útils en billao 100

Mascarillas profesionales homologadas. Caja (de 100 unidades) 100€ (Me quedan 215 cajas). Envío expreso por DHL 1-2 días. contacta por whatsapp al 607...

COMPRALO CON GARANTIA





ATAQUES



Casos de ataques a la SEGURIDAD:

Un 'ransomware' que perseguía datos de pacientes, responsable del ciberataque contra el sistema hospitalario español

El ataque en cuestión ha sido bautizado como Netwalker por los expertos.

<https://www.elboletin.com/noticia/186130/tecnologia/un-ransomware-que-perseguia-datos-de-pacientes-responsable-del-ciberataque-contra-el-sistema-hospitalario-espanol.html>



Hackerazzi

Los altos directivos tienen hasta 12 veces más posibilidades de ser víctimas de un ciberataque que cualquier otro trabajador



Hackerazzi

Jugador de la NBA compartió video explícito en Instagram; asegura que lo hackearon



Hackerazzi

Bella Thorne publica sus fotos íntimas tras ser 'hackeada'

"Durante las últimas 24 horas he estado siendo amenazada con mis propios desnudos. Me siento sucia, me siento observada, siento que alguien me ha quitado algo que solo quería que viera una persona especial". Con estas palabras la actriz Bella Thorne denunciaba en un comunicado publicado en su cuenta de Twitter el *hackeo* de fotos sexuales del que ha sido víctima.

La exchica Disney acompañaba un tuit en el que podía leerse "Que te jodan a ti y al poder que crees que tienes sobre mí" con varias de las imágenes que habían sido robadas de su teléfono móvil y en las que posa desnuda de cintura para arriba.

La actriz, modelo y cantante de 21 años, además, publicó las capturas de pantalla de conversaciones con el presunto hacker, quien dijo que tenía fotos y videos de ella.



Hackerazzi

Miguel Bosé denuncia un intento de extorsión con unas fotos de sus hijos

Para evitar extorsión, Miguel Bosé revela la identidad de sus hijos

El propio artista difundió anoche la primera imagen frontal de sus hijos para, según sus propias palabras, 'interrumpirle el negocio' a su agresor



Revelación de SECRETO

La Fiscalía pide 4 años de cárcel para un guardia civil por consultar archivos sin permisos para "espíar" a su exmujer

• La Fiscalía Provincial de Madrid solicita cuatro años de prisión para un guardia civil por presunto delito de revelación de secretos al sostener que consultó archivos sin autorización para "espíar" a su exmujer.

<https://www.lavanguardia.com/local/madrid/20200207/473324532940/la-fiscalia-pide-4-anos-de-carcel-para-un-guardia-civil-por-consultar-archivos-sin-permisos-para-espíar-a-su-exmujer.html>



ATAQUES DURANTE EL COVID-19



COVID-19

La crisis del Covid
Los problemas de
privacidad y seguridad
sacuden el éxito de
Zoom

Los problemas de privacidad y seguridad de
Zoom empañan el éxito de esta aplicación
durante la crisis del Covid 19



COVID-19

Los Mossos alertan del peligro de dos aplicaciones de videoconferencias: Jitsi y Zoom

Jitsi Meet permite que desconocidos se cuelen en tus llamadas, al igual que Zoom

Coronavirus: Los Mossos se equivocan alertando sobre la plataforma de videoconferencia Jitsi

La policía autonómica se refería a un sistema operativo que no funciona desde hace tres años



COVID-19

Vulnerabilidad de acceso a reuniones sin autenticación en Cisco Webex

Fallo en Cisco WebEx permitiría el acceso a reuniones privadas

Se ha hecho publico un fallo de seguridad en Cisco WebEx que podría permitir que un atacante remoto no autenticado ingresase en una reunión de videoconferencia protegida con contraseña. El problema se debe a la exposición involuntaria de información de la reunión en un flujo de unión a la reunión que es específico para aplicaciones móviles. Por tanto los únicos requisitos para poder aprovechar la vulnerabilidad son conocer la ID o URL de la reunión y disponer de la aplicación WebEx para los sistemas móviles IOS o Android.



COVID-19

iPhone: Alertan de un importante fallo de seguridad en su app de correo electrónico

Se trata de una vulnerabilidad que afecta a iPhone y iPads con sistema operativo IOS 6.0 o superior, incluyendo la versión más reciente, según la empresa de ciberseguridad ZecOps



COVID-19

Roban los datos de miles de usuarios de HouseParty pero la empresa niega el 'hacking'

Miles de usuarios denuncian robos, problemas en sus cuentas de plataformas como Spotify o Netflix y cambios en sus perfiles. En principio, todo vendría de la 'app' más famosa del momento





CELEBRANDSEC


Ataques a la REPUTACIÓN de MARCAS y PERSONAS



Ataque a la REPUTACIÓN

Mariah Carey terminó el año con su cuenta de Twitter *hackeada*. Adam Sandler ha comenzado el 2020 de la misma manera. Pero no son los únicos. Incluso el propio CEO de esta red social, Jack Dorsey, se ha visto afectado. El grupo de piratas informáticos Chuckling Squad ha conseguido acceder a todas estas cuentas para publicar en nombre de sus usuarios comentarios racistas o insultos contra otras celebridades conocidas.



Mariah Carey 
@MariahCarey

Eminem has a little penis

7:25 · 01 Jan 20 · [Twitter Web App](#)

8,592 Retweets **14.6K** Likes

<https://elpais.com/elpais/2020/01/03/gente/15780442...>



Crisis de REPUTACIÓN

Hackean la cuenta del presidente y fundador de Twitter

Varios mensajes de contenido racista y violento han permanecido en la cuenta del directivo durante 20 minutos hasta que han sido eliminados.



Crisis de REPUTACIÓN

Facebook reconoce el robo de datos de 30 millones de usuarios

Los ciberdelincuentes controlaron unas 400.000 cuentas a través de una "vulnerabilidad" en el código de la plataforma que afectó al modo 'Ver como'

Facebook ha reconocido en una **nota** que el **ataque informático** que hace dos semanas fue descubierto por los ingenieros de la compañía ha comprometido información de **30 millones de usuarios**, sobre todo datos personales y de contacto.

Inicialmente, la compañía pensó que la brecha de seguridad en su sistema había afectado a 50 millones de usuarios. Según **Facebook**, los piratas informáticos explotaron una "**vulnerabilidad**" en el **código** de la plataforma que afectaba al **modo 'Ver como'** -una herramienta que permite a los usuarios ver su perfil como si fuesen otras personas- de unas 400.000 cuentas, y desde ahí alcanzaron a 30 millones de usuarios.





CELEBRANDSEC

RECOMENDACIONES GENERALES



RECOMENDACIONES GENERALES

PENSAR EN NUESTRA CIBERSEGURIDAD EN 3 PARTES

1) DISPOSITIVOS



- Navegar y chatear con las cámaras TAPADAS
- Antivirus en TODOS los dispositivos
- FILTRO de privacidad física

2) COMUNICACIONES



- Navegar con WIFI CERRADAS
- NO usar el nombre ni PASS por defecto en nombre y ROUTER
- NO Compartir redes, bluetooth...
- Navegar con VPN

3) COMPORTAMIENTO HUMANO



EXTIMIDAD (deseada o no)

- Pseudo confianza: no hablar no postear de más
- Sí tienes algo que esconder
- NO comparto mis sesiones
- Cambia las contraseñas
- Activa las 2FV





PRÓXIMOS PASOS

Equipo profesional transversal y especializado en **ejercer de catalizador de todos los servicios aportando una visión, acompañamiento y solución** que aporta ayuda a departamentos o profesionales para velar y coordinar desde un nivel superior la protección de la identidad digital.



**MONITORIZACIÓN /
AUDIT DE IDENTIDAD DIGITAL**
Qué se dice de nosotros



**VALORACIÓN DEL RIESGO /
CRISIS**
Anticiparse a las crisis



POSICIONAMIENTO
Aumentar la visibilidad



**CONTROL DEL CONTENIDO
ELIMINACIÓN, DESINDEXACIÓN
Y DESPOSICIONAMIENTO**
Imponer nuestro relato



QUEDAMOS A SU DISPOSICIÓN



<https://www.facebook.com/onbranding>



<https://www.linkedin.com/company/onbranding/>



<https://twitter.com/onbranding>



<https://www.youtube.com/channel/UCTXIZD4o3JyAXGSA48rlemA>

