Recursos de interés

Kit seguridad digital para empresarios y profesionales

Yolanda Corral

Periodista y formadora especializada en ciberseguridad de tú a tú y competencias digitales

¿qué puedo hacer por ti?

www.yolandacorral.com

@yocomu in/yolandacorralm YouTube Palabra de hacker

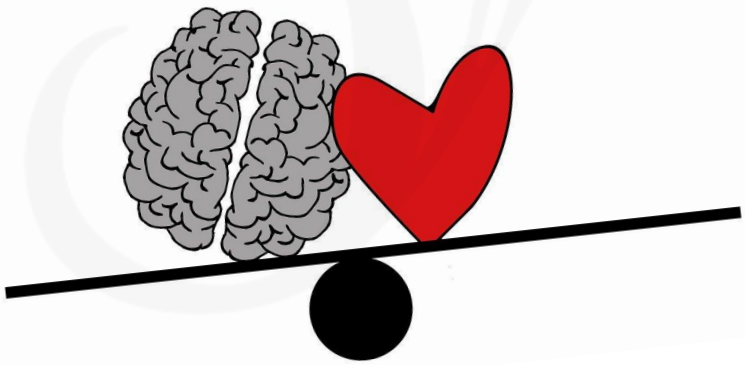
¿Qué es la seguridad digital?

Todo lo queda en manos del usuario a diferencia de la seguridad informática que implica años de desarrollo así que si está en tus manos NO te puedes quedar sin hacer nada.

El uso seguro y responsable de las Tecnologías de la Información y la Comunicación (TIC) comienza por ti.

¿Por dónde empiezo?

Aquí tienes una serie de enlaces de interés y recursos que pueden ayudarte a aprender a cuidar más tu propia seguridad digital y en la empresa.



La tecnología es muy poderosa.
Si aplicamos medidas de ciberseguridad e higiene digital, aprendemos a identificar riesgos y amenazas en la red, hacemos un uso seguro y responsable de Internet y no perdemos nunca de vista el sentido común, las oportunidades en la red se multiplican.

Buenas prácticas de seguridad digital para todos

- Mantener los sistemas operativos y todos los dispositivos actualizados.
- Buena política de copias de seguridad de los archivos e información de manera periódica, mejor diaria que semanal.
- Uso de software oficial, descargas en sitios oficiales y supervisión para que los empleados no usen servicios, herramientas, apps en la nube no autorizados ni controlados.
- Poner contraseñas robustas y diferentes para cada servicio.

Vídeo "Cómo generar contraseñas seguras":

https://youtu.be/l0nnL4xr3k0

- Tapar la webcam de los diferentes dispositivos conectados a Internet.
- Instalar un antivirus y otras herramientas anti-malware.
- Activar el doble factor de autenticación (**2FA**) en todas las cuentas en las que esté habilitado como Google, Twitter, Facebook, LinkedIn, Instagram, Dropbox, PayPal, Amazon… Usar aplicación 2FA (Google Authenticator, Authy, Microsoft Authenticator…), código por SMS o llave de seguridad.
- Cambiar el usuario y contraseña del router, no dejar la configuración como viene por defecto. Ocurre lo mismo con las cámaras IP.

Buenas prácticas de seguridad digital para todos

- Usar el cifrado para proteger archivos importantes y datos confidenciales.

- Revisar siempre las configuraciones de seguridad y privacidad de todas las cuentas y redes sociales, no dejarlas nunca configuradas por defecto.

Mi cuenta - Google:

https://myaccount.google.com

Centro de seguridad de Google:

https://www.google.com/intl/es-419/safetycente

- Tener anotado en un lugar seguro el **código IMEI** de cada dispositivo móvil pues es el número identificador del mismo y en caso de extravío o robo será necesario. ¿Cómo averiguar el IMEI del dispositivo móvil?

Marca

***#06#**

Buenas prácticas de seguridad digital para todos

- WiFi, GPS, Bluetooth, NFC, conviene desactivarlos cuando no se usen.
- No conectar USB desconocidos en los ordenadores ni cargar los dispositivos en USB públicos. Salvo que se utilice un cable solo de carga o un escudo USB para proteger de fuga de datos o infecciones, realizar la carga mediante el enchufe o cargar con baterías externas.
- Evitar conectarse a redes WiFi públicas si no es usando UVP pues tengan o no tengan contraseña ya que son inseguras.

Listado de herramientas y servicios de utilidad:

- **Gestores de contraseñas**:
  - **KeePass:** http://keepass.info
  - **LastPass:** https://www.lastpass.com
  - **Bitwarden:** https://bitwarden.com
  - **Dashlane:** https://www.dashlane.com
  - **1password:** https://1password.com/es
  - **Keeper:** https://www.keepersecurity.com/es_ES

- **Herramientas de cifrado**:
  - Cifrado para Windows, Mac y Linux.
    - **VeraCript:** https://www.veracrypt.fr
  - Cifrado de memorias USB:
    - **SecurStick:** https://www.withopf.com
    - **Rohos Mini Drive:** https://www.rohos.com
  - Cifrado de archivos en la nube:
    - **Boxcryptor:** https://www.boxcryptor.com/es/
    - **Cryptomator:** https://cryptomator.org

- **Consulta y borrado de metadatos**:
  - **Ver Exif:** https://www.verexif.com
  - Photo Exif Editor aplicación que permite cambiar metadatos.

Listado de herramientas y servicios de utilidad:

- Ante enlaces sospechosos o URLs acortadas, archivos o aplicaciones de origen desconocido, usar herramientas para hacer un escaneo previo y comprobar la reputación de las mismas:
    - **VirusTotal:** https://www.virustotal.com
    - **MetaDefender**: https://metadefender.opswat.com
    - **URLVoid:** https://www.urlvoid.com
    - **Urlex:** https://urlex.org

- Comprobar la seguridad de los códigos QR:
    - **Kaspersky QR Scanner:** https://www.kaspersky.es/qr-scanner
    - **RevealQR**: https://revealqr.app

- Comprobar si un sitio web es fraudulento, una web fake:
    - **Desenmascarame:** http://desenmascara.me

¿Tu correo o teléfono está expuesto?

¿Tu contraseña está comprometida?

https://haveibeenpwned.com

Listado de herramientas y servicios de utilidad:

- **Catálogo de herramientas gratuitas en la web de OSI**: acceso remoto, anti robo, cortafuegos, cifrados y gestores de contraseñas, privacidad y navegación, control parental, copias de seguridad, gestor de tareas, mantenimiento y limpieza, antivirus, análisis online y cleaners, análisis de tráfico: **https://www.osi.es/es/herramientas**

- **Servicio Antibotnet de OSI** para comprobar si tu conexión a Internet, la dirección IP, forma parte de una botnet: **https://www.osi.es/es/servicio-antibotnet**

- **CONAN Mobile** aplicación gratuita para comprobar el estado de seguridad de los dispositivos móviles: **https://www.osi.es/es/conan-mobile**

- **ESET**, descarga de utilidades, herramientas de desinfección de diversos ransomware y muestras: **http://descargas.eset.es/utilidades**

- **Shophos**, herramientas gratuitas: **https://www.sophos.com/es-es/products/free-tools.aspx**

- **Malwarabytes**, herramienta anti-malware: **https://es.malwarebytes.com**

- **Latch**, aplicación gratuita que funciona como interruptor de la vida digital para mantener cerrada la sesión en diferentes cuentas y servicios de Internet: **https://latch.elevenpaths.com**

Canales oficiales de información sobre seguridad en Internet

INCIBE, Instituto Nacional de Ciberseguridad: https://www.incibe.es

- Twitter: @INCIBE
- Instagram: @INCIBE
- Facebook: https://www.facebook.com/protegetuempresa
- LinkedIn: https://www.linkedin.com/company/incibe
- YouTube: https://www.youtube.com/c/INCIBE

OSI, Oficina de Seguridad del Internauta: https://www.osi.es/es

- Avisos de seguridad, listado: https://www.osi.es/es/actualidad/avisos
- Twitter: @osiseguridad
- Facebook: https://www.facebook.com/osiseguridad
- YouTube: https://www.youtube.com/user/OSIseguridad

IS4K, Internet Segura for Kids centro de referencia a nivel nacional en seguridad para menores de edad: https://www.is4k.es

- Twitter: @is4k
- Facebook: https://www.facebook.com/is4k.es
- YouTube: https://www.youtube.com/channel/UCBoX1urZFEt29_5XqB_5BTg

Canales oficiales de información sobre seguridad en Internet

INCIBE-CERT, Centro de Respuesta a Incidentes de Seguridad.

https://www.incibe-cert.es

Centro de referencia para los ciudadanos y entidades de derecho privado en España. Organismo que se encarga de la gestión de incidentes de seguridad y fraude electrónico con un canal 24/7 para ciudadanos y empresas a nivel nacional.

- Correo respuesta a incidentes ciudadanos y empresas: incidencias@incibe-cert.es
- Correo respuesta a incidentes instituciones afiliadas a la red académica y de investigación española (RedIRIS): iris@incibe-cert.es
- Correo respuesta a incidentes operadores estratégicos y de infraestructuras críticas: pic@incibe-cert.es
- Proveedores de servicios digitales: incidencias@incibe-cert.es

CSIRT-CV, Centro de Seguridad TIC de la Comunitat Valenciana.

https://www.csirtcv.gva.es

- Twitter: @csirtcv
- Facebook: http://www.facebook.com/csirtcv
- Informar de un incidente: https://www.csirtcv.gva.es/es/formulario/informar-de-un-incidente.html
- Informar de un phishing: https://www.csirtcv.gva.es/informar-de-un-phishing

Canales oficiales de información sobre seguridad en Internet

AEPD, Agencia Española de Protección de Datos:

https://www.aepd.es

- Twitter: @AEPD_es
- YouTube: https://www.youtube.com/channel/UCdKb1SWpT_D0bdqd-9BwLBw
- **Canal prioritario** para comunicar la difusión de contenido sensible y solicitar su retirada: https://www.aepd.es/canalprioritario

900 116 117 **@INCIBE017**

017, Línea de ayuda de ciberseguridad de INCIBE: línea telefónica gratuita puesta a disposición de ciudadanos, empresas, padres, menores y educadores para atender consultas e incidentes relacionados con ciberseguridad.

Kit de difusión línea 017 para centros escolares y empresas:
https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/kit-difusion

Policía 091
@policia

Denunciar delitos ↓

Guardia Civil 062
@guardiacivil

Denunciar delitos ↓

ALERTCOPS. Aplicación gratuita de seguridad ciudadana para dispositivos móviles (Android e iOS) para comunicar delitos o situaciones de riesgo (incluido el acoso escolar) a Policía y Guardia Civil.

Dispone de un **botón SOS** para alertas instantáneas con ubicación y la posibilidad de activar la función **Guardián** con hasta cinco personas.

Phishing ¿Sabrías detectar si te están engañando?

Test online de creado por Google

https://phishingquiz.withgoogle.com

¿Quieres reportar un phishing o fraude electrónico?

Correo INCIBE:

incidencias@incibe-cert.es

Formulario CSIRT-CV:

https://www.csirtcv.gva.es/informar-de-un-phishing

Guardia Civil:

ciberestafas@guardiacivil.org

Prueba de detección de Ingeniería social

Actividad creada por OSI

.

https://www.osi.es/es/campanas/ingenieria-social/prueba-deteccion-ingenieria-social

Proyecto No More Ransomware

Busca erradicar el ransomware con la participación de Europol, Intel Security, Kaspersky Lab y diferentes cuerpos de seguridad europeos entre ellos Policía Nacional y Guardia Civil.
Repositorio de descifradores gratuitos.

https://www.nomoreransom.org

Herramienta open source **AntiRansom** creada por Yago Jesús que actúa como Honeypots.

https://www.security-projects.com/?Anti_Ransom

No Ransom lista de descifradores gratuitos creada por Kaspersky Lab **https://noransom.kaspersky.com/es**

Guías recomendadas

Guía de Privacidad y Seguridad en Internet.
Publicada por INCIBE, OSI y AEPD.

Guía para aprender a identificar fraudes online.
Publicada por INCIBE y OSI.

Tu router, tu castillo. Aprende a configurar el router de forma segura.
Publicada por INCIBE y OSI.

Guías para configurar dispositivos móviles iOS y Android.
Publicadas por INCIBE y OSI.

Guía de ciberataques.
Todo lo que debes saber a nivel usuario. Publicada por INCIBE y OSI.

*Todas las guías están disponibles en PDF para su descarga gratuita.

Vídeos recomendados

Algunas de mis charlas de concienciación en ciberseguridad.

Jugando con fuego. Del sexting a la sextorsión el grooming rondando.

Cómo prevenir enfermedades de transmisión digital y otros peligros en la red.

Ciberseguridad. Cómo proteger y gestionar la identidad digital.

Oversharing: los peligros de la sobreexposición en redes sociales y Sharenting, el riesgo de compartir la crianza de los hijos en Internet.

Decálogo de buenas prácticas en redes sociales. Identidad digital, privacidad y uso seguro.

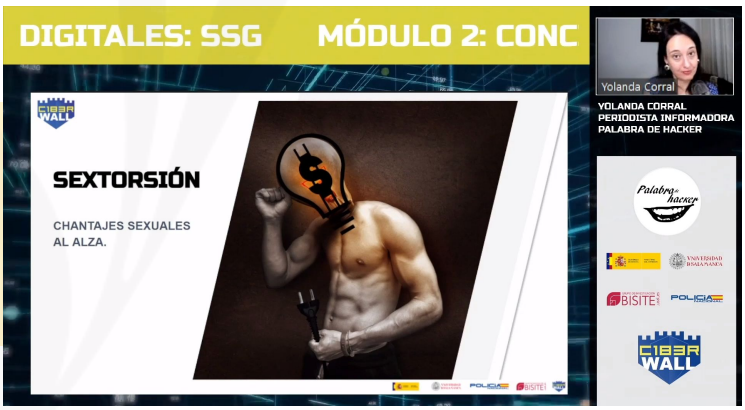
*Vídeos publicados disponibles, haz clic sobre el enlace.

Vídeos recomendados

Vídeos de mis sesiones formativas en C1b3rWall Academy 2022 sobre Prevención de riesgos digitales: SSG - Sexting, Sextorsión y Grooming.

Sexting. Sin control, se acabó la diversión.

Sextorsion. Chantajes sexuales al alza.



Grooming. Depredadores de la inocencia.

*Vídeos publicados disponibles, haz clic sobre el enlace.

Vídeos recomendados

Algunos de los ciberdebates divulgativos realizados en mi canal **Palabra de hacker**, ciberseguridad de tú a tú.

Sextorsión. Cómo afrontar el chantaje sexual por Internet.

¿Qué es el Vishing? Estafas y engaños que llegan por llamadas telefónicas.

Estafa del CEO. Qué es y cómo funciona este fraude electrónico.

Ransomware ¿qué es y cómo actuar?

Fraudes online. Cómo identificarlos y evitarlos.

*Vídeos publicados disponibles, haz clic sobre el enlace.

Vídeos recomendados

Algunos de los vídeos de carácter didáctico publicados en mi canal **Palabra de hacker**, ciberseguridad de tú a tú.

Phishing demo con Socialfish. Concienciando en el uso de Internet.

Cómo desenmascarar acosadores en redes sociales.

Ingeniería social: repaso a la evolución del Phishing avanzado.

Una mirada a la Dark Web y la suplantación de identidades.

*Vídeos publicados disponibles, haz clic.

Vídeos recomendados

Algunos de los vídeos de carácter didáctico publicados en mi canal **Palabra de hacker**, ciberseguridad de tú a tú.

Prevención de ataques de ingeniería social.

Seguridad en Internet y dispositivos móviles: peligros de los QR y URLs acortadas.

Delitos informáticos, consejos a la hora de denunciar.

¿Se puede desaparecer de Internet?

Trabajo, talento y otras cosas del montón.

*Vídeos publicados disponibles, haz clic.

Si necesitas formación, hablemos

"El aprendizaje constante es la gasolina necesaria para enfrentarse a una sociedad cambiante"

Yolanda Corral

Periodista y formadora especializada en ciberseguridad de tú a tú y competencias digitales

¿qué puedo hacer por ti?

www.yolandacorral.com

@yocomu in/yolandacorralm YouTube Palabra de hacker