

Consejos prácticos para proteger tu vida personal y tu negocio en Internet


Carlos Lozano Sánchez

Carlos Lozano Sánchez



- Ingeniero Informático
- Ingeniero Software
- Emprendedor

Aviso legal

1. Todas las marcas, marcas registradas, logotipos e imágenes mostrados en esta presentación, son propiedad de sus respectivos propietarios.
2. El resto de contenidos sigue la licencia: 
3. Los consejos ofrecidos en esta presentación, se basan en la experiencia y opinión personal del autor.
4. Los consejos ofrecidos en esta presentación, no garantizan una seguridad total.

La seguridad total no existe

¿Cómo protejo mis cuentas?

Artículo para conocer la jerga de la seguridad informática: https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/Jerga_seguridad_de_que_hablamos_cuando_decimos

Un millón de cuentas

facebook.

amazon

 Microsoft

Google

 Dropbox



ING  DIRECT

twitter 

 Santander

 Spotify®



¿NECESITO USAR ESTE SERVICIO?

Contraseñas del 2015

starwars
master
solo baseball qwertyuiop
111111 123456789 passw0rd
dragon 1234 12345678
abc123 qwerty login
football password 1qaz2wsx
123456 12345 welcome
letmein 1234567 monkey
1234567890
princess

¿SON SEGURAS MIS CONTRASEÑAS?

10 contraseñas que suelen probar los hackers: <http://www.adslzone.net/2016/03/04/estas-son-las-10-contrasenas-que-suelen-probar-los-cibercriminales-en-sus-ataques/>

Muchos usuarios no utilizan estas contraseñas intencionadamente, pero muchos dispositivos traen por defecto dichas contraseñas y por lo tanto el usuario es vulnerable si no cambia las contraseñas por defecto.

¿Qué es una contraseña segura?

RECOMENDACIÓN:

1. Usar más de 15 caracteres. (Fuerza bruta)
2. Usar minúsculas, mayúsculas, números y símbolos. (Fuerza bruta)
3. NO usar la misma contraseña en varios servicios. (Robo)
4. NO usar contraseñas utilizadas anteriormente. (Robo)
5. NO usar palabras de diccionario de ningún idioma. (Diccionario)
6. NO usar datos de personas, perros, robots, películas, ... (Social)
7. NO seguir patrones como F15EmPrende, T15EmPrende. (Robo)

PROBLEMAS:

- No todos los servicios permiten contraseñas largas
- No todos los servicios permiten letras, números o símbolos
- No todos los teclados tienen ciertos caracteres (ñ, €, ¿, ¡)

Ejemplo de que una contraseña segura puede no ser suficiente: <http://muyseguridad.net/2016/03/09/fallo-hackear-cuenta-facebook-facilidad/>

De cualquier modo es preferible tener contraseñas seguras, las vulnerabilidades se reparan y de nuevo tu contraseña vuelve a ser eficaz.

¿Y cómo nos acordamos de las contraseñas?



¿ES SEGURO?

¿ES EFICIENTE?

LastPass...|

CARACTERÍSTICAS:

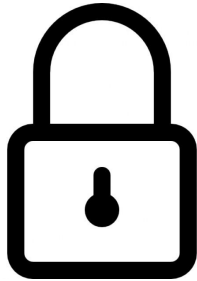
- Gestor de contraseñas
- Notas y documentos seguros
- Multiplataforma
- Almacenamiento en la nube => Accesible desde cualquier lugar
- Cifrado de alta seguridad
- Precio: ~13€ anuales (invitaciones)

PROBLEMA:

- Si te roban la contraseña maestra, te roban todas tus cuentas

LastPass: <https://lastpass.com/>

Doble autenticación / Verificación en dos pasos



Algo que conocemos
(Usuario / Contraseña)



Algo que tenemos
(Móvil / U2F)

ACTIVAR EN LOS SERVICIOS QUE LO PERMITAN

Al activar la autenticación en dos pasos te detallan la aplicación que necesitas usar en el móvil.

La otra opción que comenté se llama Latch (cerrojos virtuales para desactivar los servicios mientras no los usas): <https://latch.elevenpaths.com/>

Recuperación de cuentas

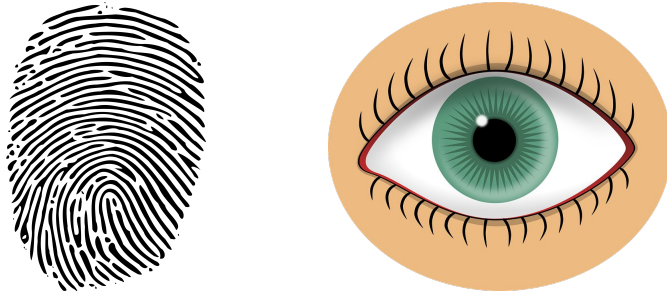


Email alternativo

Preguntas secretas con respuestas aleatorias (LastPass)
(Móvil)

Preguntas secreta con respuestas reales

El futuro de las contraseñas



Artículo que demuestra que es posible saltarse la protección por huella dactilar: <http://www.muycomputer.com/2016/03/07/hackean-smartphones-una-impresora>

Navegación segura: https://

FUNCIONALIDAD:

- Permitir la transferencia segura de datos
- Cifrar todas las comunicaciones entre cliente y servidor

IMPORTANCIA:

- Evitar ataques Man-in-the-middle
- Garantizar integridad de tus datos
- Garantizar confidencialidad de tus datos

RECOMENDACIÓN:

- Usar SIEMPRE HTTPS para datos confidenciales

En cuanto a los certificados SSL (para poder activar HTTPS), muchos hostings te gestionan la compra e instalación de dichos certificados. En caso de tener que comprarlo por nuestra cuenta hay muchas empresas reconocidas:

- Symantec: <http://www.symantec.com/es/es/ssl-certificates/>
- GeoTrust: <https://www.geotrust.com/es/>
- DigiCert: <https://www.digicert.com/es/>
- Thawte: <https://www.thawte.com/>

Además hay una iniciativa para automatizar la creación de los certificados de manera gratuita: <https://letsencrypt.org>

Esta iniciativa ya está teniendo los primeros problemas (aunque personalmente creo que iniciativas como estas van a triunfar): <http://www.redeszone.net/2016/01/08/los-certificados-https-emitados-por-lets-encrypt-son-utilizados-en-paginas-web-fraudulentas/>

Ingeniería social y Phishing

EJEMPLOS:

- Web: Introduzca su tarjeta de crédito para verificar su edad
- Popup: Su cuenta de YYYY ha sido comprometida...
- Email: Te ofrecemos una comisión por ayudarnos...
- En persona: ¿Cómo se llama tu perro?

POSIBLES RESULTADOS:

- Robo de tarjetas de crédito
- Robo de cuentas
- Robo de datos para suplantación de identidad
- Estafa

Artículo sobre ingeniería social y como evitar dichos ataques: https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios//Toma_conciencia_e_vitar_ataques_ingenieria_social

Ejemplo de phishing: <http://es.gizmodo.com/el-principe-nigeriano-que-te-ofrecia-dinero-ahora-es-un-1758809806>

Bulo de McDonalds a través de WhatsApp: <http://www.adslzone.net/2016/02/25/un-bulo-de-mcdonalds-por-whatsapp-roba-tus-datos-prometiendo-un-cupon-de-50-euros/>

Phishing que suplanta a Mercadona: <http://www.adslzone.net/2016/03/02/nueva-alerta-por-un-phising-que-suplanta-a-mercadona-regalando-500-euros/>

Ejemplo de robo de cuentas bancarias: <http://www.adslzone.net/2016/03/09/cuidado-este-malware-te-puede-robar-los-datos-de-acceso-a-tu-banco/>

Ejemplo de ingeniería social



¿Cómo protejo mis sistemas?

Artículo sobre el software libre en la empresa (también decenas herramientas libres que se pueden utilizar para evitar herramientas cerradas): <http://www.linuxadictos.com/software-empresarial-codigo-abierto.html>

Actuar con precaución

No descargar adjuntos sospechosos

No descargar aplicaciones para móvil desde fuera de las stores

No descargar aplicaciones de ordenador desde páginas no oficiales

No instalar aplicaciones con licencias ilegales o cracks

No ejecutar archivos desconocidos

No navegar por páginas desconocidas

No pulsar enlaces o botones de publicidad y engañosos

No usar cuentas de administrador

TODOS LOS SISTEMAS PUEDEN SER INFECTADOS

Informe sobre la importancia de no usar cuentas de administrador: <http://muyseguridad.net/2016/02/06/86-vulnerabilidades-windows-evitables/>

Consejos para proteger Android: <http://www.xatakandroid.com/seguridad/como-proteger-tu-dispositivo-android>

Consejos para proteger iOS: <http://www.applesfera.com/iphone/9-medidas-de-seguridad-para-convertir-tu-iphone-y-ipad-en-inquebrantables>

Ingeniería social y Phishing

EJEMPLOS:

- Web: ¡Se han encontrado 4 virus en tu ordenador!
- Popup: ¡Le ha tocado un coche!, introduzca su móvil/email
- Email: Le adjuntamos un aviso legal ...

POSIBLES RESULTADOS:

- Instalación de malware
- SPAM
- Suscripción a servicios de SMS Premium

Ejemplo de paquete de emojis que te subscriben a SMS premium: <http://www.adslzone.net/2016/03/07/nuevo-paquete-de-emojis-para-whatsapp-cuidado-con-el-timo-que-suscribe-a-sms-premium/>

Ejemplo de sorteo de un Mercedes: <http://www.adslzone.net/2016/03/14/el-timo-del-sorteo-de-un-mercedes-que-arrasa-en-facebook-solo-quiere-tus-datos/>

Control de acceso

¿Dejarías la puerta de tu casa o coche abierta?

Entonces, ¿por qué lo haces con tu ordenador o móvil?

RECOMENDACIÓN:

- Crear una cuenta para cada usuario
- Proteger las cuentas con contraseña / PIN / patrón
- No utilizar privilegios de administrador
- No compartir cuentas ni contraseñas
- Bloquear el sistema automáticamente si no hay actividad

Antivirus: Windows Defender





Comparativa de antivirus:

- www.av-test.org
- www.av-comparatives.org

Antivirus:

- Kaspersky: <http://www.kaspersky.es/>
- Bitdefender: <http://www.bitdefender.es/>
- Avira: <https://www.avira.com/>
- Avast: <https://www.avast.com/es-es/>

Ejemplo de malware que es capaz de saltarse todos los antivirus más usados: <http://www.adslzone.net/2016/02/09/este-malware-es-capaz-de-saltarse-las-barreras-de-seguridad-de-24-antivirus/>

Ejemplo de malware para Android: <http://www.adslzone.net/2016/03/03/triada-el-nuevo-troyano-que-se-hace-con-el-control-de-tu-movil-android/>

Artículo sobre los antivirus gratuitos: <http://www.xataka.com/aplicaciones/antivirus-gratis-y-negocio-asi-funciona-y-hace-dinero-la-seguridad-informatica-que-no-cobra>

Firewall

FUNCIONALIDAD:

- Gestionar y filtrar tráfico entrante desde Internet
- Gestionar y filtrar tráfico salientes hacia Internet
- Evitar intrusiones
- Evitar que nuestra información se filtre.

RECOMENDACIÓN:

- Usar el firewall por defecto del sistema operativo
- Usar el firewall incluido en algunos antivirus

Navegadores Web



Mozilla Firefox



Google Chrome

Mozilla Firefox: <https://www.mozilla.org/es-ES/firefox/new/>

Google Chrome: <https://www.google.com/chrome/>

Extensiones para navegadores

REGLA:

Menos extensiones y plugins => Más seguridad

RECOMENDACIÓN:

- Desactivar extensiones y plugins no utilizados
- NO instalar extensiones de antivirus / antimalware
- Usar bloqueadores de anuncios / trackers (uBlock Origin)

PROBLEMAS:

- Bloqueo de ciertas páginas web que pueden contener malware
- Disminución de funcionalidades en ciertas páginas web

Enlaces de uBlock Origin:

- Mozilla Firefox: <https://addons.mozilla.org/en-us/firefox/addon/ublock-origin/>
- Google Chrome: <https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?hl=en>

Web con herramientas para proteger la privacidad: <https://www.privacytools.io/>

Artículo que comenta las vulnerabilidades de las extensiones de antimalware: <http://muyseguridad.net/2016/02/10/no-extensiones-antimalware-seguridad/>

Aplicaciones y datos

RECOMENDACIÓN:

- Eliminar todas las aplicaciones que no son usadas.
- Eliminar todos los documentos / datos que no son necesarios.
- Eliminar instaladores de las aplicaciones.

REGLA:

- Menos elementos => Menos vulnerabilidades
- Menos vulnerabilidades => Menos ataques
- Menos ataques => Más seguridad

Ejemplo de vulnerabilidades en instaladores guardados en la carpeta de descargas:
<http://www.adslzone.net/2016/02/22/acumular-archivos-en-tu-carpeta-de-descargas-puede-abrir-al-malware-la-puerta-de-tu-pc/>

Actualizaciones (MUY IMPORTANTE)

1. Sistema Operativo
2. Navegadores Web
3. Antivirus / Antimalware / Firewall
4. Java
5. Lector PDF
6. Microsoft Office
7. Aplicaciones / Extensiones / Plugins / Temas / Servidores
8. Drivers (Impresoras, tarjetas gráficas, ...)
9. Router
10. BIOS / Firmware

Opciones para actualizar drivers:

- Quizás el fabricante del ordenador te proporciona una herramienta
- Buscar manualmente cada mes, nuevas actualizaciones en las web oficiales
- <http://www.adslzone.net/2016/03/12/como-actualizar-facil-y-gratis-todos-los-drivers-de-tu-pc/>

Ejemplo de malware para Android que afecta a versiones antiguas: <http://muyseguridad.net/2016/03/14/malware-android-3/>

Este malware afecta al 61,5% de los móviles Android porque tienen instaladas versiones antiguas de hace más de 18 meses.

Copias de seguridad / Backups

¿POR QUÉ?:

- Eliminación accidental de datos
- Robo de dispositivo (ordenador, móvil, USB, ...)
- Rotura del dispositivo (disco duro, ordenador, USB, móvil, ...)
- Infección con malware

RECOMENDACIÓN:

- Usar las herramientas del sistema operativo
- Automatizar el proceso
- Si es posible, una copia de seguridad por día

Cifrar datos

¿PARA QUÉ?:

- Proteger los datos
- Cumplir con la LOPD

RECOMENDACIÓN:

- Cifrar los discos duros (herramientas del sistema)
- Cifrar los móviles (herramientas del sistema)
- Cifrar datos confidenciales
- Cifrar usando algoritmo AES

CONSECUENCIA:

- Mayor lentitud al arrancar el sistema
- Mayor lentitud al acceder a los datos

Artículo que explica la polémica entre el FBI y Apple por el cifrado de iOS: <http://www.applesfera.com/apple-1/guia-para-entender-que-esta-pasando-con-el-fbi-y-el-cifrado-del-iphone>

Las grandes van a mejorar sus cifrados para garantizar la privacidad del usuario: <http://www.adslzone.net/2016/03/14/whatsapp-facebook-google-y-las-grandes-de-internet-van-a-blindar-tu-privacidad/>

Herramientas externas multiplataforma para cifrado:

- Veracrypt: <https://veracrypt.codeplex.com/>
- AES Crypt: <https://www.aescrypt.com/>

Localización, bloqueo y eliminación remota

¿PARA QUÉ?:

- Localizar tu dispositivo en caso de robo o pérdida
- Bloquear tu dispositivo en caso de robo o pérdida
- Eliminar todos los datos del dispositivo en caso necesario
- Gestionar tu dispositivo de forma remota

RECOMENDACIÓN:

- Activar los sistemas por defecto de gestión remota
- Si no hay sistema por defecto, usar alguna herramienta externa

PROBLEMA:

- El sistema de gestión externa, se convierte en una amenaza

Artículo que explica la polémica entre el FBI y Apple por el cifrado de iOS: <http://www.applesfera.com/apple-1/guia-para-entender-que-esta-pasando-con-el-fbi-y-el-cifrado-del-iphone>

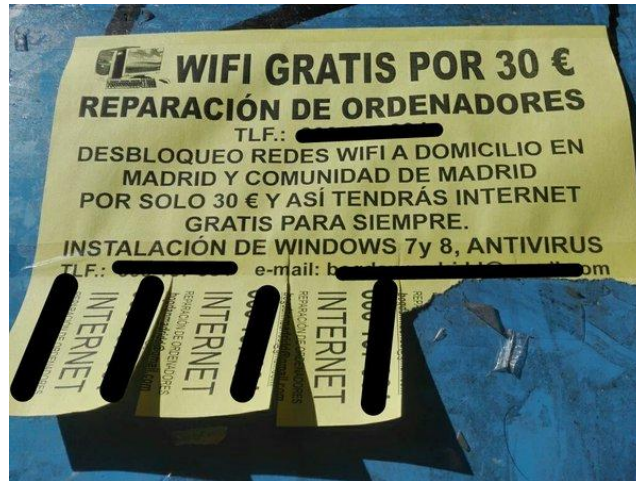
Herramientas externas multiplataforma para cifrado:

- Veracrypt: <https://veracrypt.codeplex.com/>
- AES Crypt: <https://www.aescrypt.com/>

Dispositivos desconocidos (de la calle)



Soporte técnico



¿Cómo limpio mi sistema?

Síntomas de infección

- El sistema funciona muy lento
- El sistema se reinicia inesperadamente
- El sistema cambia de idioma
- El sistema pierde conexión a Internet
- El sistema actúa de forma autónoma
- El navegador cambia la página de inicio
- El navegador muestra muchos popup o páginas no deseadas
- Algunas aplicaciones dejan de funcionar
- El antivirus y/o el firewall se desactiva

La magia no existe en informática

Ransomware



Ejemplo de cómo limpiar un ransomware: <http://muyseguridad.net/2016/02/16/descifra-ransomware-hydracrypt-umbrecrypt/>

Como demuestra el ejemplo anterior, algunos ransomware se pueden eliminar con herramientas específicas creadas para ese malware en concreto sin necesidad de pagar la extorsión. Hay algunos ransomware que no tiene solución y la única opción es pagar el rescate.

Artículos sobre un ransomware que pedía 3 millones a un hospital:

- <http://www.adslzone.net/2016/02/16/un-ransomware-secuestra-los-datos-de-un-hospital-y-piden-3-millones-por-el-rescate/>
- <http://www.adslzone.net/2016/02/18/el-hospital-victima-de-ransomware-paga-finalmente-15-000-euros-por-el-rescate/>
- <http://www.adslzone.net/2016/02/28/ya-no-son-solo-hospitales-cada-vez-son-mas-las-instituciones-publicas-victimas-de-ransomware/>

Medidas para evitar que te secuestren tus dispositivos: https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios//Que_no_te_secuestre_en_elordenador_Medidas_para_evitarlo

Ejemplo de Ransomware camuflado en un documento Word:

<http://www.adslzone.net/2016/02/19/abrir-un-simple-documento-de-word-puede-secuestrar-nuestro-ordenador/>

Ejemplo de Ransomware para OSX:

<http://www.applesfera.com/os-x/keranger-el-primer-ransomware-capaz-de-afectar-a-os-x-ha-sido-detectado-y-eliminado>

Ejemplo de Ransomware para Android:

<http://www.pandasecurity.com/spain/mediacenter/noticias/virus-policia-android/>

ESET advierte de infecciones masivas por ransomware: <http://revistaesecurity.com/eset-advierte-de-infecciones-masivas-por-los-ransomware-locky-y-teslacrypt/>

Antivirus de Rescate

1. **Descargar** el antivirus (Kaspersky, Bitdefender, Avira, Avast, ...)
2. **Grabar** el antivirus en un CD o USB (instrucciones del fabricante)
3. **Reiniciar** el ordenador con el CD metido o el USB enchufado
4. **Esperar** que el ordenador arranque con el antivirus (varios minutos)
5. **Analizar** el ordenador con el antivirus (varias horas)
6. **Desinfectar** los virus encontrados
7. **Reiniciar** el ordenador.

Si no arranca el antivirus, buscar en Google un tutorial para “Configurar la BIOS para arrancar desde CD / USB”

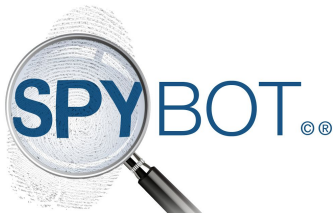
Los antivirus de rescate pueden eliminar ciertos ransomware y otros tipos de malware. Normalmente se utilizan si algún malware te impide arrancar el sistema operativo.

Antivirus de rescate:

- Kaspersky: <http://support.kaspersky.com/viruses/rescuedisk>
- Bitdefender: <http://www.bitdefender.es/support/c%D1%86%D0%81mo-preparar-un-bitdefender-rescue-cd-1249.html>
- Avira: <http://www.avira.com/es/download/product/avira-rescue-system>
- Avast: <https://www.avast.com/es-es/faq.php?article=AVKB114>

Aparte de los antivirus de rescate, hay antivirus online que te analizan si estas infectado (normalmente no te eliminan la amenaza). Únicamente utilizar este tipo de antivirus si son de marcas reconocidas mundialmente ya que podría tratarse de malware.

Herramientas de limpieza



Herramientas:

- AdwCleaner: <https://toolslib.net/downloads/viewdownload/1-adwcleaner/>
- CCleaner: <https://www.piriform.com/ccleaner>
- SpyBot: <https://www.safer-networking.org/>
- MalwareBytes: <https://www.malwarebytes.org/>

Herramienta avanzada:

- TronScript: <https://www.reddit.com/r/TronScript>

Otras herramientas complementarias:

- <http://www.adslzone.net/2016/02/29/las-mejores-aplicaciones-gratis-para-proteger-la-seguridad-de-tu-movil-u-ordenador/>
- <http://www.adslzone.net/2016/03/01/comprueba-facilmente-con-esta-web-si-tu-pc-esta-a-salvo-de-ataques-informaticos/>

Instalación limpia

BENEFICIO:

- Aumenta el rendimiento
- Evita problemas causados por actualizaciones
- Elimina cualquier resto de malware
- Elimina cualquier resto de aplicaciones desinstaladas
- Organización de tus documentos y backup

RECOMENDACIÓN:

- Realizar al menos una instalación limpia al año
- Evitar actualizar los sistemas operativos

CUIDADO: Las copias de seguridad pueden tener malware

¿Cómo protejo mi red?

Configuración del router WiFi

RECOMENDACIÓN:

- Usar cifrado WPA2-PSK (AES)
- Desactivar WPS (WiFi Protected Setup)
- Cambiar la contraseña de la red inalámbrica (LastPass)
- Cambiar la contraseña de acceso al router (LastPass)

PROBLEMAS:

- No todos los dispositivos soportan WPA2-PSK (AES)

MÁS SEGURIDAD => MENOS COMODIDAD Y COMPATIBILIDAD

Noticia sobre Hackers que acceden a tu router para protegerte: <http://www.adslzone.net/2016/02/10/los-caballeros-blancos-de-internet-los-hackers-que-usan-una-botnet-para-proteger-tu-router/>

Herramientas para conocer si alguien está en tu red: <http://www.genbeta.com/seguridad/7-consejos-y-herramientas-gratis-para-saber-quien-te-puede-estar-robando-wifi>

WiFi de Invitados

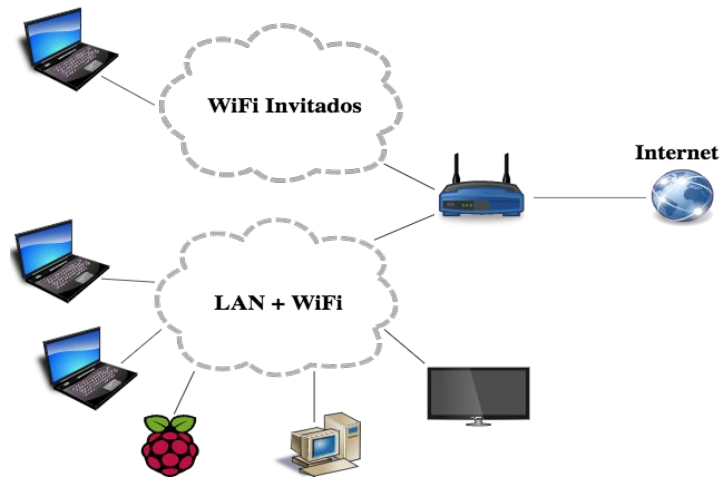


Imagen original: <http://linux.xvx.cz/2013/08/tp-link-tl-wr1043nd-and-openwrt-1209.html>

¿Cómo protejo mi empresa?

8 refranes para la ciberseguridad de tu empresa: https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios//Emprendedor_Los_8_refranes_para_la_ciberseguridad_de_tu_empresa

Artículo sobre buenas prácticas en seguridad móvil: https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios//Decalogo_buenas_practicas_seguridad_movil

El 71% de las empresas han sufrido como mínimo 5 incidentes de seguridad en el último año: <http://revistaesecurity.com/el-71-de-las-organizaciones-ha-sufrido-como-minimo-5-incidentes-de-seguridad-en-el-ultimo-ano/>

Cuentas de empleado

RECOMENDACIÓN:

- Cada empleado debe tener sus propias cuentas
- No se deben compartir cuentas entre empleados
- Se deben cambiar las contraseñas periódicamente
- Política de privilegio mínimo (solo acceden a lo que necesitan)

PROBLEMAS:

- No todos los servicios son multiusuario

BENEFICIOS:

- Control de los datos
- Control de los empleados

Artículo sobre la seguridad de cambiar periódicamente las contraseñas: <http://www.genbeta.com/seguridad/cambiar-de-contrasena-cada-dos-por-tres-mala-idea-si-buscas-mas-seguridad>

Separación personal y profesional

- ¿Cómo de seguro es conectar dispositivos personales a la red interna del trabajo?
- ¿Cómo de seguro es usar los mismos dispositivos para tareas tanto personales como profesionales?
- ¿Cómo de seguro es llevarte datos de la empresa a casa?
- ¿Cómo operamos cuando manejamos los mismos servicios (Facebook, Twitter, ...) tanto personalmente como profesionalmente?
- ¿Deben los empleados usar / instalar cualquier aplicación en la empresa? ¿Y si usa una licencia ilegal?

MUCHAS PREGUNTAS, POCAS RESPUESTAS

Artículo que analiza los problemas de permitir el uso de dispositivos de nuestros empleados: https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios//Ser_o_no_ser_movil_he_aqui_el_dilema

Dispositivos externos

PROBLEMAS:

- Los ordenadores, móviles y memorias USB personales pueden estar infectados con malware y no disponer de las medidas de seguridad adecuadas

EJEMPLOS:

- Stuxnet
- USB promocionales
- Dispositivos con malware de fábrica.

RECOMENDACIÓN:

- Controlar que dispositivos se usan y su seguridad
- Incluir en el contrato, cuando se firma la política de la empresa

Descripción de Stuxnet (Una de las primeras armas cibernéticas): <https://es.wikipedia.org/wiki/Stuxnet>

IBM distribuye malware en USB promocionales: <https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/1309-se-distribuyen-dispositivos-usb-infectados-en-conferencia-de-seguridad.html>

Caso de Lenovo por sus ordenadores con malware: <http://www.xataka.com/ordenadores/polemica-con-lenovo-y-su-malware-instalado-de-fabrica-en-sus-ordenadores-explicamos-como-eliminarlo>

Dispositivos perdidos (USB, móviles, portatil)

¿Qué pasa si se pierde o te roban un dispositivo con información confidencial de la empresa?

¿Qué pasa si hay un incendio donde se almacenan los datos de la empresa?

Sólo se puede actuar si se han tomado medidas **preventivas**

Baja de empleados

PROCEDIMIENTO:

1. Conocer los privilegios del empleado
2. Darle de baja de TODOS los servicios de la empresa a los que puede acceder: servidores, sistemas operativos, impresoras, red WiFi, correo electrónico, bases de datos, ...
3. Revocar el acceso a TODOS los datos de la empresa a los que puede acceder
4. Recuperar TODOS los dispositivos de empresa y efectuar un borrado seguro de todos los dispositivos (Caso Bárcenas)
5. Si el ciclo de vida del dispositivo ha terminado, hay que destruir físicamente los discos duros y las memorías

CONSEJO: Incluir en el contrato, cómo debe actuar el ex empleado

Método Guttman para formatear discos duros: <http://www.libertaddigital.com/ciencia-tecnologia/tecnologia/2016-02-15/metodo-guttman-por-que-el-disco-duro-de-barcenas-se-borro-35-veces-y-no-34-o-36-1276567859/>

Contraseñas por defecto

REVISAR:

- Sistemas operativos (Administrador)
- Routers
- Impresoras
- Servidores
- Servicios y aplicaciones
- Bases de datos
- Cámaras IP
- ...

SIEMPRE REVISAR LA CONFIGURACIÓN POR DEFECTO

Legislación

- Ley Orgánica de Protección de Datos de Carácter Personal
- Ley de la Sociedad de Servicios de la Información y de Comercio Electrónico
- Ley de Cookies
- (Ley de Ordenación del Comercio Minorista)
- (Ley General para la Defensa de los Consumidores y Usuarios)
- (Ley General de Telecomunicaciones)
- (Ley de Medidas de Impulso de la Sociedad de la Información)

Ley de protección de datos (LOPD)

DENTRO DE LA UE:

- No ha cambiado la normativa vigente
- Proximamente: Aplicación de la nueva legislación europea

FUERA DE LA UE:

- 6 de Octubre de 2015: Fin de Safe Harbour
- Actualmente: Contratos personalizados o consentimiento
- Próximamente: Privacy Shield

¿Y SI NO LA APLICAMOS CORRECTAMENTE?:

MULTAS entre 600€ y 600.000€

Guía del Responsable de Ficheros: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf

Guía de Seguridad de Datos: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf

Información sobre la nueva legislación europea: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

Artículo sobre Safe Harbour: <http://hipertextual.com/2015/10/anulacion-safe-harbor>

Artículo sobre cómo actuar hasta que Privacy Shield sea legal: <http://infoautonomos.economista.es/blog/safe-harbor-lopd-dropbox-mailchimp-google/>

Artículos sobre Privacy Shield:

- <http://www.adslzone.net/2016/02/29/privacy-shield-asi-es-el-acuerdo-de-europa-y-estados-unidos-para-el-intercambio-de-informacion/>
- https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios//adios_puerto_seguro_bienvenido_escudo_privacidad

Ley de cookies

¿QUÉ ES UNA COOKIE?:

Trozos de información que se guardan en el navegador del usuario y que pueden servir entre otras cosas para rastrearlo

¿Y PARA QUÉ SIRVE LA LEY?:

Sirve para informar de las cookies que se van a utilizar y pedir consentimiento al usuario

¿CÓMO LA APLICAMOS?:

- Haciendo el paripé
- Cookie Consent / Plugins

¿Y SI NO LA APLICAMOS?:

MULTAS de hasta 150.000€

Guía sobre cookies: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf

Herramienta Cookie Consent: <https://silktide.com/tools/cookie-consent/>

Textos legales

SOBRE GOOD FOOD
[SOBRE NOSOTROS](#)
[AVISO LEGAL](#)
[POLÍTICA DE PRIVACIDAD](#)
[POLÍTICA DE COOKIES](#)
[TERMINOS Y CONDICIONES](#)

MI CUENTA
[MIS COMPRAS](#)
[MIS DEVOLUCIONES](#)
[MIS VALES DESCUENTO](#)
[MIS DIRECCIONES](#)
[MIS DATOS PERSONALES](#)
[MIS VALES](#)

INFORMACIÓN
[PROMOCIONES ESPECIALES](#)
[NOVEDADES](#)
[TOP SELLERS](#)
[CONTACTE CON NOSOTROS](#)
[MAPA DEL SITIO](#)

ENVIO
[ENVÍO](#)
[DEVOLUCIONES](#)

CONTACTE CON NOSOTROS

📍 C/ VALDEIRIBAS 30, ALMACÉN 14,
MADRID 28007

☎ Llámanos ahora: 911 274 035 / 673
702 553

✉ EMAIL: MONICA@GOOD-FOOD.ES

FORMA DE PAGO


BOLETÍN

APUNTARSE AL NEWSLETTER

☒ HE LEÍDO Y ACEPTO DE LA [POLÍTICA DE PRIVACIDAD](#)

Utilizamos nuestras cookies propias y de terceros para ofrecerle una mejor experiencia y servicio de acuerdo a sus hábitos de navegación.
Acepte nuestra para continuar navegando con todas las características. Puede obtener más información en nuestro:



Derechos de autor y propiedad intelectual

MUCHAS PREGUNTAS:

- ¿Cómo sabemos si la obra está protegida?
- ¿Cómo sabemos quién es el autor?
- ¿Qué puedo hacer si la obra está protegida?
- ¿Qué puedo hacer si usan mi obra sin mi consentimiento?
- ¿Dónde puedo conseguir obras libres?

LICENCIAS:



Creative Commons



Attribution

Others can copy, distribute, display, perform and remix your work if they credit your name as requested by you



No Derivative Works

Others can only copy, distribute, display or perform verbatim copies of your work



Share Alike

Others can distribute your work only under a license identical to the one you have chosen for your work



Non-Commercial

Others can copy, distribute, display, perform or remix your work but for non-commercial purposes only.

Creative Commons: <https://creativecommons.org/>

Formación a empleados

**“Si crees que la educación es cara,
¡prueba con la ignorancia!”**

(Derek Bok, Rector de Harvard de 1971 a 1991)

Prácticas que hay que enseñar a los empleados: https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/En_puesto_trabajo_empleado_es_superheroe_ciberseguridad

Ingeniería social y Phishing

EJEMPLOS:

- Llamadas desde “soporte técnico”
- Email de la empresa, pidiendo algún dato
- Email de la empresa, pidiendo algún dato para promocionar

POSIBLES RESULTADOS:

- Instalación de malware
- Acceso a la red interna
- Robo de información

Ejemplo de paquete de emojis que te suscriben a SMS premium: <http://www.adslzone.net/2016/03/07/nuevo-paquete-de-emojis-para-whatsapp-cuidado-con-el-timo-que-suscribe-a-sms-premium/>

Auditorías de seguridad

BENEFICIO:

1. ¿Dónde estamos?
2. ¿Qué estamos haciendo bien?
3. ¿Qué estamos haciendo mal?
4. ¿Qué problemas tenemos?
5. ¿Cómo podemos mejorar?

EJEMPLO DE BICIMAD:

- Coste: 45.000.000€ en 12 años = 3.750.000€ al año
- Problemas: DoS propios, vídeo pornográfico, ...

¿Y si tenemos una brecha de seguridad?

1. Actuar rápido para solucionar la brecha
2. Informar correctamente a nuestros clientes/usuarios sobre lo que ha pasado, las medidas que se han aplicado y si tienen que seguir algún procedimiento
3. Decir siempre la verdad
4. Ayudarles en caso de que necesiten ayuda para protegerse
5. Crear planes de contingencia para minimizar las brechas

Los clientes / usuarios no son tontos.

Prefieren las empresa que se preocupan por su seguridad.

¿Cómo me protejo en entornos
públicos?

Redes no seguras (Públicas o no)

RIESGOS:

- Robo de datos / credenciales transmitidos (Man-in-the-middle)
- Ataque e infección de nuestros dispositivos conectados
- Robo de información de nuestros dispositivos conectados
- Suplantación de identidad

RECOMENDACIÓN:

- Intentar no usar redes no seguras
- No iniciar sesión en tus servicios
- No realizar compras online
- Usar una VPN (Virtual Private Network)

Experimento de Avast durante MWC2016 con redes WiFi públicas: <http://es.gizmodo.com/wifi-gratis-en-el-mwc-como-avast-robo-los-datos-privad-1760758811>

Artículos sobre cómo protegerte al usar redes no seguras:

- <https://www.osi.es/es/wifi-publica.html>
- <http://hipertextual.com/archivo/2014/09/protegerte-red-wifi-publica/>
- <http://www.pandasecurity.com/spain/mediacenter/consejos/redes-wifi-publicas-seguras/>

Ordenadores no seguros (Públicos o no)

RIESGOS:

- Altísimo riesgo de infección con malware
- Altísimo riesgo de robo de datos / credenciales (keyloggers)
- Suplantación de identidad

RECOMENDACIÓN:

- NO USAR ORDENADORES NO SEGUROS
- Activar navegación privada
- No iniciar sesión en tus servicios
- No realizar compras online
- No enchufar dispositivos USB

Es mejor una red no segura que un ordenador no seguro

Artículo sobre cómo usar ordenadores públicos: <http://profesoradeinformatica.com/consejos-para-proteger-tus-datos-usando-ordenadores-publicos/>

Ejemplo de ataques



¿Cómo protejo a mi familia?

Dispositivos IoT (Internet of Things)



Cámaras IP: <http://wifihacker.es/hackear-camaras-web/>

Drones:

- <http://www.adslzone.net/2016/03/02/un-hacker-es-capaz-de-estrellar-a-voluntad-un-dron-de-30-000-euros-usado-por-la-policia/>
- <http://www.muycomputer.com/2015/08/16/drones-parrot-hackear-facilmente>

Barbie: <http://www.genbeta.com/actualidad/hello-barbie-y-su-dudosa-politica-de-privacidad-asi-podria-usar-tus-datos-la-muneca-de-mattel>

Un chico alemán hace un documental para demostrar fallos de seguridad en sitios públicos: <https://www.youtube.com/watch?v=Eq05kzMRVzU>

Redes sociales

RECOMENDACIÓN:

- No insultar, ni faltar al respeto
- Cuidado con lo que publicáis (religión, empresas, política, ...)
- Cuidado con lo que compartáis (imágenes, videos, ...)
- Gestionar quién está en vuestra red de contactos
- **Configurar y revisar** los ajustes de privacidad periódicamente

Lo que se sube a Internet, se queda en Internet

Aunque ahora tenemos derecho al olvido

Las empresas revisan las redes sociales: <http://www.elblogsalmon.com/mundo-laboral/cuidado-con-lo-que-escribes-en-twitter-nueve-de-cada-diez-empresas-consultan-las-redes-de-sus-candidatos>

6 errores que pueden arruinar tus posibilidades de conseguir empleo: <http://erafbadia.blogspot.com.es/2015/08/6-errores-en-redes-sociales-pueden.html>

Artículo sobre subir fotos de tus hijos: <http://www.genbeta.com/redes-sociales-y-comunidades/la-policia-francesa-advierte-a-los-padres-del-peligro-de-subir-fotos-de-sus-hijos-a-facebook>

<http://www.adslzone.net/2015/10/06/detenido-por-abrir-una-cuenta-falsa-en-redes-sociales-y-suplantar-la-identidad/>

Puedes estar cometiendo un delito sin saberlo: <http://www.internautas.org/html/7494.html>

Formación desde pequeños

REFLEXIONES:

- Hoy en día no tenemos excusas para no formarnos y aprender
- Tenemos la oportunidad de aprender juntos:

**“Dime y lo olvido, enséñame y lo recuerdo,
involúcrame y lo aprendo”**

(Benjamin Franklin)

- Si queremos ayudarles, tenemos que sacrificarnos

**“Si le enseñaste a mirar antes de cruzar,
¿por qué no le enseñas a usar Internet de forma segura?”**

(Carlos Lozano Sánchez)

Uso responsable y seguro de Internet: http://www.fapar.org/escuela_padres/ayuda_padres_madres/uso_internet_recomendaciones.htm

Iniciativa que promociona el uso seguro de Internet: <http://www.pantallasamigas.net/>

Control parental

FUNCIONALIDAD:

- Bloqueo de aplicaciones
- Bloqueo de páginas web
- Control del tiempo
- Monitorización de la actividad

RECOMENDACIÓN:

- Restringir de acuerdo a la edad (no ser muy estricto)
- Proteger desde la educación
- En empresas, cuidado con las restricciones al empleados
- Probar los controles parentales que traen por defecto los sistemas operativos y navegadores

Cómo bloquear contenido inapropiado en YouTube: <http://www.adslzone.net/2016/03/03/como-bloquear-el-contenido-inapropiado-para-nuestros-hijos-en-youtube/>

Modo niños de Netflix: <http://www.xatakandroid.com/aplicaciones-android/netflix-incluye-un-modo-para-ninos-que-finalmente-los-ninos-querran-usar>

Mi reflexión: Los controles parentales son adecuados para proteger a los menores de edad, pero debemos de comprender que si quieren ver algún contenido bloqueado buscarán la forma de saltarse las protecciones. En dicho momento, dejarás de tener el control y puede que estés poniendo en peligro a tu hijo o hija. Es mejor educarlos para que conozcan los límites, para que aprendan a identificar páginas peligrosas, a detectar y evitar estafas, a usar redes sociales de forma segura, a detectar focos de infección con malware. Pero no olvidemos que tienen su vida y deben equivocarse para ir aprendiendo.

Compras online



RECOMENDACIÓN:

- Comprar desde redes y dispositivos seguros
- Comprar en tiendas online de confianza y legales
- Buscar algún sello de confianza
- Leer los comentarios y valoraciones de otros clientes
- Leer las condiciones de devolución y de garantía
- Comprobar el coste total (con gastos de envío)
- Comprobar la fecha de entrega
- Utilizar una tarjeta de prepago o virtual
- Tener cuidado con las ofertas y precios bajos
- No todos los gastos de gestión son legales
- Nunca te pedirán que introduzcas el PIN de la tarjeta

Consejos para comprar seguro:

- http://www.elconfidencial.com/tecnologia/2014-12-25/diez-consejos-para-comprar-online-de-forma-segura-estas-navidades_600368/
- <http://gemaberrio.com/blog/consejos-comprar-seguro-por-internet/>
- <http://www.finanzasparatodos.es/es/kitsupervivencia/tarjetascreditodebito/seguridadcomprasinternet.html>

Cuidado con las tiendas online falsas: <http://revistaesecurity.com/spam-y-falsas-tiendas-online-no-todo-es-amor-en-san-valentin/>

Artículo para prevenir compras fraudulentas en TU tienda: https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/tienda_online_conoce_como_prevenir_compras_fraudulentas

No te pueden cobrar por pagar con tarjeta: <http://www.ocu.org/dinero/tarjetas/noticias/prohibicion-recargos-tarjeta>

Sellos de confianza (suelen requerir auditorías):

- Confianza online: <https://www.confianzaonline.es/>
- Trusted shops: <http://www.trustedshops.es/>
- eKomi (para garantizar las valoraciones de los usuarios): <https://www.ekomi.es/es/>

Artículo sobre los sellos de confianza: http://www.eldiario.es/hojaderouter/internet/sellos-confianza-seguridad-comercio_electronico_0_327567271.html

Cómo me mantengo informado

NO HACER CASO a las cadenas de email / WhatsApp

CONSULTAR:

- El Twitter de la Policía Nacional (@policia)
- El instituto nacional de ciberseguridad (INCIBE)
- Blogs especializados en tecnologías y seguridad
- Páginas oficiales de los proyectos (nuevas releases y CVE)
- Google

Último consejo

No compartas **NUNCA** tus cuentas.

Ni con tu familia. Ni con tu pareja.

Ni con tus amigos. Ni con tus empleados.

La confianza no se gana conociendo las cuentas.