

APLICA la Cultura de Protección de Datos en tu Vida y en tu Empresa

Su Seguro Servidor

AMPARO D. VALCÁRCE

ROSA F. FERNÁNDEZ

© Amparo D. Valcárce y Rosa F.Fernández. Todos los Derechos Reservados.
No se puede reproducir el contenido de este libro relativo a contenidos e imágenes por ningún canal ni formato.
Todas las imágenes, enlaces (links), videos y reproducciones gráficas son de producción propia de las autoras con licencia estándar o libre para su uso didáctico. Los tipos de letra (fuentes) on line y enlaces tienen licencia estándar y/o creative commons.
Para permisos dirigirse a las autoras a su dirección de correo electrónico: soluciones@futurasoluciones.es

DRM FuturaSoluciones
1ª edición Agosto 2015
Última Edición Revisada Abril 2023

Con el RGPD que deroga a la histórica y veterana LOPD de 1999, y nace con el empeño en su espíritu legislativo de aumentar y proteger los derechos del usuario sobre sus datos, recogiendo un amplio espectro tecnológico desde sus orígenes en el año 2011. Actualmente decir protección de datos es pensar en robo de contraseñas, piratas (hackers), brechas de seguridad , derecho al olvido y privacidad por defecto.

Pero ¿qué pensaría usted si por usar una sencilla pulsera, de esas que miden pulsaciones, y que regalan con los cupones del periódico mañana le llama una compañía de seguros para ofrecerle sus servicios?

Así es, querido lector, querida lectora, estamos en manos de los "big data", es decir, de las empresas que manejan esos volúmenes de datos recopilados con mucha paciencia y sin esfuerzo- recuerde que la mayoría de los datos se los HA REGALADO USTED a cambio de una suscripción gratuita, un envío de blog o un cupón descuento- y que tienen un buen retrato de cada uno de nosotros.

También estamos en manos de los buscadores: explorer, mozilla, google… que a cambio de una información rápida y cómoda tienen lo que no está en los escritos de nuestra vida tanto personal como profesional. Además del acoso (mobbing) digital, los chantajes desde las redes sociales y otras lindezas ciberdelincuentes, que no significan ni más ni menos que estar con la espalda abierta en todo momento.

Pero no se preocupe, puede que usted no lo sepa, **LA SEGURIDAD ESTÁ EN SU MANO.** Al igual que poco a poco ha construido un perímetro de seguridad para su casa, para su hogar, para su garaje, para su coche….así puede hacerlo para su oficina, para su empresa y para su familia. Y ¿de qué forma? aplicando la cultura de protección de datos, trabajando desde la prevención y no desde la incidencia y, sobre todo, aplicando el sentido común a cada transacción y desde cada dispositivo.

Usted sabe que nos gusta protegerle y que una de nuestras líneas de servicio es la de protección de datos y seguridad de la información. Por eso queremos compartir con usted unos cuantos conceptos que puede aplicar en su día a día, e incluirlo en su rutina diaria.

Porque usted nos importa, le enseñamos a protegerse, para que proteja a sus clientes, a su familia y a su privacidad. Leános y descubra por qué somos los Guardianes de sus Datos.

Su segura servidora,
la consejera de seguridad


zona vigilada
SegurConsejos

Si usted vive en la Sociedad de la Información (¿y quién no?) y trabaja con los canales digitales habituales:

-internet
-redes sociales
-datos en la nube

es de vital importancia que conozca y que adquiera hábitos de seguridad para usted, su familia y su negocio.

Traemos una selección muy granada de conceptos y usos que hemos realizado de iniciativas y comunicaciones de páginas especializadas, así como del Colegio Profesional de Ingeniería en Informática de Galicia.

Al igual que ocurre con los hábitos saludables, que cuanto antes los adquiera será mejor para su salud, la adquisición y la aplicación de hábitos en seguridad, para trabajar desde la prevención y la información, harán que su perímetro de seguridad aumente y por tanto que los riesgos disminuyan.

Vamos allá.


zona vigilada
SegurConsejos



antivirus

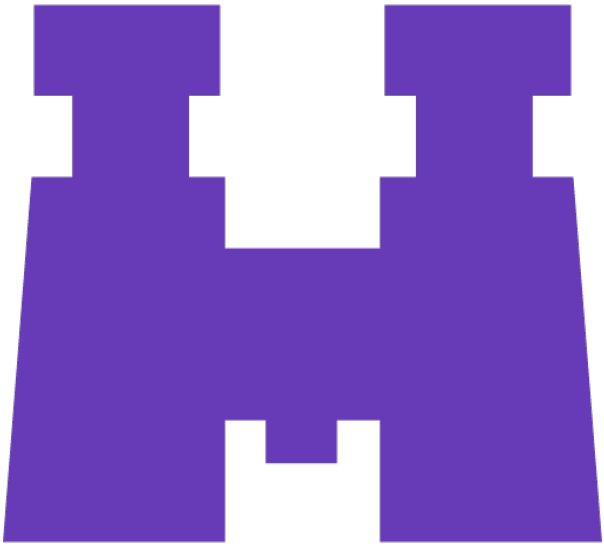
compra la Licencia

Compre licencias originales.

Compre tantas como dispositivos vaya a utilizar.

Actualice periódicamente su software. Usted sabe que puede elegir qué actualizar.

Es necesario que configure el software de su navegador con las opciones de seguridad más restrictivas.



buscadores

Configurarlos

Tenga muy en cuenta que cuando usa un buscador, usted está metiendo información en casa de la empresa del buscador. Es decir, los datos que usted pone en el buscador serán empleados, como mínimo, para ofrecerle anuncios y publicidad comercial.

Lèase las condiciones de uso del buscador que más utilice.

Los buscadores pueden obtener perfiles completos sobre nuestra información pública en internet, además de conocer los gustos y hábitos de consumo, gracias a las herramientas de análisis de navegación.



Cámaras web

Vigila y Controla

Antes de instalar una cámara web que reproduzca imágenes en internet, asegúrese de que la captación sea lo menos intrusiva posible.

Garantice la seguridad impidiendo el acceso no autorizado a imágenes captadas por el uso de este tipo de cámaras.

Y OJITO con las cámaras que ya vienen integradas en su portàtil: quizás al entrar en una web se active la cámara y le estén grabando sin que lo sepa.

Un remedio casero pero eficaz si no usa la videoconferencia: clausure el ojo de la cámara antes de conectarse a internet.



Contraseñas

Solo para tus ojos

A ser posible, tenga contraseñas distintas para cada servicio al que esté suscrito en la web o para los sitios a los que acceda en internet.

Procure que no coincidan con el PIN de su tarjeta bancaria o el acceso a su banca electrónica, y nada previsible como su fecha de nacimiento, ni ponga palabras del diccionario ni diminutivos.

Lo deseable es que sean largas, que combinen todo tipo de caracteres: mayúsculas con minúsculas, números, otros caracteres y, sobretodo que a usted le resulten fáciles de recordar y a un extraño muy difíciles de adivinar.

Y RECUERDE, su contraseña debe ser como su cepillo de dientes:

-Úselo cada día

-Cámbielo regularmente

-NO lo comparta con sus amigos ni familiares



Compartir

Dónde y Con Quién

Compartir es un verbo que llevado a internet tiene mucho peligro.

Conlleva el riesgo implícito de llevar, con sus datos, otros datos o perfiles que le han confiado otros miembros de su red.

Configurar las opciones de seguridad, de visionado y de publicación es básico para no incurrir en riesgos de seguridad con sus datos y, sobre todo, con datos de sus clientes o de terceros que no han autorizado o simplemente que no están de acuerdo en compartir lo que a usted le parece oportuno.



cookies

El Monstruo de las Galletas

Es muy conveniente borrar con regularidad las cookies o archivos temporales de internet, así como el historial de navegación, especialmente cuando se acceda a internet desde un ordenador al que acceden otros usuarios.

Una medida de seguridad preventiva es borrar el rastro, es decir, borrar ese historial de navegación antes de cerrar su sesión.



e-mail

vísteme despacio que tengo prisa

No conteste INMEDIATAMENTE al correo electrónico. Aunque sea urgente, tómese un tiempo antes de contestar para asegurarse de que es el destinatario correcto, de que ha puesto el asunto adecuado y de que lleva el protocolo exigido por el RGPD en su firma.

Cuando envìe mensajes de correo electrónico a diferentes destinatarios, asegúrese de que ha puesto a todos en el campo CCO (CON COPIA OCULTA) y el primer destinatario que sea su propio correo, no el de un destinatario.

En el caso de envìos masivos, utilice “Listas de Distribución”.

Y revise todo ANTES de darle a enviar. ¡“Una vez hecho pop, ya no hay stop”!


EXE

ejecutables

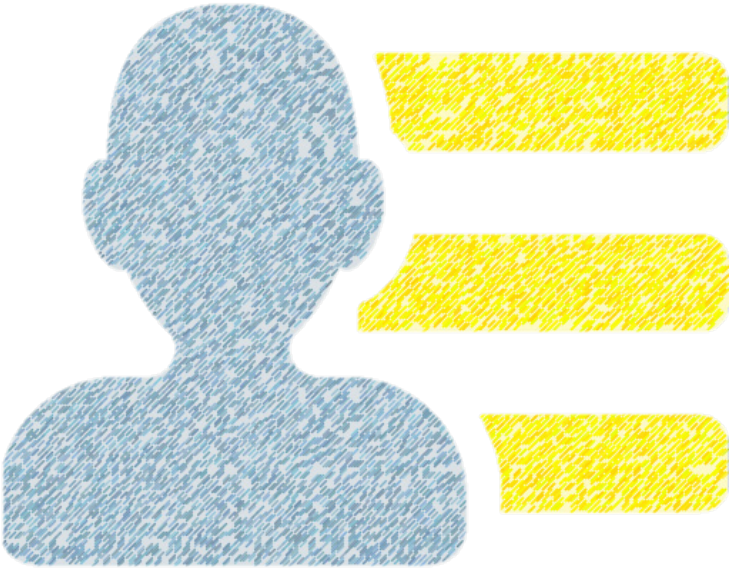
A veces vienen con sorpresa

Son cantos de sirena que aparecen en el ordenador como una solución demasiado tentadora e, inmediatamente, tendemos a darle al botón de "descargar"(downloaded). ERRRORRRR!

Antes de descargar ningún archivo ".exe", es decir, EJECUTABLES y por tanto con capacidad para hacer cambios, a veces, indeseables en su equipo. Compruebe que el sitio del que proviene la descarga NO ES MALICIOSO o no está catalogado como uno de los sitios peligrosos en internet.

Es preferible no descargar ficheros ejecutables, pero, si no le queda más remedio, proteja su equipo con programas (software) de detección o eliminación de programas espia.

Si usted tiene una licencia antivirus legal y correctamente actualizada, su antivirus lanzará una alarma o bloqueara la página o el enlace de la descarga, protegiendo así el equipo.



Identificador

Enséñame la patita por debajo de la puerta

Cuando le pidan que se identifique, tenga que dar para ello datos de carácter personal o bancarios, asegure su perímetro y hágalo sólo en zonas y en sitios web que dispongan de protocolos seguros (https-SSL) y que tengan el cumplimiento normativo aplicado a su entorno web (aviso legal, política de privacidad, condiciones de uso y política sobre cookies).

Nunca proporcione sus datos de usuario o cualquier otra información de identificación y mucho menos su claves de acceso. Su entidad bancaria nunca le pedirá datos de forma poco ortodoxa y por cualquier medio, y si lo hiciera desconfíe.

Ponga especial atención en avisos de sorteos, ofertas telefónicas, correos con avisos de premios, ingresos en su cuenta o promociones comerciales de cualquier tipo.

Si tiene dudas consulte a su banco, a su proveedor de internet o dè aviso o denuncie el hecho a la ciberpolicìa



imagen

Derecho a la intimidad

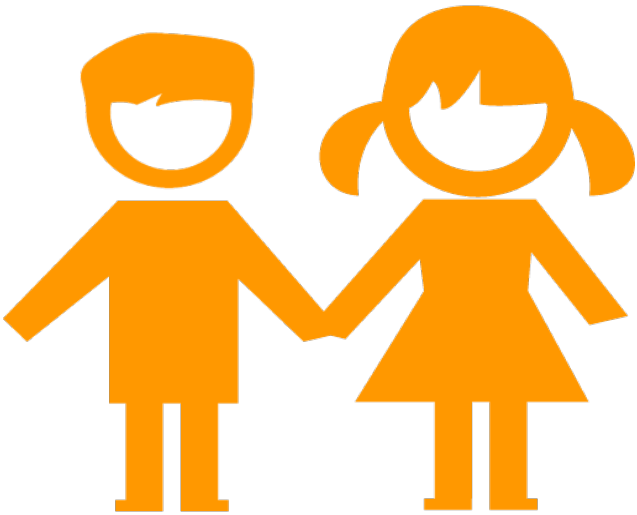
Usted debe saber que la imagen ES UN DATO DE CARÁCTER PERSONAL cuya difusión o acceso no autorizado puede ser particularmente molesto, dañino y causa de denuncia ante la Autoridad de Control o sea ante la Agencia Española de Protección de Datos.

Si además incluyese imágenes de menores, ... aún más sancionable.

Al publicar una foto, compartirla en una red social, o escribir en un foro puede estar incluyendo información de otras personas, y por tanto, vulnerando su derecho a la protección de datos recogido por el RGPD

Sea consciente de la obligación que tiene de respetar estos derechos, ya que puede ser objeto de sanción y de consecuencias jurídicas por su inobservancia.

Y recuerde **LA IGNORANCIA DE LAS LEYES NO EXCUSA DE SU CUMPLIMIENTO**, así que OJO CON LOS AUTORRETRATOS (SELFIES).



infancia

Los Mas Vulnerables

La seguridad de los menores en la red DEPENDE DE USTED, de los hábitos de seguridad y prevención que tengan establecido y de las pautas y controles parentales que haya implantado en su casa y con su familia.

Tener un sólo ordenador para uso familiar en uno de los espacios comunes, acudir a talleres y seminarios sobre la red y los riesgos para menores y adolescentes o controlar las horas de uso de ordenador, así como limitar el acceso a redes sociales son medidas que sus hijos le agradecerán y con las cuales usted ampliará el perímetro de seguridad de su hogar.

Comparta sus dudas con otros padres y madres y solicite información en caso de duda a expertos en la materia.

Aquí encontrará información de utilidad



nube

dónde está el servidor

Cuando usa Google Drive, se descarga o sube un archivo a Dropbox o utiliza una aplicación en modo gratuito como Evernote, usted deja sus datos en servidores de otras empresas.

La nube es muy cómoda porque puede acceder desde cualquier sitio e incluso aunque no lleve un “lápiz” o dispositivo usb puede tener acceso a su información y, claro está, otros también.

Si va a compartir información de su empresa, esté atento y configure adecuadamente las opciones y los privilegios de quien recibe dicha información.

Y como siempre, sea consciente de que en esos paquetes de información puede haber datos que no son suyos.

Lo recomendable, en estos casos, es tener al día el cumplimiento normativo, saber dónde están fisicamente los servidores en los que se alojan sus datos y si la relación es continuada, tener su contrato de encargado de tratamiento formalizado con su proveedor.
Y si trabaja con y en la "nube" deberá saber si es un exportador y/o importador de datos: el RGPD es muy riguroso en este tema.


g
t
f

redes sociales

yo quiero tener un millón de amigos

Cuando utiliza las redes sociales, usted está abriendo, compartiendo e intercambiando datos propios y ajenos, es decir, datos que son suyos personales y/o profesionales pero también datos de otras personas que tiene en su red, en su grupo o en su foro.

No haga menciones personales, ya que, dependiendo de su configuración, podrán leerlo personas ajenas al interesado.

Debe garantizar la seguridad de intercambio de la información y de datos en sus redes sociales, realizando una configuración de seguridad ajustada a su perfil, a su grupo o a sus objetivos y empleando contraseñas.

No permita que los buscadores puedan permitirle a un tercero obtener información pública de su perfil.

Cuando se suscriba a algún enlace de su interés rechace la opción de compartir “desde su red social”, que muchas veces viene por defecto, evitará perder el control sobre el acceso a su espacio en la red.



smartphone

el mundo en tus manos

Un excelente invento que se ha convertido, en materia de seguridad, en un “arma de destrucción masiva”.

Puede que a usted le parezca una expresión exagerada pero, cuando activa su teléfono móvil accede desde ese pequeño dispositivo a sus datos, a la nube, a la red, a las redes sociales, a aplicaciones que no tienen ninguna seguridad o que, en el mejor de los casos le alojan archivos indeseables o molestos, o simplemente están espiando todos sus accesos y claves.

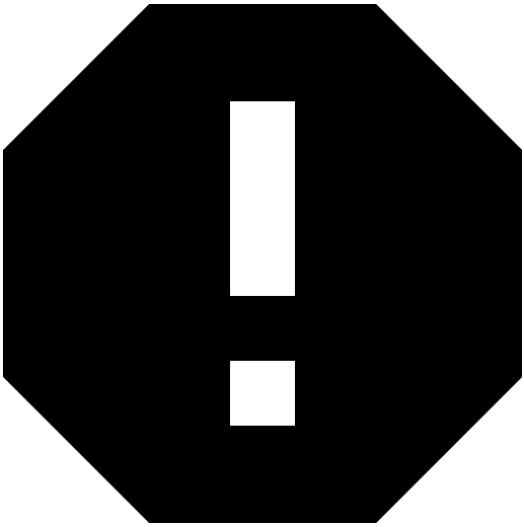
Usar un dispositivo móvil se ha convertido en un ejercicio de riesgos, que aumentan si se controla desde ahí la seguridad de su hogar, las compras del supermercado o el acceso a la banca electrónica.

Toda una perita en dulce para “los malos” de la red.

Lo importante: no acceder desde cualquier lugar que ofrezcan wifi gratis, y ser mucho más restrictivo en su uso que en un entorno de confianza.

Bloquee el acceso a su dispositivo con una contraseña o con un identificador táctil, no tenga ni maneje datos relevantes desde su móvil y limite los chateos en mensajeria instantanea tipo Whatsapp a mensajes lacónicos.

RECUERDE: si no quiere que se sepa, no lo cuente por esos canales digitales.



correo basura (spam)

¿Por qué tengo esto en mi correo?

Si usted recibe correos no deseados o el llamado correo basura (spam) lo recomendable es NO CONTESTAR, ya que si lo hiciera estaría abriendo las puertas de su libreta de direcciones y confirmando su dirección de correo electrónico.

Es conveniente desactivar la opción que envía un acuse de recibo al remitente.

Cuando se suscriba a algún blog o página de su interés sea cuidadoso a la hora de aceptar la política de protección de datos, normalmente en el formulario de contacto incluyen (ya pincha-da) la opción de recibir información comercial. Sepa que es una práctica ilegal y que el RGPD lo persigue con todo su rigor y sus enormes sanciones.

Ah, y si "una chica rusa" le envía un mensaje con información para usted o alguien que quiere confirmar que ha recibido el ingreso en su cuenta corriente, etc... elimínelo sin abrir.


Wi Fi
ZONE

wifi

caramelo envenenado

Ojito con el wifi gratis: centros comerciales, tiendas, restaurantes, cafeterías ... wifi gratis es sinónimo de ALTO RIESGO, es decir, toodo el mundo podrá acceder a todos los datos de su dispositivo.

Tenga en cuenta que toda su información podrá ser capturada, incluídas contraseñas, histórico de su navegación, número de sus cuentas y tipo de transacciones, datos de identificación, correos electrónicos, archivos ... pueden ser encontrados y susceptibles de usarlos de forma indebida con fines no autorizados.

Prohibido engancharse a una wifi gratis para “trabajar” desde un centro comercial mientras se toma el café: puede salirle muy caro.

Se recomienda usar sólo wifi con acceso bloqueado por contraseña, y protocolos lo más actualizados posible (WPA/WPA2).

Que el wifi tenga acceso sin cables no significa que acceda sin red a la red.

DE LAS AUTORAS

Amparo D. Valcárce, es Auditora Senior y Consejera de Seguridad.
De formación humanista, tiene formación especializada en Gestión de la Protección de Datos y en comercio electrónico (INCIBE) y en Calidad.
Es coautora de los libros: “Como cumplir la ley sin aspirinas”, “Ahora voy y lo Twitteo.Su Queja 3.0” (edición digital), “Reglamento Europeo de Privacidad”, así como coautora de la web especializada en seguridad, privacidad, y protección de datos ZonaVigilada.net

Rosa F. Fernández, es Consultora Senior y Consejera de Seguridad.
De formación jurídica y humanista, tiene formación especializada en Gestión de la Protección de Datos y Negocio Tecnológico y Seguridad TIC y en Calidad.
Es Formadora Consultora en Protección de Datos y Gestión de Reclamaciones en la Asociación Española para la Calidad, así como ponente sobre la materia en distintos foros.
Es coautora de los libros: “Como cumplir la ley sin aspirinas”,
“Ahora voy y lo Twitteo.Su Queja 3.0” (edición digital),
“Reglamento Europeo de Privacidad”, así como coautora de la web especializada en seguridad, privacidad y protección de datos zonavigilada.net.
Miembro del Comité Técnico de MetroRisk.es



¿NECESITA MÁS?

admin@zonavigilada.net

Aplique la cultura de protección de datos a su actividad diaria, a su trabajo, en su empresa, con su familia.

Protejase con la protección, aprenda a manejarse en los nuevos canales y con las nuevas herramientas y no permita que nada ni nadie le ponga en riesgo.
La seguridad está en su mano.

Vigila Tus Datos



Agencia de Seguridad y Protección de Datos

ZonaVigilada.net

q f e X m` ^ ` c X [X+ e \ k