eBook

EDUCACIÓN Y BIENESTAR DIGITAL

BIENESTAR DIGITAL

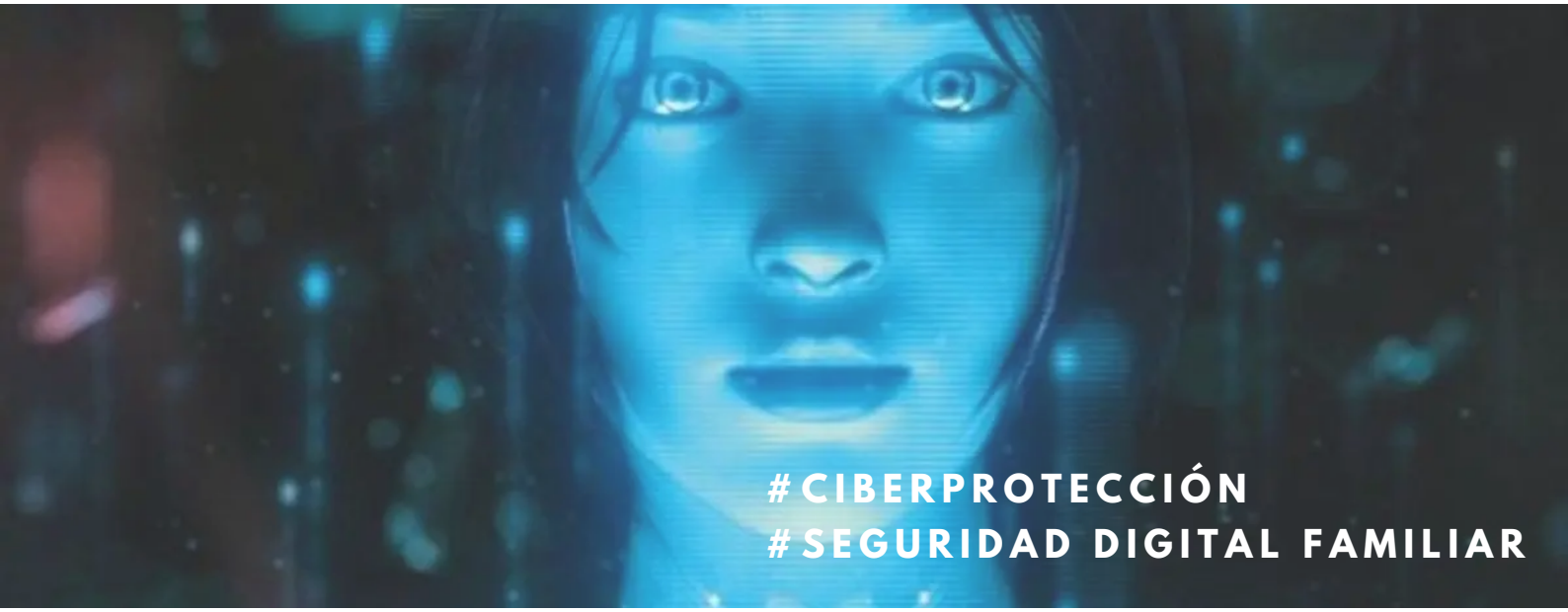
#RIESGOS2021

#EDUCACIÓN DIGITAL
#CIBERPROTECCIÓN

Gaptain
www.gaptain.com

EDUCACIÓN

BIENESTAR



ASISTENTES VIRTUALES. ¿DE VERDAD QUIERES QUE PIENSEN POR TI?

La moda de los asistentes inteligentes o asistentes de voz

¿Eres usuario de pago de Youtube? ¿O de Google One? … En caso afirmativo, seguro que has visto como en los últimos días el propio Google te regalaba uno de sus dispositivos Home Mini. En los últimos meses las redes sociales se han llenado de comentarios sobre este regalo que el gigante tecnológico quería enviar a casa de todo aquel que lo quisiera. Algo que ha levantado también muchos recelos. Porque ya sabemos que "cuando algo es gratis, el producto eres tú".

Y además, si activas tu tan necesario **pensamiento crítico,** enseguida te encuentras con una incoherencia que hace sospechar …´¿No es extraño que el innovador dispositivo estrella que toda persona humana necesitará durante 2020 cueste solo 20 euros?…

Portátil, móvil, Tablet , iWatch, smartTV, ... todos costaban al menos 400 o 500 € cuando salieron, ¿porqué el nuevo dispositivo 2020 se regala? ... Listar aquí las peregrinas respuestas que nuestra conciencia construye para justificar la necesidad de hacernos con uno YA, darían una buena muestra de lo 'inocentes' e 'incoherentes' que somos consumiendo tecnología...
¿Qué se esconde detrás de este regalo? ¿Conocemos realmente lo que implica meter un asistente de voz inteligente en casa?

Un hogar cada vez más conectado

Lavadoras, frigoríficos, televisores, aspiradoras y hasta bombillas. Cada vez es más común que los aparatos del hogar permitan una conexión a Internet a través de una app, bluetooth, wifi... Un mercado emergente que en cinco años se prevé que alcance los más de 150.000 millones de facturación. Y entre los aparatos que más está colonizando los hogares están los asistentes inteligentes.
Permiten hacer consultas de voz, poner alarmas, gestionar aplicaciones móvil y controlar cualquier electrodoméstico o dispositivo electrónico que tengas en el hogar. Algo que aumenta tu comodidad y la de tu familia pero que plantea varios interrogantes...
¿Está la seguridad de estos aparatos IoT garantizada ? ¿me hacen mas vulnerable y dependiente? ¿y a mis hijos también? ¿Invaden nuestra privacidad y derechos fundamentales? ¿recogen la información para luego venderla o para manipularme? ....
No vamos a darte las respuestas, queremos que las encuentres tu.

Piensa en quien es el fabricante, cuales son sus prioridades, su histórico con la justicia y compromiso social, si ha ocultado algo alguna vez a sus usuarios o realizado prácticas abusivas, y si pasa el filtro, ¿qué problema te resuelve? y, ¿es realmente algo que no lo tenías resuelto?.
Considera también si no has pagado ya 20 veces por lo mismo, tecnología que sirve para poner música, llevar tu agenda y contactos, decirte el tiempo que va a hacer, y acceder a internet es demasiado cansino ya,

En mi caso, tengo al menos 5 dispositivos 'que hacen lo mismo' comprados en los últimos 5 años, ¿en qué momento me hicieron pensar que los necesitaba todos? ¿Tengo la casa tan domotizada como para necesitar un asistente que gestione a los demás aparatos IoT?

Enseguida vendrán los teléfonos que se doblan … perdonad la carcajada pero, ¿para qué quiero yo un teléfono que se doble? :-)) pues vendrá alguien a convencernos que nuestra vida depende de lo que se doble tu teléfono, muy pronto.

Personalizando tus experiencias con la marca

Los fabricantes argumentan (tras requerimiento judicial) que en ocasiones graban conversaciones y recopilan información únicamente para personalizar nuestra experiencia con su marca pero, ¿alguien me ha preguntado a mi si quiero que la personalicen? …
Pues por si quedaba alguna duda: NO, no quiero que la personalices. Y SI quiero que dejes de seguirme y grabarme. Me incomoda, y además se trata de un abuso.

"Hola soy tu vecino, vengo a instalar una cámara y un micrófono en tu habitación. No te preocupes, es para personalizar mi saludo a las mañanas en el ascensor …"

Y si nos ponemos un poco más trascendentales, … ¿realmente soy yo el que está decidiendo como quiero que sea mi vida y la de los míos? ¿podría estar poniéndoles en riesgo con algunas de mis decisiones?

Los riesgos de los asistentes inteligentes para el hogar

1. Escucha constante: estos dispositivos son altavoces que graban todo lo que se habla y lo almacenan en sus servidores.
2. Riesgo de hackeo: como cualquier dispositivo conectado a Internet, corre el riesgo de ser hackeado. Los ciberdelincuentes pueden acceder a través de los asistentes y hacerse con el control de toda la casa.
3. Proporcionar información personal: para poder utilizar las funciones de estos asistentes de voz es necesario que introduzcas tus cuentas personales. Dándoles acceso a todo tipo de información privada.
4. Compras no autorizadas: teniendo en cuenta que si acceden al dispositivo pueden tener en sus manos tus datos personales y la gestión de esos mismo aparatos, los hackers pueden llegar a hacer compras con tu dinero.
5. Robos en vivienda: si un delincuente tiene el control de la luz, la alarma...¿Qué le impide entrar en tu vivienda con impunidad?
6. Malware: según estos asistentes van teniendo más presencia en la vida de las personas aumenta el riesgo de que los ciberdelincuentes desarrollen códigos maliciosos que ataquen a estos aparatos. ¿El objetivo? "Secuestrarlos" para pedir un rescate, chantajes...
7. Distinción de voz: estos asistentes aún no pueden distinguir las voces de sus "dueños" de las de otros. Por lo que cualquiera puede usarlos y activar sus comandos.

Dolphins attacks. Ataques diseñados para los asistentes de voz

Existe un riesgo creado específicamente para atacar a los asistentes inteligentes del hogar. ¿En qué consiste?

Los cibercriminales emiten un sonido imperceptible para el oído humano pero que sí lo escuchan estos dispositivos. Este sonido se traduce en un comando de voz que permite robarte la información personal sin que te des cuenta.

¿Cómo evitar estos riesgos?

Si después de considerar todo esto, has decidido que necesitas un asistente de voz inteligente para ayudarte a gestionar tu vida y agenda. Debes tener lo siguiente en cuenta:

1. Lo primero de todo es conocer sus instrucciones de uso y las condiciones de privacidad que estás aceptando.
2. Además, al igual que sucede con las webcams, apaga los micrófonos mientras no los estés utilizando, algunos de los fabricantes ya han tenido que reconocer ante la justicia que están grabando conversaciones privadas de sus clientes.
3. Instala un antivirus siempre que sea posible.
4. Configura el aparato de tal manera que para realizar a través de él cualquier compra se requiera una contraseña.
5. No enlaces la seguridad del hogar con los comandos de voz.

Tener un **hogar conectado** ofrece muchas comodidades. Sin embargo, no debes olvidar los riesgos que entraña para ti y tu familia.
Imprescindible, estar informado/a, invertir en educación digital y tener en mente siempre la ciberseguridad, ... y el pensamiento crítico.

Gaptain es Responsabilidad digital.

CULTURA DE CIBERSEGURIDAD Y ALFABETIZACIÓN DIGITAL

El derecho de acceso universal a Internet de todas las personas

No se trata de una frase hecha, el acceso a internet es un derecho de cada ciudadano. El artículo 81 de la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD), establece que:

1) “Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica”
2) Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población”.

Hoy en día, todo ciudadano lleva un móvil en la mano, y por tanto la posibilidad de enviar mensajes en masa a cientos de miles de personas conectadas entre si a través de internet.

Es por lo que se ha vuelto especialmente importante que los usuarios cotidianos tengamos conocimientos de los medios y canales digitales disponibles para comunicar, y que comprendamos las consecuencias de las acciones que se ejecutan en la red, así cómo la forma en que funciona la tecnología, las redes sociales, las apps, los asistentes de voz ….

Para cubrir esta necesidad nace el término alfabetización mediática, y con él soluciones de capacitación como Segureskola,, o el itinerario formativo para familias ‘‘educando en digital‘ , recientemente presentado por Gaptain.

¿Qué es la alfabetización digital o mediática?

La alfabetización mediática es la capacidad de acceder, analizar, crear y actuar utilizando todas las formas de comunicación. Desde interpretar emojis, hasta comprender los mensajes subliminales en anuncios, producir vídeos virales o reconocer la publicidad nativa.

Muchos usuarios no son conscientes del impacto de sus acciones en el ámbito digital en los demás, ni de los susceptibles que somos a la manipulación por parte de los medios digitales.
Por eso es importante disponer de una cultura de ciberseguridad que nos permita educar desde edades tempranas en un uso seguro y saludable de la tecnología, aprender a navegar, encontrar la información que buscamos de forma fluida, a crear y compartir contenido, y por supuesto a identificar la información que pudiera ser falsa de la verdadera.

¿Recuerdas la polémica que trascendió tras las anteriores elecciones americanas donde se descubrió que se había manipulado información y noticias para favorecer al candidato Donald Trump?.
En ese momento se popularizo el término “fake news”, o noticias falsas que pasan por verdaderas con el objetivo de confundir la opinión de las personas, y que puso en la palestra la manipulación de pensamiento que sufrimos los ciudadanos a través de canales digitales.

Las 5 premisas de la alfabetización digital

Según la UNESCO existen 5 derechos fundamentales de todo ciudadano digital que se deben preservar en la nueva sociedad digital:

- La información, y los medios que la transmiten, deben estar disponibles para toda la ciudadanía, sin exclusión de colectivos o comunidad alguna.
- Todo ciudadano debe saber crear contenido y compartirlo con los demás, ya que todo el mundo tiene derecho a comunicarse y expresarse.
- La información no siempre es neutral, ni procede de fuentes independientes o fiables. La aplicación de la alfabetización mediática debe hacerse según los principios de fiabilidad y accesibilidad para todos los ciudadanos.
- La capacidad de acceso y comprensión de la información, o a la comunicación, no pueden verse comprometidos bajo ningún concepto.
- La alfabetización mediática es un aprendizaje continuo de cada ciudadano, y resulta mucho más completo cuando incluye conocimientos, habilidades y aptitudes, además de acceso y cobertura a los medios de comunicación.

Pero, ¿Cómo podemos sentar estas bases y transferir estos conocimientos a los ciudadanos de la sociedad digital?

La cultura de ciberseguridad y la alfabetización mediática

Los padres y educadores necesitan estar capacitados y tener instrumentos para enseñar a los niños y niñas a hacer un uso seguro y responsable de los medios de comunicación digitales, y la tecnología en general.

En países como Finlandia ya se ha incluido en sus modelos educativos la alfabetización mediática con el objetivo de que los menores desarrollen tres habilidades principales:

1. **Pensamiento crítico:** la observación e interpretación nos permite cuestionar la norma y reinterpretar los mensajes cotidianos, favoreciendo tomar decisiones inteligentes.
2. **Autoexpresión:** estudiar cómo los demás transmiten los medios para comunicar mensajes o emociones ayuda a conceptualizar y producir contenidos propios. Conocer lo que funciona, inspira la creatividad.
3. **Responsabilidad digital:** los jóvenes de hoy serán los encargados en el futuro de crear y difundir los contenidos a través de los medios digitales.

Por eso deben interiorizar unas bases éticas de comportamiento que garanticen la **convivencia en el ámbito digital.**
Además de esto, se hace imprescindible capacitar a la ciudadanía con **competencias digitales** que les permitan usar de forma saludable la tecnología, y garantizar su propia seguridad en el entorno digital.

Conocer en profundidad la tecnología es necesario frente a las manipulaciones de pensamiento y abusos tan habituales en este ámbito. Es una batalla colectiva en defensa de la libertad individual y contra la manipulación de pensamiento, que finalizará cuando consigamos que en la sociedad impere cultura de ciberseguridad y pensamiento crítico. y los ciudadanos tengamos un papel activo y responsable sobre la información que consumimos.
No es tarea fácil, sin duda. Pero ya estamos en el camino.

CÓMO HACER QUE TU COLEGIO APRUEBE EN MATERIA DE PROTECCIÓN DE DATOS

Los centros educativos y la protección de datos, un binomio posible y necesario

Los retos a los que nos enfrentamos en nuestro mundo con la digitalización de la educación son enormes. La falta de medios y en algunos casos de formación, hace que a veces sea complicado aunar una educación digital o mixta, con el cumplimiento de la normativa en protección de datos.

Pero debemos entender, que ambos conceptos deben ir juntos ya que la protección y los intereses de los/as menores están por encima de cualquier otra discusión. Y tanto, tienen derecho a una educación de calidad, como a que sus datos personales estén protegidos.

Desde el Reglamento General de Protección de Datos, se obliga a las administraciones y centros educativos a cumplir ciertos requisitos para proteger los datos de carácter personal que se tratan en estos lugares.

La Agencia Española de Protección de Datos ha creado diversas guías e infografías que nos pueden ayudar a comprender mejor las obligaciones que tenemos como centro educativo en materia de protección de datos.

También, se puede optar por el **programa Segureskol**a, que ofrece un itinerario completo de acompañamiento al centro educativo en su adaptación a un mundo digital seguro. Además, nos permite cumplir con el concepto de proactividad que exige el nuevo Reglamento General de Protección de datos.

Qué debes tener en cuenta para cumplir con la Ley de protección de datos

Sabemos que a veces complicado cambiar procesos que tenemos altamente interiorizados y mecanizados en nuestro día a día. Comprender cómo poner en práctica los cambios que nos exigen, no es tarea sencilla.

Por ello, vamos a intentar proponer algunos puntos básicos en los que incidir en los centros educativos para que el cumplimiento de las leyes en materia de protección de datos sea más comprensible y sencillo de implementar.

Medidas para tener un ’10’ en protección de datos.

1. El personal del centro debe tratar los datos de carácter personal del alumnado y de sus familiares con cuidado y respeto por la privacidad e intimidad, y siempre teniendo presente el interés y la protección de los menores.

2. Las Administraciones y centros educativos como responsables del tratamiento de los datos, deben ofrecer formación continua sobre los principios básicos y cómo tratar correctamente los datos de carácter personal.
3. En general, los centros educativos no necesitan el consentimiento de los titulares ya que está justificado en el ejercicio de la función educativa y en la relación ocasionada con las matrículas de los alumnos. Pero siempre se ha de informar de forma sencilla de:
a) La finalidad para la que se recaban los datos y su licitud.
b) La obligatoriedad o no de facilitar los datos y las consecuencias de negarse a utilizarlos.
c) Los destinatarios de los datos.
d) Los derechos de los interesados y cómo ejercitarlos.
e) La identidad del responsable del tratamiento: la administración educativa o el centro.
f) Además se debe facilitar a los titulares de los datos cuando se recaben de ellos mismos: los datos de contacto del delegado de protección de datos y el plazo de conservación o los criterios para determinarlo.
4. Cuando se deba obtener el consentimiento de los alumnos o de sus progenitores o tutores para utilizar sus datos personales con finales distintas de la función educativa, se debe informar con claridad de cada una de ellas, posibilitando ejercer el derecho a oposición de los interesados.
5. Se deben conocer las aplicaciones TIC que se van a utilizar, la política de privacidad y sus condiciones de uso, antes de ponerlas a disposición del personal docente o del alumnado. Aquellas que no ofrezcan garantías, o información, sobre el tratamiento de los datos personales que realizan, deben ser descartadas.
6. Las administraciones educativas y los centros, deben disponer de protocolos, guías, directrices o recomendaciones sobre el uso de las TIC. Los profesores, deberán utilizar las que las administraciones o el propio centro educativo hayan dispuesto para cada caso de uso, adaptándose cada una de ellas al grado de desarrollo del niño/a.

7. Las comunicaciones entre el profesorado, los progenitores y el alumnado deben realizarse preferentemente a través de los medios recomendados por el centro educativo, por ejemplo: plataformas educativas, correo electrónico, aplicación móvil del centro, etc.
8. El uso de aplicaciones de mensajería instantánea, como por ejemplo WhatsApp, para mantener comunicaciones entre el equipo docente, los progenitores y el alumnado, no es recomendable. En el caso de que el interés superior del menor estuviere comprometido, como por ejemplo, cuando ocurre un accidente o indisposición a un alumno/a en una excursión y con la finalidad de tranquilizar a los progenitores o a los titulares de la patria potestad, se podrán captar imágenes y enviárselas.
9. El profesorado debe enseñar a sus alumnos/as a valorar la privacidad tanto de uno mismo/a como la de sus compañeros/as con instrucciones como por ejemplo:
a) no tomar fotos, ni grabar audios o vídeos de sus compañeros/as , ni del personal del centro escolar sin su consentimiento;
b) utilizar la empatía y el ponerse en el lugar del otro siempre antes de publicar o compartir cualquier contenido en las redes sociales;
c) animarles a no participar en conversaciones en las que se incite a la violencia o al acoso, contra otras personas o colectivos. Incluso, apoyarles para que lo comuniquen a alguna persona adulta y que de esta manera se pueda frenar la situación en la medida de lo posible;
d) si reciben mensajes o comentarios que les molestan o que les hacen sentirse mal, incluso toques o mensajes en sus teléfonos o tablets a horas intempestivas, que sepan detectar qué eso es acoso. Instarles a que deben contarlo a alguna persona que pueda ayudarles como sus progenitores, profesores/as, etc.;
e) apagar el gps, wifi y bluetooth de los dispositivos cuando no se estén utilizando;
f) tapar la cámara de sus dispositivos cuando no la estén usando;
g) cuando se vaya a instalar una nueva aplicación, revisar los permisos que nos pide dicha aplicación y en caso de que los consideremos inapropiados o excesivos, no instalar dicha aplicación.

10. Los centros educativos suelen organizar actividades a las que suelen asistir familiares de los alumnos/as, como por ejemplo fiestas de fin de curso, graduaciones, eventos deportivos, etc. En estos casos, sería conveniente por ejemplo: solicitarles la autorización para participar, o avisar mediante carteles de la posibilidad de grabar o tomar imágenes exclusivamente para uso personal o doméstico.

Espero que estos tips os sirvan para comprender un poco mejor la importancia de la protección de datos en la educación.

Los que nos dedicamos a este sector, sabemos muy bien que las adaptaciones a la normativa, pueden ser difíciles al principio. Pero el esfuerzo, merece la pena, os lo aseguro.

EL INTERNET DE LAS COSAS (IOT) EN EL HOGAR

Quizá hayas empezado alguna frase con «Oye, Siri», «OK Google» o «Alexa» ya que el denominado Internet de las cosas (IoT) está creciendo exponencialmente.
Es un término que suena cada vez con más frecuencia pero, ¿sabes en que consiste el IoT? ¿qué nos puede aportar? ¿tiene riesgos que tengamos que conocer?. Vamos a intentar explicar todos esto en las siguientes líneas.

¿Qué es el Internet de las cosas (IoT)?

Cualquier dispositivo o aparato que pueda conectarse a Internet se puede considerar IoT. En función del uso que le demos a esos dispositivos podemos hablar de hogares, industrias o incluso ciudades inteligentes.
El IoT crece día a día con nuevos dispositivos, ya no sólo se conecta a Internet nuestro móvil, tablet u ordenador, también lo hacen las cerraduras, televisores, pulseras de ejercicio, tostadoras, neveras, cafeteras, bombillas, alarmas, detectores de humo, cámaras de seguridad, enchufes, relojes, termostatos, altavoces inteligentes...

Son dispositivos que pueden hacernos la vida mucho más fácil o más divertida. Imagina que te despiertas poco a poco y con tu música preferida, en la cocina tienes tu café preparado y se ha puesto en marcha la calefacción un poco antes para que la temperatura sea perfecta. A la hora que quieras puedes tener la comida preparada sólo con añadir los ingredientes a tu robot de cocina y, mientras estás fuera, tienes otro aparato que limpia la casa para que esté perfecta cuando vuelvas.
Y no sólo eso, cuentas con una pulsera de actividad que te pone retos para mantenerte en forma y enchufes que encienden y apagan los electrodomésticos cuando no estás para que consuman menos energía y ahorres algo de dinero, ¿no te gustaría?.

Con el IoT tenemos todo esto y mucho más al alcance de nuestra mano y no es algo futurista, podemos encontrarlo ya y a un coste bastante accesible

¿Cómo funcionan estos dispositivos?

Y ¿qué diferencia un objeto cotidiano como una bombilla normal de uno con IoT como una bombilla inteligente?. Para que una bombilla u otro objeto pueda conectarse a Internet e incluso comunicarse con otros dispositivos de nuestro hogar necesita de un sensor. En función del tipo de sensor que incorporen, el dispositivo podrá recoger información, transmitirla o realizar alguna acción.

Por ejemplo, podemos tener sensores que si detectan algún movimiento en nuestra casa cuando no estamos nos envíen un mensaje a nuestro móvil o se pongan en contacto con una empresa de seguridad, o dispositivos que nos avisen si llevamos mucho tiempo sentados o nos preparen un plan de ejercicios basado en nuestra actividad física.
Además, podemos unir varios de esos dispositivos y permitirles que se comuniquen entre ellos sin necesidad de nuestra intervención creando un hogar inteligente. Así, podríamos tener un termómetro que mida la temperatura de nuestra casa de forma que si baja de cierto valor se comunique con la calefacción y la encienda.

5 riesgos de los dispositivos IoT

Ya hemos visto que los dispositivos IoT pueden ayudarnos de muchas formas pero no debemos olvidarnos de que también pueden suponer una amenaza en diferentes aspectos.
En función del dispositivo podemos hablar de unos riesgos u otros, veamos los más habituales:

Problemas de privacidad
Una de las amenazas más importantes de los dispositivos IoT hace referencia a la privacidad. Para que estos dispositivos funcionen bien y sean eficaces tienen que recoger muchos datos. Por ejemplo nuestra cerradura inteligente sabe en qué momento llegamos a casa, cuando nos vamos, cuantas visitas recibimos... un altavoz sabe la música que escuchamos, el televisor nuestros gustos y aficiones, el robot aspirador conoce en detalle nuestra casa y su distribución y nuestra pulsera de actividad conoce incluso cuanto tiempo dormimos.

Todos esos datos se envían a los proveedores de esos dispositivos para que los traten e incluso algunos los comparten (o venden) con terceros. En los últimos años se ha descubierto que algunos televisores, robots de cocina, altavoces inteligentes e incluso juguetes grababan conversaciones que luego enviaban al fabricante.

Amenazas de seguridad y malware
Si hablamos de dispositivos conectados a internet tenemos que tener en cuenta que cualquiera de ellos puede ser atacado y, si un dispositivo es atacado puede poner en peligro toda nuestra red de casa ya que en la mayoría de los casos se conectan a través de la red Wifi.
Es probable que en tu ordenador o en tu teléfono móvil tengas instalado un antivirus pero, ¿tienes algún tipo de protección para tu televisión inteligente, para tu pulsera de actividad o para la cerradura inteligente de tu casa?.

Y no sólo eso, estamos acostumbrados a que nuestros ordenadores y dispositivos móviles se actualicen de forma regular. Quizá nos resulte molesto pero estas actualizaciones suelen tapar fallos de seguridad o solucionar problemas que se van detectando con el uso. Sin embargo, con muchos de los dispositivos IoT no tenemos esas actualizaciones con lo que su seguridad se va degradando con el paso del tiempo.
Además, como el IoT es cada vez más popular, muchos hackers han comenzado a desarrollar software diseñado para atacar a los dispositivos inteligentes porque, como decíamos, no suelen prestar demasiada atención a la seguridad y acceden a mucha información personal.

Robos
Como hemos comentado muchos dispositivos inteligentes almacenan mucha información que puede ponernos en riesgo. Una cerradura o un sistema de seguridad tiene información sobre nuestros movimientos, conocen nuestra rutinas y saben cuando estamos en casa y cuando no. En incluso con otros dispositivos se puede conocer la distribución de la casa en detalle y los objetos alojados en ella. Imaginemos si esos datos son interceptados por personas que quieren robar en nuestra casa.

Además, algunos dispositivos pueden llegar a almacenar nuestras contraseñas, documentos de identidad, datos de tarjetas de crédito... si esos datos no están cifrados o almacenados de forma correcta podrían suponer un problema importante para nuestra economía.

Secuestro de dispositivos
Cada vez se oyen más casos de secuestro de dispositivos IoT en los que los hackers se hacen con el control de diferentes dispositivos para causar algún problema de seguridad o para pedir un «rescate» económico que permita recuperar el control de los aparatos.
Se han conocido casos de toma de control de cámaras, amenazas de secuestros a menores, comunicaciones de desconocidos por medio de altavoces inteligentes, toma de control de termostatos e incluso aperturas automáticas de cerraduras.

Problemas con los comandos de voz
Muchos de los dispositivos IoT están configurados para que les podamos dar órdenes a través de los comandos de voz. Es algo que puede resultar muy útil pero a la vez muy peligroso. Un comando de voz es susceptible de ser reproducido por ejemplo por un ordenador con lo que tenemos que tener cuidado.

Recientemente se han conocido casos de cerraduras inteligentes que se comunicaban con altavoces inteligentes para que, mediante comandos de voz, se pudieran abrir y cerrar. Algo que puede resultar interesante siempre que no se pueda acceder a ese altavoz por otro medio, ¿verdad?.

¿Cómo podemos evitar los riesgos?

- Mantener los dispositivos y los controladores actualizados.
- Poner contraseñas seguras para acceder a los dispositivos. Estas contraseñas no deberían tener datos personales y deberíamos cambiarlas con cierta frecuencia.
- Si disponen de doble factor de autentificación o opciones de acceso biométrico es recomendable activarlos.
- Protegerse nuestra red y los dispositivos que lo permitan con antivirus y antimalware.
- Antes de comprar estos dispositivos verificar si el fabricante proporciona actualizaciones de seguridad y la política de protección de datos personales que tiene.

Tener un hogar inteligente nos ofrece muchas comodidades pero no olvides los riesgos que puede entrañar para ti y para tu familia.

Si quieres estar siempre informado/a y formado/a, puedes ayudarte con el **programa online para familias** "Educando en digital".
En formato vídeo tutorial , diseñado por expertos para toda la familia.
Lo podrás consultar cuando y donde quieras.
.

¿CUIDAS TU IDENTIDAD DIGITAL?

Debemos mantener saludable nuestra identidad digital

Quizás somos poco conscientes de la importancia que tiene actualmente nuestra identidad digital y más en un mundo en plena digitalización y en el que debido a la pandemia los eventos y las reuniones presenciales se han reducido a la mínima expresión.
¿Has puesto tu nombre y apellido en Google? ¿Qué huella digital aparece?

Quizás tu Facebook, tu perfil de Instagram, tu cuenta de Twitter o LinkedIn, tu blog... cuando cambias de pestaña y solicitas imágenes, videos, noticias... la información que aparece ¿proyecta una imagen que encaje con tu propósito, valores, que genere confianza y profesionalidad?

¿Te puede ayudar a conseguir nuevos proyectos de negocio o empleo?
Te animo a mirar este video que hice para CaixaBank de 1 minuto en el que hablo de ello

Trabajar la marca personal

Se decía lo de “el conocimiento es poder”. Ahora por el contrario, “somos lo que compartimos”, debemos trabajar nuestra marca personal aportando contenido de valor mediante un buen artículo en una revista del sector, una entrevista en un podcast, una frase interesante en Instagram, un artículo en un periódico, etc. para ganar visibilidad en un entorno VUCAH y de carreras líquidas, como decía Bauman, de lo contrario, nos será mucho más difícil conseguir encadenar proyectos en un paradigma laboral en el que el “trabajo para toda la vida” ha quedado para unos pocos casos.

Es más, los programas de “Embajadores de Marca» o employee Advocacy que estamos fomentando en las organizaciones, ponen en valor esta identidad digital y todo el capital social que tenga el empleado, para ayudar a promocionar su carrera profesional y desde una visión win-win, ayudar a atraer clientes o talento a la empresa.

La huella digital de los jóvenes puede condicionar su futuro

¿Enseñamos esto a nuestros hijos? ¿Les hablamos de que toda esa huella digital pude ser revisada el día de mañana por un reclutador cuando busquen empleo?

Los jóvenes millennials y la Generación Z están acostumbrados a compartir información en redes sociales como Instagram, Wahtaspp, TikTok... pero eso no significa que lo hagan con conciencia de que están sembrando 0 y 1 que les pueden ayudar o frenar en sus vidas.

El curriculum social

Propongo que desde los distintos ámbitos (familiar, educativo, político, social...) se ayude a estas nuevas generaciones a cuidar su currículum social (CV Social) porque tendrá tanto o más peso que el currículum en PDF que enviamos a las ofertas de empleo.

De hecho, la selección sin oferta publicada y sin CV enviado, o sea, captación de talento por parte de seleccionadores que buscan en LinkedIn, Twitter, Instagram... en formato nethunting, está aumentando al igual que el cambio de modelo de comprador que es más proactivo informándose, consultando las opiniones en Amazón, Google, foros de opinión... en lugar de ser un comprador pasivo que se deja asesorar por el vendedor, luego, vuelve a ser muy importante, si el día de mañana nuestros hijos/as son emprendedores o empresarios y quieren ganar clientes/ventas, que sea buena, su marca digital. ¿No? ...

Educando en digital

Desde Gaptain, esperamos de corazón haberte ayudado en algo con este eBook. Puedes contactar con nosotros en el buzón: **info@gaptain.com**, y recuerda, "***la mejor prevención es la educación***":

Mira ahora el Itinerario online para Familias "**Educando en digital**", te encantará.

Gaptain
www.gaptain.com