CLUB DE EXCELENCIA EN
SOSTENIBILIDAD

CLUBSOSTENIBILIDAD.ORG

Guía sobre el
USO RESPONSABLE DE LA TECNOLOGÍA
EN EL ENTORNO FAMILIAR

orange™

S2 GRUPO

Por un uso Love de la tecnología

Índice

Consejo Asesor

Juan Alfaro
Club de Excelencia en Sostenibilidad

Juan Pablo Barrios
SEAT

Francisco Alfonso Batuecas
Ministerio del Interior – Subdirección General de Sistemas de Información y Comunicación para la Seguridad

María Eugenia de Blas
Orange

Guillermo Cánovas
EducaLike

José María Chiquillo
Diputado del Congreso

Ana Gómez Blanco
BBVA

Valle Jiménez Cristobal
S2 Grupo

Rosa Kariger
Iberdrola

Rocío Miranda de Larra
Orange

Andrés Nuñez Baroja
S2 Grupo

José Rosell
S2 Grupo

Ana Belén Santos Pintor
Instituto Nacional de Ciberseguridad (INCIBE)

José Manuel Sedes
Vodafone

Victor Suárez
Orange

Alejandro Javier Tosina
RED.ES

Alicia Vicente,
Unidad Técnica de Policía Judicial de la Guardia Civil

Prólogo

ORANGE

Cuando hace unos meses nos reunimos con el Club de Excelencia en Sostenibilidad para analizar la posibilidad de elaborar una guía destinada al público empresarial y que tratase un tema de actualidad en el ámbito de la RSC, no pestañeamos dos veces. Esa guía tenía que hablar del papel que juega la tecnología en la vida de niños y jóvenes y, más concretamente, de las oportunidades que ofrece y los mecanismos que pone a nuestra disposición para prevenir los posibles riesgos derivados de su uso.

Tendemos a pensar que es un debate limitado a padres y educadores, e incluso al sector público, pero ¿acaso no son los empleados de una empresa padres, tíos, voluntarios y, en definitiva, ciudadanos? Las empresas no podemos mantenernos al margen de las preocupaciones sociales. En Orange pensamos que es responsabilidad de todos facilitar que los menores y adolescentes hagan una incorporación positiva de la tecnología y favorecer un buen uso de la misma.

Como operador de referencia que somos, estamos convencidos de que nos compete ocuparnos del uso que niños y adolescentes hacen de las tecnologías digitales, así como de su potencial para su desarrollo intelectual y social. En este aspecto, afrontamos un desafiante reto: conseguir que el alumnado pase de ser mero consumidor de contenido a tener un papel activo en el desarrollo de la tecnología. Por eso, en los últimos años hemos lanzado numerosos proyectos e iniciativas destinados a ofrecer pautas a padres y educadores para fomentar una utilización positiva de la tecnología.

En el ámbito educativo, en 2014 lanzamos Educainternet, www.educainternet.es, una plataforma destinada a que los profesores se formen en el uso seguro y responsable de la tecnología y puedan compartir buenas prácticas sobre este buen uso con sus alumnos. Gracias a esta plataforma se han formado más de 1.700 profesores, se han creado 14.000 recursos educativos digitales, y cuenta con más de 3.700 profesores registrados.

En el entorno familiar, el programa “Por un uso Love de la tecnología”, www.usolovedelatecnologia.com, a través de vídeos centrados en temáticas de interés como el *ciberbullying*, *sharenting*, la gestión de las pantallas, etc. pretende sensibilizar y generar debate en el seno familiar para que, juntos, aprendan a hacer un uso responsable de la tecnología. En los primeros seis meses de programa, ha sumado ya más de ocho millones de visualizaciones.

En este mismo escenario, *FamilyON* contiene una serie de actividades para que la familia adquiera competencias digitales y disfrute junta de la tecnología.

Y en el campo del voluntariado hemos formado a más de 450 empleados, que han dado charlas de sensibilización a más de 18.000 alumnos.

Con esta guía pretendemos dar un paso más e introducir esa reflexión en el ámbito empresarial, mostrando una serie de buenas prácticas, que esperamos sirvan para ampliar el debate y que se conviertan en fuente de inspiración para que, entre todos, acompañemos a nuestros niños y jóvenes a desarrollarse plenamente en esta Era Digital en la que les ha tocado vivir.

Rocío Miranda de Larra
Directora de RSC y Sostenibilidad en Orange España

1

La tecnología en los hogares españoles

La tecnología y el acceso a Internet forman parte indispensable de nuestra vida y actos cotidianos, del mismo modo que también están presentes en los niños desde edades cada vez más tempranas.

Vivimos en un nuevo entorno, el digital, que nos facilita la gestión de las actividades cotidianas, el entretenimiento, el aprendizaje y la comunicación.

A los más pequeños les proporciona juguetes inteligentes, gafas de realidad virtual, consolas y todo tipo de gadgets. El uso de Internet y, sobre todo, de los ordenadores, móviles, tabletas, etc., se ha convertido en una práctica mayoritaria entre los menores con edades inferiores a los 10 años.

Las posibilidades de conexión son cada vez más variadas y lo seguirán siendo, la tecnología e Internet evolucionarán, pero no se marcharán, están aquí para quedarse. Esto supone un nuevo reto para las familias: la educación digital.

Los padres tienen que ser conscientes de que a medida que avanza la tecnología y las oportunidades de conexión, nuestras interacciones cambian, se generan nuevas experiencias y a la vez, pueden surgir nuevas amenazas.

La sociedad digital nos adentra en un futuro que muchas veces escapa a nuestra imaginación y nos obliga a estar en un proceso continuo de aprendizaje, protección, actualización, y comunicación eficaz entre todos los miembros de la familia.

1.1. SOCIEDAD DIGITAL: NATIVOS, INMIGRANTES Y AGNÓSTICOS DIGITALES

La sociedad, en términos digitales, está principalmente compuesta por tres miembros diferentes: nativos, inmigrantes y agnósticos digitales.

LOS NATIVOS DIGITALES

Los nativos digitales son todas aquellas personas que han nacido y se han formado rodeados de tecnología utilizando la particular "lengua digital" de juegos por ordenador, vídeo e Internet.

Los nativos digitales están inmersos desde su nacimiento en la tecnología y en las nuevas formas de acceder y procesar la información que estas propician. Han nacido rodeados de ordenadores, tabletas, móviles, etc., que les han permitido establecer ese entorno digital como su hábitat natural. Esta familiaridad con el mundo digital genera en los nativos, una **habilidad innata del lenguaje y uso del entorno digital.**

%	Habitación privada	En casa/otra habitación	Escuela	Otros lugares	En trayectos
Ordenador de sobremesa	10	11	9	4	2
Ordenador portátil	30	26	13	4	2
Teléfono móvil (no Smartphone)	6	4	1	3	3
Smartphone	68	57	10	44	79
Tableta	24	25	1	6	5
E-book	1	0	0	0	0
Otro dispositivo portátil	5	3	1	2	4
Consolas domésticas	6	6	0	3	3
Acceso por lo menos una vez al día	45	64	15	14	15

Encuesta de dispositivos utilizados por los menores para conectarse diariamente desde diversos lugares
Fuente: *Informe Net Children Go Mobile: Risk and Opportunities*

La **tecnología ocupa un lugar central en sus vidas** y se hace omnipresente según van creciendo. Sus actos cotidianos dependen de esta, la usan para entretenerse, estudiar, informarse, comunicarse, comprar o divertirse. Publican todo a sus contactos en la red y sin ser del todo

conscientes, van construyendo su propio **"yo digital"**. Una **"identidad digital"** que se alimenta de las interacciones con los demás a través de la red y de su repercusión (likes, comentarios a sus publicaciones, etc.), que irá formando su **"reputación digital"**, tan o más importante que su reputación *offline*, especialmente en la etapa adolescente.

Pero los nativos digitales no dejan de ser menores, niños, que en esta sociedad digital son una **población especialmente vulnerable** por las características inherentes a su edad: curiosidad innata, confianza excesiva, ansia por experimentar o el miedo a denunciar por si les pueden regañar.

Estos rasgos conducen a los menores a navegar con fluidez por la red, simultaneando tareas, abriendo enlaces y/o descargando toda la información que se les ofrece sin analizar, subestimando, e incluso, sin ser conscientes, de los riesgos que pueden encontrarse en Internet. En ocasiones, por miedo a la represalia de los padres o por vergüenza, no son capaces de comunicar cuando han sido víctimas de alguna de las amenazas existentes en la red, motivo por el que se hace fundamental el **apoyo de la familia en la era digital.**

Otra peculiaridad de los nativos digitales es el **acceso al conocimiento**. Muchos de los valores y conocimientos que tradicionalmente se han transmitido de generación en generación en un entorno doméstico, se han traslado a las redes sociales donde se promueven otros valores y se incita a realizar conductas que escapan al control parental. Se puede tomar como ejemplo de esta afirmación a los *youtubers*, cuyos vídeos y mensajes son vistos por millones de seguidores y tienen un enorme impacto entre niños y adolescentes, que acaban condicionando muchos de sus comportamientos dentro y fuera de la red.

La **cantidad de información que ofrece Internet** hace que los nativos digitales encuentren rápidamente respuesta a todas sus dudas, en ocasiones, sin conocimiento de sus padres y sin serconscientes de que están expuestos a páginas webs falsas, contenido inapropiado o información distorsionada.

LOS INMIGRANTES DIGITALES

Por otro lado, aquellos que han nacido con anterioridad a la eclosión tecnológica pero que conviven en la sociedad digital actual y han tenido que adaptarse a estos nuevos escenarios digitales son los denominados "inmigrantes digitales", nomenclatura en la que podríamos incluir a una parte de los padres de hoy en día.

Podemos afirmar que son la **generación predigital que proviene del mundo analógico.** A diferencia de sus hijos, han visto cómo ha evolucionado la tecnología y la comunicación a través de Internet introduciéndose en sus vidas. Además, algunos de los inmigrantes digitales desconocen los nuevos códigos de lenguaje y escritura de los nativos digitales, comúnmente compuestos por signos y abreviaturas.

Los inmigrantes digitales han tenido que adaptarse progresivamente a medida que ha avanzado la tecnología y se ha impuesto la sociedad digital.

Uno de los rasgos diferenciales entre los inmigrantes digitales y los nativos está en la **dependencia considerablemente menor de la tecnología**, especialmente en lo referente a las relaciones interpersonales y la necesidad de compartir cada instante en las redes.

Su **"yo digital" no es tan fuerte** ni tan determinante como el de los nativos, que muchas veces, dan más importancia a su identidad digital que a su identidad física.

La manera de convivir con la tecnología e Internet y la influencia sobre ellos, marca la distancia entre nativos e inmigrantes digitales.

LOS AGNÓSTICOS DIGITALES

Por último, la sociedad digital recoge dentro de sus miembros a los agnósticos digitales, que al igual que los inmigrantes digitales no han nacido ni se han formado en la era digital, pero a diferencia de éstos últimos, los agnósticos digitales no tienen interés en adaptarse a la tecnología, no ven necesario transformar sus hábitos analógicos en digitales llegando incluso a renegar de ella.

Es importante destacar que los principales perfiles digitales descritos suelen determinar el uso de Internet y los dispositivos con los que prefieren conectarse.

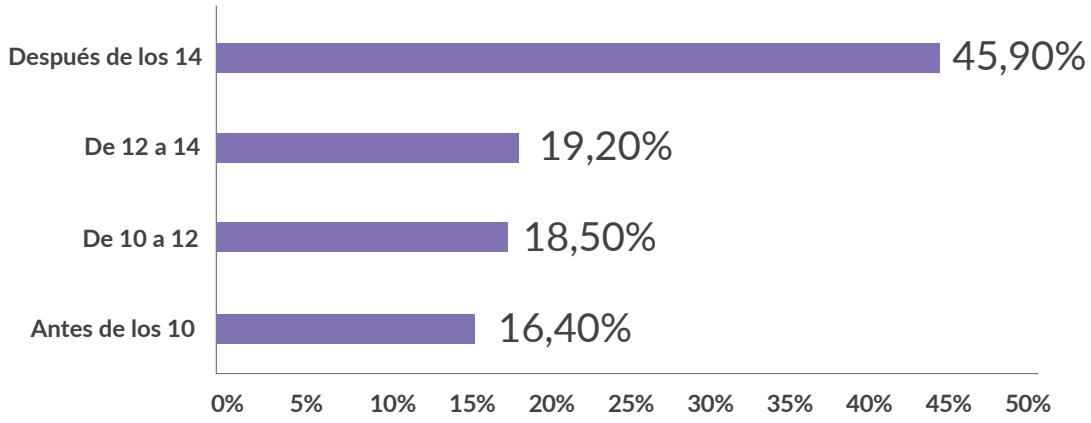
1.2. ACCESO A INTERNET Y USO DE LAS TIC EN LOS MAYORES DE 16 AÑOS

El uso de Internet en los hogares españoles es toda una realidad. Más de 13 millones de viviendas familiares tienen acceso a Internet, de hecho, dos de cada tres personas lo utilizan a diario.

En esta franja de edad, destacan los menores en su etapa final de la adolescencia, que afirman hacer un uso diario de Internet al tener un móvil o tableta propios para su uso privado.

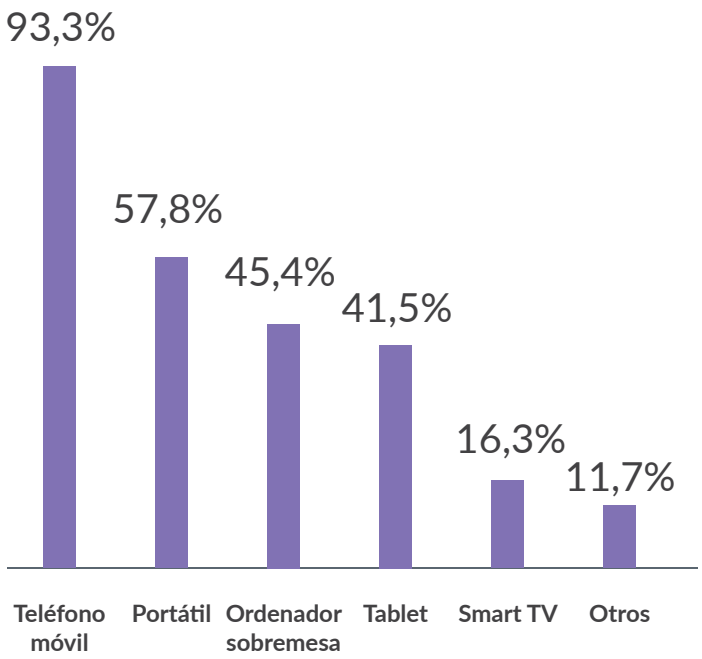
Esta realidad ha traído como consecuencia que el uso de Internet esté extendido, bien sea para ver vídeos, películas, realizar compras online, utilizar redes sociales o realizar cualquier otra acción. Además, la mayoría de las personas mayores de 16 años que se conectan a Internet utilizan el móvil como dispositivo principal (93,3%). Por detrás de él se sitúa el portátil, ordenador de sobremesa, tableta y otros dispositivos como la TV.

¿A qué edad ha tenido tu hijo su primer smartphone?



Propiedad de dispositivos móviles por edad / Fuente: Hijos Digitales

Dispositivos utilizados para conectarse a Internet



Dispositivos utilizados para conectarse a Internet / Fuente: INE

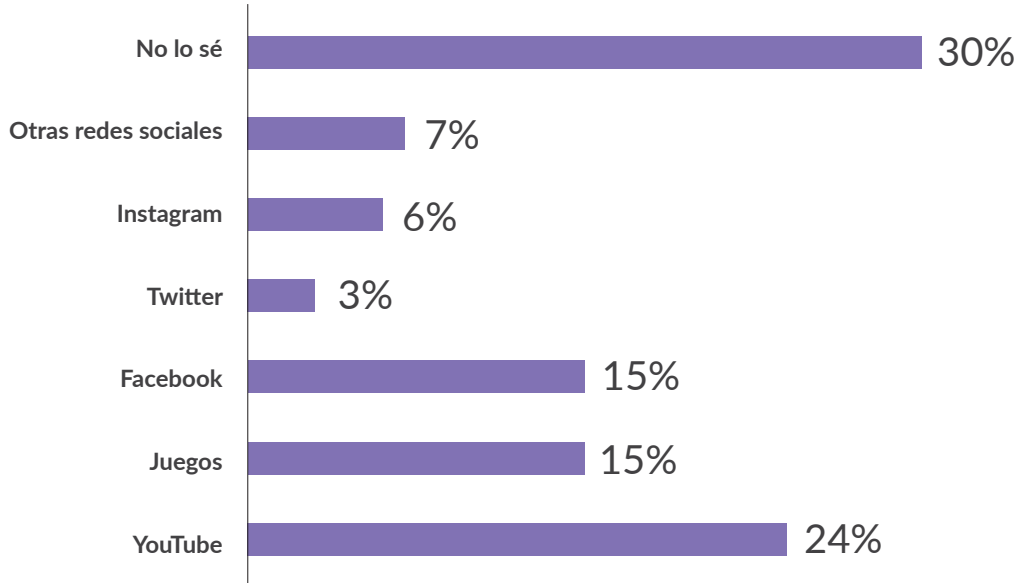
1.3. ACCESO A INTERNET Y USO DE LAS TIC EN LOS MENORES

El uso de Internet, así como del ordenador, móviles, tabletas, etc., se ha convertido en una práctica mayoritaria entre los menores, siendo cada vez más temprana la edad de acceso. De hecho, son cada vez más los menores que a partir de los **10 años tienen teléfono móvil propio, siendo los 15 años** la edad en la que casi la mitad de la población dispone de su primer teléfono móvil.

Hoy en día, **el 95,2% de los menores utiliza Internet**, habiéndose convertido este hábito en una rutina diaria; el 29% de los menores indica que dedica **más de 10 horas a la semana a Internet,** y lo hacen sobre todo para visualizar vídeos de Youtube, consultar sus redes sociales o jugar a los diferentes juegos online.

A pesar de que la mayoría de padres son conocedores de esta actividad por parte de sus hijos, existe un porcentaje (30%) que **desconoce el uso que realizan sus hijos de Internet.**

¿Qué hace tu hijo cuando está en Internet?



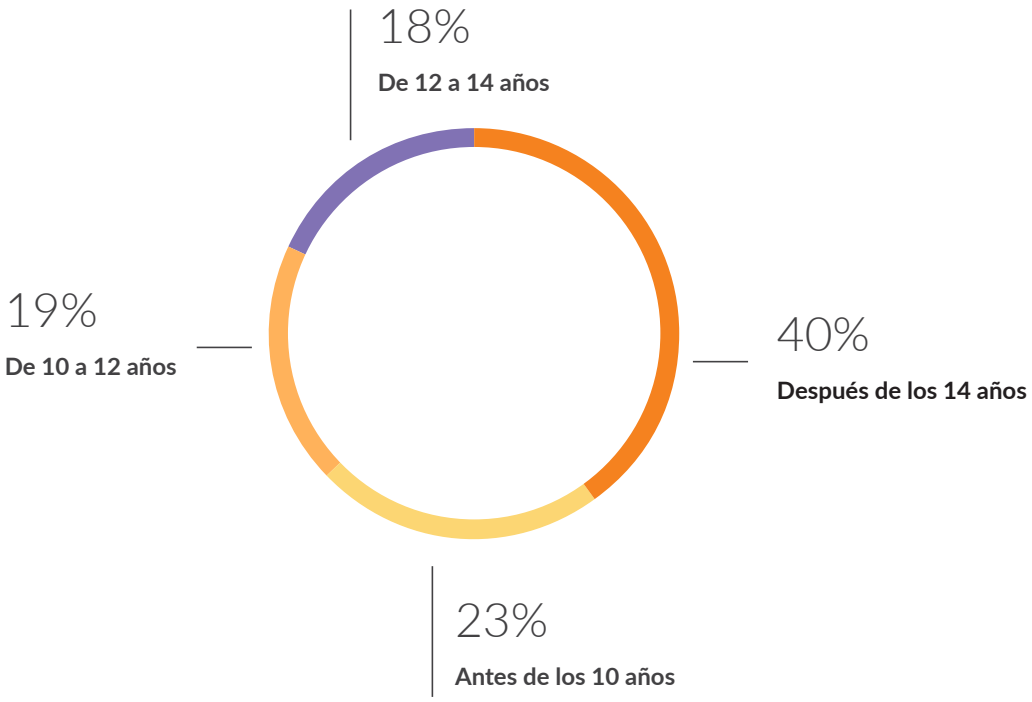
Fuente: Encuesta Hijos Digitales

1.4. REDES SOCIALES

Los menores están a la vanguardia del uso de las redes sociales, en ellas refuerzan vínculos sociales ya establecidos y crean nuevas amistades, por tanto, forman parte tanto de su vida digital como real, de hecho, los jóvenes de 16 a 24 años (91,1%) son los más participativos.

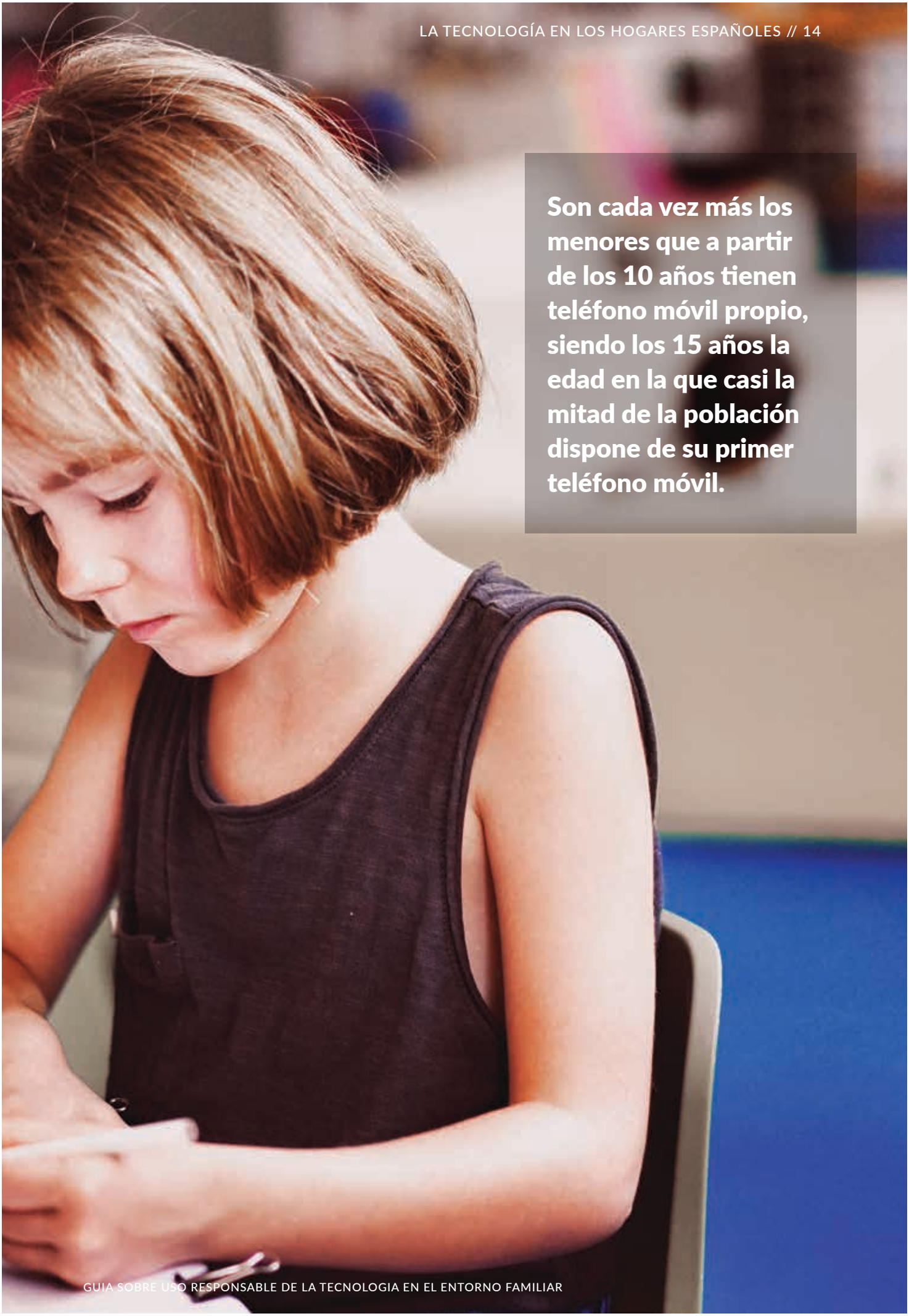
A partir de los 14 años es cuando la mayoría de los jóvenes comienzan a usarlas, tal y como podemos ver en el siguiente gráfico.

Edad a la que comienzan a usar las redes sociales los menores



Fuente: Encuesta Hijos Digitales

Todo ello plantea un nuevo escenario con nuevos retos para las familias, compuestas por diferentes miembros de la sociedad digital.



Son cada vez más los menores que a partir de los 10 años tienen teléfono móvil propio, siendo los 15 años la edad en la que casi la mitad de la población dispone de su primer teléfono móvil.

2

Transformación digital: oportunidades e implicaciones

La expansión y acceso masivo a las nuevas tecnologías y uso de la red ha supuesto una de las mayores y más rápidas transformaciones de la historia de la humanidad. En este cambio Internet y los dispositivos móviles juegan un papel fundamental. A través de ellos los más jóvenes han cambiado la forma de comunicarse, relacionarse, conectarse, aprender y jugar.

La transformación digital de los niños y jóvenes no tiene nada que ver con la relación con las tecnologías de los adultos. Es imprescindible entender cómo se relacionan los niños con los dispositivos digitales para saber cómo educarlos en ello.

Los menores han desarrollado unas características propias en el uso de las nuevas tecnologías. Estas características se pueden resumir en:

- **El *Smartphone* como núcleo de la vida digital:** el teléfono inteligente es el dispositivo más usado por los menores para acceder a Internet. Desde este dispositivo los menores acceden a redes sociales, envían mensajes instantáneos, navegan por la web, hacen fotos y las comparten… A diferencia de los adultos, para los menores la llamada telefónica se convierte en una funcionalidad secundaria.
- **Nueva forma de comunicación:** la multifuncionalidad de las aplicaciones del Smartphone permite a los menores el acceso de nuevas formas de comunicación. Los menores se comunican a través de email, mensajería instantánea, a través de una foto, un vídeo, una nota de voz, un emoticono, etc.. Tienen múltiples maneras de relacionarse con sus amigos o familiares y transmitir lo que quieren decir.
- **Conexión permanente:** los teléfonos inteligentes permiten el acceso a la web las veinticuatro horas del día, estemos donde estemos. Esto ha producido una verdadera revolución en el comportamiento de los usuarios, se crea un nuevo concepto llamado micromomentos. Estos son breves lapsos de tiempo que antes no se dedicaban a hacer nada en concreto y ahora se usan para comunicarse y acceder a Internet. Por ejemplo, tiempo de espera en un médico, durante un trayecto en coche o en autobús, mientras espera a su amigo en la puerta de su casa…
- **Conexión multipantalla:** una de las características del modelo de conexión digital es el fenómeno multipantalla. Esto se refiere al uso de distintos dispositivos en función de la actividad a realizar.
- **Multitarea:** los jóvenes y menores han desarrollado una serie de nuevas capacidades a través de la tecnología. Han desarrollado una mayor inteligencia visual e hipertextual y la capacidad de realizar múltiples tareas al mismo tiempo con distintos dispositivos o usando un solo dispositivo. Son capaces de ver un vídeo mientras postean sus comentarios sobre el video o leen los comentarios del mismo.

NUEVA CIUDADANÍA DIGITAL

Los anteriores elementos demuestran que se ha producido un drástico cambio social en las nuevas generaciones. Este cambio está transformando los mercados y condicionarán y redefinirán el futuro de las profesiones en los próximos 10 años. Según los expertos siete de cada diez niños que ahora están en la guardería trabajarán en profesiones que hoy día no existen.

El mercado laboral demandará un conjunto de habilidades que el hijo no puede aprender solo del padre. Las capacidades que el niño necesitará para relacionarse y para trabajar han de ser aprendidas entre iguales. Tradicionalmente el niño ha sido educado en distintos espacios educativos, el espacio urbano, el espacio de la escuela, de los amigos, de la familia, del ocio... Internet se convierte ahora en un espacio donde las personas se relacionan, desarrollan y aprenden. Por tanto, en el nuevo siglo en que vivimos los valores de comunidad se construyen por igual en espacios físicos y virtuales.

Como padres aparece el reto de acompañar a nuestros hijos en el mundo que les ha tocado vivir. Las habilidades digitales se han convertido en una competencia clave necesaria para tener éxito en la mayoría de las profesiones. Por ello, el niño deberá aprender una serie de competencias digitales si quiere sobrevivir en el futuro tecnológico que les espera.

2.1. OPORTUNIDADES DE LAS TIC

El acceso a Internet proporciona a los menores oportunidades para la sociabilidad, la auto-expresión, creatividad y autoaprendizaje:

ACCESO A INFORMACIÓN

Las nuevas tecnologías permiten un acceso sencillo y rápido a una cantidad de información inimaginable no hace muchos años.

Internet brinda a los niños la oportunidad de estar actualizados en todo momento, enterarse de lo que ocurre a nivel mundial, consultar noticias, apoyo con las tareas. Así como disfrutar de la infinidad de contenidos multimedia accesibles en la web.

Además, está demostrado que a los niños les proporciona una sensación de libertad y autonomía.

COMUNICACIÓN CON LOS PADRES

Las tecnologías permiten a los niños comunicarse constantemente, no solo con amigos, sino con los propios padres. No importa dónde se encuentre la otra persona, existen infinidad de posibilidades de contactar, ya sea por llamada telefónica, mensajería instantánea, chats, etc. Un padre puede saber casi permanentemente donde se encuentra su hijo, existe la posibilidad incluso de localizar con exactitud a los miembros de la familia.

SOCIALIZACIÓN

Las nuevas tecnologías de la comunicación sirven para crear y mantener relaciones sociales tan importantes a esas edades (los móviles, Internet a través de los chat, los foros o el correo electrónico). Estar integrados en un grupo, ayudarse entre ellos instantáneamente, comunicar noticias e intereses comunes y por supuesto, divertirse compartiendo juegos, vídeos, fotos, etc.

Otro de sus principales potencialidades consiste en la reducción de las distancias y por tanto la ruptura de fronteras, ya que nos podemos relacionar con personas de todo el mundo.

APRENDIZAJE

El modo de aprendizaje de los niños ha cambiado mucho en los últimos años, la forma en la que se dictan las clases dentro de las escuelas nada tienen que ver con cómo se hacía hace 10 años. La integración de las TIC en la enseñanza motiva a los niños al involucrar herramientas con otros dinamismos en el proceso de aprendizaje. El niño accede a canciones, videos o webs que ilustran los contenidos a aprender.

Por tanto las tecnologías se convierten en instrumentos que promueven un aprendizaje atractivo y sencillo. Además las webs suponen un escaparate de información en el que cualquier niño curioso puede aprender sin darse cuenta.

JUEGOS Y DIVERSIÓN

Los videojuegos ofrecen numerosas ventajas tanto sociales como didácticas. Se convierten en una fuente de entretenimiento y una vía para establecer relaciones sociales ya que pueden ser practicados en compañía de sus amistades.

También a través de ellos los menores desarrollan habilidades manuales, de coordinación, de orientación espacial, etc. Se ejercitan en la toma de decisiones y la resolución de problemas.

La clave está en elegir un videojuego adecuado a las características de nuestro hijo o hija y en tener presente una serie de pautas para su buen uso.

2.2. IMPLICACIONES DE UN USO NO RESPONSABLE DE LA TECNOLOGÍA

La sociedad digital demanda la necesidad de adecuar las habilidades parentales a la nueva realidad digital en la que vivimos.

El uso de la tecnología por los menores, lejos de ser perjudicial para su desarrollo, es una capacidad imprescindible que debe ser enseñada de forma adecuada, y en donde **la participación de los padres dentro del ámbito familiar es fundamental para su éxito.**

¿Cómo deben afrontar las familias los nuevos desafíos digitales?

La educación digital debe formar parte importante del catálogo de competencias que se deben trabajar en familia. **La supervisión, el acompañamiento y la orientación** de los padres en el acceso a la tecnología de los más pequeños, es esencial para promover el uso seguro y responsable de la misma. Los padres han de tener claro que **nativo digital no es igual a competente digital.**

RETOS QUE DEBEN SUPERAR LOS PADRES

Para que los nativos digitales puedan obtener la guía y acompañamiento que necesitan en su vida digital, los padres tienen ante sí grandes retos en la transmisión de una cultura tecnológica responsable en el entorno familiar. A destacar:

1. APRENDER A TRANSMITIR HÁBITOS DE NAVEGACIÓN SEGUROS Y HACER UN USO RESPONSABLE DE LAS TIC, para que desde muy pequeños, conozcan las conductas de riesgo, las sepan identificar y aprendan a evitarlas.

2. ENSEÑARLES A GESTIONAR LAS EXPERIENCIAS NEGATIVAS de forma eficaz, haciendo que acudan a ellos siempre que se sientan inseguros o hayan cometido errores, así como detectar cuáles son las respuestas más adecuadas y efectivas para cada situación.

DESAFÍOS A LOS QUE SE ENFRENTAN LOS HIJOS

Si bien es cierto que los nativos digitales están muy familiarizados con el uso de la red y la tecnología, no lo están tanto en el abuso que pueden hacer de las mismas otras personas y/u organizaciones malintencionadas, que pretenden comprometer la seguridad de los entornos digitales. Por eso, entre los principales desafíos que tienen los nativos digitales destacan:

1. APRENDER A HACER UN USO SEGURO DE LOS DISPOSITIVOS QUE UTILIZAN. Hay estudios que ponen de manifiesto "el mito del nativo experto" y revelan que gran parte de los nativos digitales "saben cómo utilizar los dispositivos desde la perspectiva del ocio pero no desde la perspectiva de la seguridad" y que la mayoría, no saben cómo administrar las contraseñas de sus cuentas ni cómo crear contraseñas robustas. Desde pequeños, deberán ir **aprendiendo medidas de seguridad básicas, como gestionar sus cuentas y contraseñas**, y de esta manera, ir adquiriendo **comportamientos seguros.**

2. CUIDAR SU PRIVACIDAD EN INTERNET Y NAVEGAR DE FORMA SEGURA. Incluso se habla de la **"mala higiene digital"** que tienen los nativos digitales, especialmente, los más pequeños: no entienden la privacidad, comparten las cuentas con sus amigos y dan permisos ilimitados a las aplicaciones que descargan, incluyendo las que permiten acceder a todas sus fotos y videos, sin cuestionar lo que puede implicar desde el punto de vista de su privacidad.

3. PROTEGER SU IDENTIDAD DIGITAL. Los menores y, más concretamente los adolescentes, no tienen noción de permanencia en términos de "huella digital", no reparan en las repercusiones que pueden tener sus publicaciones actuales en un futuro no muy lejano, ni se plantean cómo pueden llegar a afectar incluso a su incorporación en el mercado laboral.

4. SER CONSCIENTES DE QUE HAY OTRAS PERSONAS QUE SABEN MÁS QUE ELLOS EN LA RED Y QUE PUEDE SER, QUE NO TENGAN BUENAS INTENCIONES. Los nativos digitales han nacido aprendidos y lo saben. Este exceso de confianza es uno de los mayores inconvenientes de cara a su seguridad y uno de los retos más significativos que deben superar. Habitualmente, no ponen interés en comprender cómo puede afectarles una publicación en una red social o el mal uso de los dispositivos y/o aplicaciones, así como las consecuencias negativas que de todo ello se puede desprender, ya que tienen tendencia a percibir que lo tienen todo controlado.

Pero tampoco son conscientes de que hay otras personas en la red que pueden tener más conocimientos que ellos, que les pueden engañar, estafar o suplantar la identidad. Por tanto, deben aprender a controlar su exceso de confianza en el mundo digital.

5. ADQUIRIR PENSAMIENTO CRÍTICO. Aprender a discernir las fuentes fiables de las dudosas, cuestionar la información a la que se tiene acceso, identificar una página web falsa o simplemente, saber, que todo el contenido que aparece en la red no es la verdad absoluta. En definitiva, adquirir un pensamiento crítico desde pequeños será un elemento clave en su educación digital.

6. APRENDER A CUIDAR SU SALUD FÍSICA Y MENTAL. Los menores deben aprender a hacer un uso racional y equilibrado de la tecnología ya que un uso excesivo y no controlado de esta, puede crear adicción, pudiendo afectar a sus relaciones sociales, rendimiento escolar, actividades deportivas, sueño, etc. Desde el inicio en el uso de la tecnología, es conveniente establecer un horario de uso de los dispositivos y que aprendan a gestionar correctamente sus tiempos.

En muchas de las actividades que se realizan en familia interviene la tecnología, ya sea el uso de tabletas y móviles para fotografiar, jugar, hacer vídeos, grabar audios, comentar lo que se está haciendo… usos habituales de los dispositivos en el entorno familiar, pero ¿cuántas veces hemos realizado una copia de seguridad de las fotos del móvil? o ¿hemos instalado antivirus en los dispositivos que utilizamos en casa? o ¿hemos revisado la configuración de seguridad en las redes sociales? Y es que estas tareas de mantenimiento y prevención que pueden aparentar no ser tan divertidas, son más importantes de lo que creemos y nos pueden evitar más de un disgusto.

La usurpación de identidad puede realizarse fácilmente mediante la creación de un perfil que suplante la identidad del objetivo o accediendo a este sin su consentimiento y publicando en su nombre.

DESAFÍOS A LOS QUE SE ENFRENTAN LAS FAMILIAS DIGITALES

Para que los nativos puedan obtener la guía y acompañamiento que necesitan en su vida digital, los padres tienen ante sí grandes retos en la transmisión de una cultura tecnológica responsable en el entorno familiar. A destacar:

MALWARE

Nos conectamos tan rápido y fácil a Internet y desde cualquier dispositivo que a veces no nos damos cuenta que desde el momento en que establecemos una conexión a la red, el riesgo de ser infectado por malware (tipo de software que tiene como objetivo infiltrarse o dañar un ordenador sin el consentimiento de su propietario) está presente.

Tanto los nativos como los inmigrantes digitales deben aplicar unas **medidas de seguridad básicas, tales como:**

- Instalar un antivirus y mantenerlo actualizado.
- Cerciorarnos que tanto los sistemas operativos como las aplicaciones, navegadores y programas que usemos en nuestros dispositivos tengan las últimas actualizaciones instaladas de forma periódica.
- Evitar descargas que sean de origen desconocido.

Recomendaciones para tener buenos hábitos de navegación

- Aprender a detenerse y pensar dónde se accede antes de hacer click, en especial, en enlaces que puedan resultar sospechosos o provenir de fuentes dudosas.

- Evitar las descargas instantáneas y masivas, siempre deben elegirse páginas oficiales de descarga y revisar los comentarios de otros usuarios. En el caso de las aplicaciones, es importante revisar los permisos que requieren antes de descargarlas para asegurarse que solo solicitan los necesarios para funcionar.
- Sospechar de los correos de remitentes desconocidos y tener precaución, ante la duda, es mejor no responder y eliminarlos. Lo mismo con los archivos adjuntos, aunque provengan de un remitente conocido, se deben analizar, si no los estamos esperando o si nos generan duda, es mejor eliminarlos antes de descargarlos.

USURPACIÓN Y ROBO DE IDENTIDAD

Otro de los retos que se encuentran las familias en el ámbito digital es el robo o la usurpación de identidad de los menores.

Uno de los medios habituales son las redes sociales. La usurpación de identidad puede realizarse fácilmente mediante la creación de un perfil que suplante la identidad del objetivo o accediendo a este sin su consentimiento y publicando en su nombre.

Las motivaciones pueden ser diversas: dañar la reputación de la víctima, robarle información y/o dinero, etc.

¿Qué podemos hacer para ayudar a los más pequeños de la casa? Proteger la identidad digital demanda una cultura de seguridad adquiriendo hábitos para hacer una buena gestión de contraseñas desde bien pequeños: aprender a crear contraseñas robustas (de una longitud mínima determinada, que combine mayúsculas, minúsculas, números y símbolos), usar contraseñas diferentes para cada servicio y saber que son la llave de su vida digital. Este es un reto clave en el proceso de creación de la identidad digital.

Asimismo, es importante recordar cerrar las sesiones tras utilizar servicios en línea (correo electrónico, redes sociales…), especialmente en aquellos ordenadores o dispositivos compartidos o que estén accesibles a más personas.

Otra medida de precaución básica para evitar el robo o la usurpación de identidad es evitar utilizar WiFi públicas para manejar información personal, ya que desconocemos cómo están configuradas desde el punto de vista de seguridad y si, en un momento dado, alguien se hace con el control de la red, tendrá acceso a toda la información de los dispositivos conectados a la misma.

Asimismo, se debe evitar la sobreexposición de información personal en las redes sociales, como el número de teléfono, la dirección, horarios, rutinas, viajes, etc., que sobre todo, gusta tanto comunicar a los adolescentes.

CIBERBULLYING

El *ciberbullying* es una forma de agresión intencional y repetida que utiliza los medios digitales para llevar a cabo la agresión entre menores, a través de los sistemas de mensajería instantánea, los chats y las redes sociales.

Los nativos digitales viven rodeados de cámaras, les gusta utilizarlas y sus dispositivos llevan una incorporada susceptible de captar cualquier imagen o escena que pueda resultar comprometida, sin darse cuenta que pueden ser utilizadas en un momento dado en su contra. Otras veces, una simple broma de mal gusto puede tener enormes repercusiones en quien la padece.

Muchas veces, los menores no son conscientes del impacto de este tipo de comportamientos sobre la víctima, tampoco quienes por inacción, temor o desconocimiento contribuyen activa o pasivamente con el acosador, ya sea por no denunciar el acoso o por colaborar en la difusión o propagación del contenido utilizado contra la víctima.

También tienen que comprender que cuanta más información personal difundan (y en especial imágenes comprometidas), más expuestos estarán a ser víctimas de algún tipo de acoso. Aprender a no responder a las provocaciones, saber utilizar los mecanismos y herramientas para solucionar conflictos en la red, tales como el bloqueo de usuarios y aplicaciones o teléfonos de ayuda y denuncia, como veremos en el apartado 3, serán elementos importantes para combatir el *ciberbullying*.

Recomendaciones para prevenir el *ciberbullying*

Es importante dar a conocer a los menores las consecuencias negativas de este tipo de comportamientos. Se debe explicar a nuestros hijos que los comportamientos agresivos aunque se produzcan a través de la red son igual de dañinos. Deben entender que puede causar a la persona sentimientos de tristeza, angustia, inseguridad, aislamiento, etc. En este caso es muy útil el uso de la empatía (“¿Y si fueras tú quien se siente acosado?”).

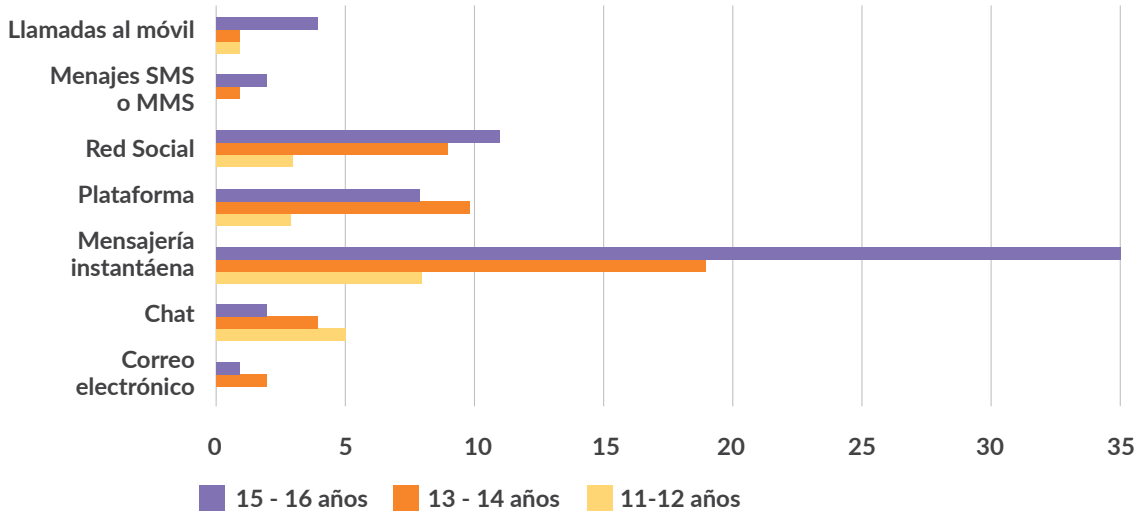
También es importante que los menores encuentren en casa un lugar seguro donde poder contar si están siendo víctimas de algún acoso o si han sido testigos de algún caso de *ciberbullying*. En estos casos hay que tener tolerancia cero y una censura explícita contra el acosador y quien colabore con él.

SEXTING

El *sexting* forma parte de las conductas de riesgo más habituales entre los nativos digitales cuando son adolescentes, por la facilidad de difundir imágenes gracias a los dispositivos y la red.

Cuando se habla de *sexting* se alude al intercambio de imágenes propias de contenido sexual a través del teléfono móvil y a través de sistemas de mensajería instantánea como WhatsApp, aplicaciones tipo Snapchat o redes sociales por las que se envían o comparten las imágenes.

Modos en los que los/las menores recibieron mensajes sexuales en los últimos 12 meses



Fuente: Informe Net Children Go Mobile: Risk and Opportunities

El peligro asociado al *sexting* se debe, fundamentalmente, a la capacidad de propagación de imágenes en la red que escapa al control del emisor en cuanto las publica o comparte. Una imagen sacada de contexto o remitida a otras personas sin consentimiento del emisor puede tener enormes repercusiones en la vida de un menor, con pérdida de su privacidad y deterioro de su imagen pública.

Recomendaciones para prevenir el *sexting*

Para poder prevenir este tipo de comportamientos los adultos deben hacer conocer a los menores los peligros que entraña el envío de información personal. Deben ser conscientes de que una vez enviada una foto o vídeo se pierde completamente el control sobre ella. A partir de ese momento cualquier usuario de Internet puede acceder a la foto o vídeo enviado. La información puede ser utilizada en su contra cuando cae en manos equivocadas en el corto y largo plazo.

GROOMING

El *grooming* consiste en una serie de acciones emprendidas por un adulto cuya finalidad es ganarse la confianza del menor, para obtener satisfacción sexual mediante imágenes comprometidas de su víctima o como preparación de un encuentro sexual.

Inicialmente, contactan con el menor haciéndose pasar por otra persona, simulando ser menores para acercarse a las víctimas. Progresivamente, entablan una relación de confianza basada en aficiones comunes, intercambio de experiencias o comunicaciones personales. Una vez establecida la confianza, el adulto comienza a requerir imágenes del menor, y cuando las obtiene, empieza el acoso y la extorsión.

En las redes sociales es donde encuentran habitualmente el escenario perfecto para conectar con las víctimas. Las redes sociales permiten la comunicación instantánea y el contacto directo con cientos de potenciales víctimas.

Los nativos deben comprender que en Internet no todo el mundo es quien dice ser, que puede haber personas que busquen acercarse a ellos y ganarse su confianza con la misión de abusar de ellos, comprometiendo su seguridad y su intimidad.

Es primordial que aprendan a sospechar de las personas desconocidas que contactan con ellos por las redes sociales, negarse a compartir imágenes privadas y nunca facilitar información personal.

Recomendaciones para prevenir el *grooming*

Una forma de prevenir el *grooming* fácil de entender para los menores es a través de la pregunta ¿Por qué hacer en Internet lo que no hacemos en la vida *offline*?. En la red hay tantas o más amenazas que en la vida *offline* por lo que los menores deben tener unos conocimientos básicos de cómo comportarse en Internet:

- No utilizar datos que puedan identificarlos fácilmente (nombre, edad, dirección, etc.)
- No confiar en quien no conocen
- Eliminar, bloquear y desconectar cualquier conversación que les haga sentirse incómodos

LUDOPATÍA

Uno de los nuevos retos y fenómenos a los que nos enfrentamos es el aumento considerable de la ludopatía entre los menores, centrado especialmente en las apuestas deportivas.

Los dispositivos conectados a la red, como los teléfonos móviles, permiten que la accesibilidad por parte de los menores a los juegos de azar online sea muy sencilla. La inmediatez a la hora de realizar las apuestas, así como el bajo coste de las mismas han fomentado un incremento de la ludopatía entre los adolescentes.

La presión social a la que muchas veces se ven sometidos por sus propios amigos no ayuda a evitar este tipo de hábitos poco recomendables, a la vez que el anonimato dentro de estas aplicaciones fomenta su uso.

Será importante preparar y advertir a los nativos digitales sobre los peligros del juego, educando desde el entorno familiar y ayudando a los menores a que sean capaces de desarrollar las habilidades necesarias para no ceder a la presión de grupo.

EXPOSICIÓN A MATERIAL INADECUADO

Internet alberga cantidades ingentes de contenidos violentos y sexuales para adultos a los que pueden acceder niños y adolescentes desde sus dispositivos. De esta manera, los caminos que llevan al conocimiento de la sexualidad en los niños, no siempre se originan de forma educativa como ocurre en la familia o en el centro escolar.

Para evitar el acceso a contenidos inadecuados por parte de los menores, es importante aprender a utilizar filtros y controles parentales que permitan un desarrollo sano de los nativos digitales, y establecer una serie de medidas de seguimiento y supervisión en el uso de la tecnología y el acceso a Internet.

ENLACES Y SERVICIOS DE INTERÉS

A través de los siguientes enlaces, las familias y empresas pueden ampliar la información tratada en esta Guía, obtener recursos y tener acceso a servicios gratuitos:

SERVICIOS DIRIGIDOS A LAS FAMILIAS, MENORES Y CIUDADANÍA EN GENERAL:

Canal de denuncia de la Guardia Civil: La UCO (Unidad Central Operativa) de la Guardia Civil posee un canal de denuncia donde los usuarios podrán gestionar y tramitar todas sus inquietudes, información, colaboraciones, preguntas...etc. A través del siguiente enlace se accede a la web del grupo de Delitos Telemáticos.

https://gdt.guardiacivil.es/webgdt/colabora.php

La Oficina de Seguridad del Internauta es el servicio de INCIBE para ayudar a los ciudadanos en el día a día sobre aspectos de ciberseguridad doméstica.

http://www.osi.es

Internet Segura For Kids es el Centro de Seguridad para Menores en Internet operado por INCIBE en él se pueden encontrar recursos, actualidad, guías, juegos, etc. para fomentar un uso positivo, seguro y responsable de la Tecnología e Internet entre los menores. Además se ofrece una Línea de Ayuda confidencial, personalizada y gratuita a través del 900 116 117.

http://www.is4k.es

Hijos Digitales: este canal es un punto de encuentro entre padres, hijos y profesionales que sirve para que puedan intercambiar opiniones, conversar, resolver dudas, etc., sobre el nuevo paradigma en el que vivimos. Los profesionales de S2 Grupo proporcionan la información y recursos de apoyo necesarios para que las familias puedan hacer un uso seguro de las tecnologías en el hogar.

https://www.hijosdigitales.es/es

Tu decides internet: La Agencia Española de Protección de Datos ha creado este canal con el objetivo de ofrecer a padres y centros educativos información, consejos, materiales y recursos con las claves necesarias para el uso seguro y responsable de los datos personales en la Red. En el canal también ofrece un espacio con talleres en forma de video para familias.

http://www.tudecideseninternet.es/agpd1/

SERVICIOS DIRIGIDOS A LAS EMPRESAS:

Centro Criptológico Nacional: https://www.ccn-cert.cni.es/

Es el organismo responsable de contribuir a la mejora de la ciberseguridad española, como centro de alerta y respuesta nacional, coopera y ayuda a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas. Pone a disposición de las organizaciones las Series CCN-STIC, normas, instrucciones, guías y recomendaciones con el fin de mejorar el grado de ciberseguridad de las organizaciones. Estas series son:

- Guías de Acceso Público CCN-STIC
- 000 Políticas
- 100 Procedimientos
- 200 Normas
- 300 Instrucciones técnicas
- 400 Guías generales
- 500 Guías de entornos Windows
- 600 Guías de otros entornos
- 800 Guía Esquema Nacional de Seguridad
- 900 Informes Técnicos
- 1000 Procedimientos de empleo seguro

El servicio **Protege Tu empresa** de INCIBE es el canal para acercar y fomentar la ciberseguridad en el entorno empresarial, con recursos de gran utilidad como el Kit de Concienciación para empleados.

https://www.incibe.es/protege-tu-empresa

Security art Work: es un canal de referencia en ciberseguridad que proporciona información y recursos de actualidad en ciberseguridad tanto a los profesionales como a las empresas.

https://www.securityartwork.es

3

¿Cómo impulsar un uso responsable de la tecnología desde el ámbito empresarial?

Todas las organizaciones, están inmersas de forma directa o indirecta en el proceso de trasformación digital que vive nuestra sociedad. Esta realidad, les hace cada vez más conscientes de cómo puede impactar de forma drástica un problema derivado del mal uso o abuso de la tecnología que da soporte a sus procesos de negocio.

Es por ello, que realizan grandes esfuerzos en mejorar sus infraestructuras tecnológicas y en disponer de los recursos técnicos necesarios para su operación y mantenimiento. Son, sin duda, medidas adecuadas pero, de poco sirven, si al final los empleados hacen un uso irresponsable de las tecnologías que tienen a su alcance para desempeñar sus funciones, pudiendo afectar a la continuidad del negocio de la organización.

Todos los empleados y no solo los equipos técnicos, desempeñan un papel importante en el adecuado uso y protección de la tecnología y de la información manejada a través de éstas. Pero ¿tienen los empleados el conocimiento suficiente para hacer un uso responsable de la tecnología?Ante este escenario, las organizaciones se enfrentan al reto de concienciar a todos sus empleados en el uso responsable de la tecnología, con el objetivo de conseguir su implicación en la adopción de buenas prácticas.

3.1. ESTADO ACTUAL

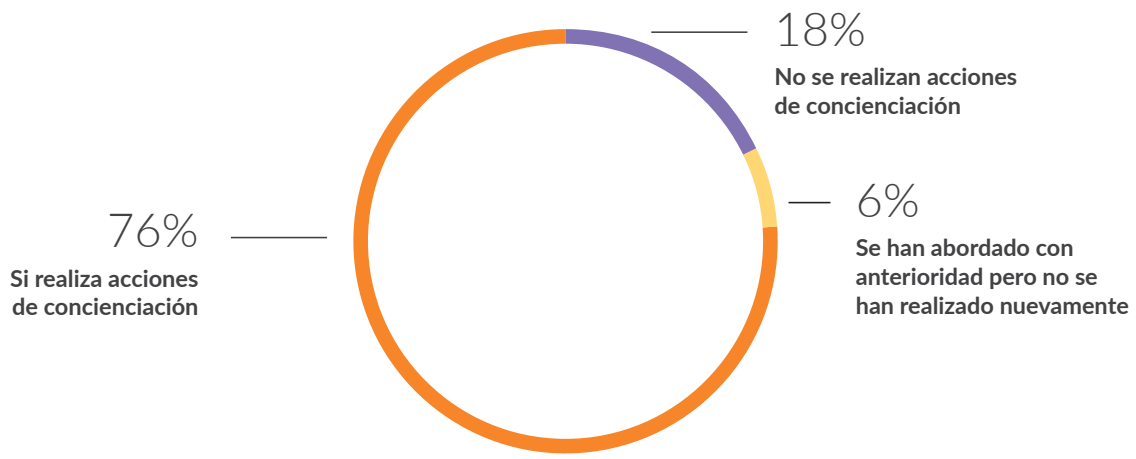
Son muchas las empresas que desarrollan planes de concienciación entre sus empleados para impulsar un uso responsable de las tecnologías en el entorno familiar. Con el objetivo de analizar esta tendencia, el Club de Excelencia en Sostenibilidad lanzó una encuesta formada por 18 indicadores a una muestra representativa de 34 empresas españolas, para conocer de forma cuantitativa cuál es la situación actual y las perspectivas de futuro, así como, calibrar las herramientas más efectivas en la materia.

ACCIONES EMPRESARIALES DE CONCIENCIACIÓN/ SENSIBILIZACIÓN EN MATERIA DE USO RESPONSABLE DE LA TECNOLOGÍA

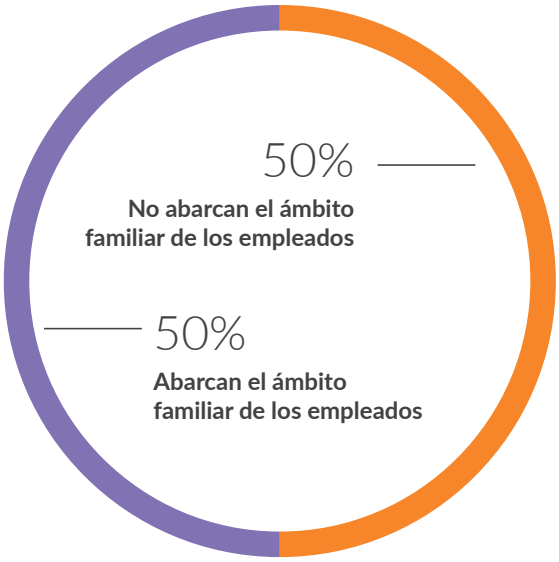
La encuesta pretende examinar si las empresas realizan acciones para concienciar a sus empleados sobre el uso responsable de la tecnología. El 76% de las empresas encuestadas dicen realizar acciones en este ámbito. Además, el 50% de ellas realiza acciones de concienciación que abarcan el entorno familiar de los empleados.

También encontramos que algunas empresas (6%) realizaron acciones de concienciación sobre el uso responsable de la tecnología en el pasado, pero lo han descartado como opción futura.

Su empresa aborda regularmente acciones de concienciación/sensibilización en materia de uso seguro y responsable de la tecnología en el entorno familiar?



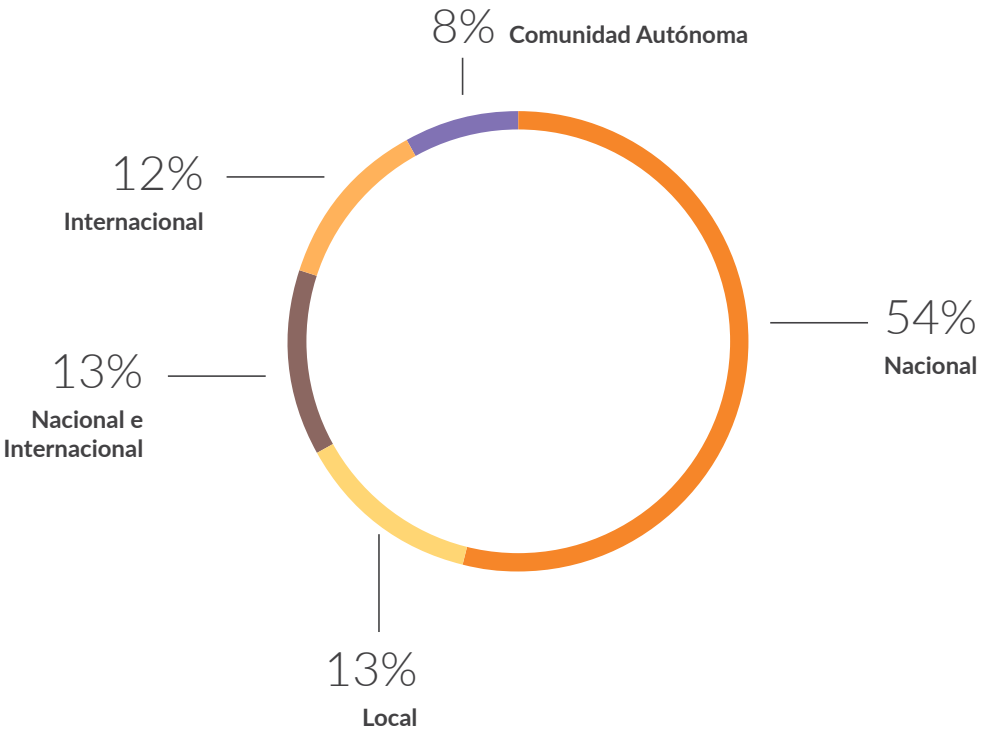
¿Las acciones de concienciación/sensibilización en materia de uso seguro y responsable de la tecnología abarcan también el ámbito personal/familiar de los empleados?



ÁREA GEOGRÁFICA

La mayoría de las empresas, en concreto un 54%, lleva a cabo proyectos de este ámbito en el área nacional. Cabe destacar, que muchas de ellas también proyectan sus proyectos en áreas internacionales.

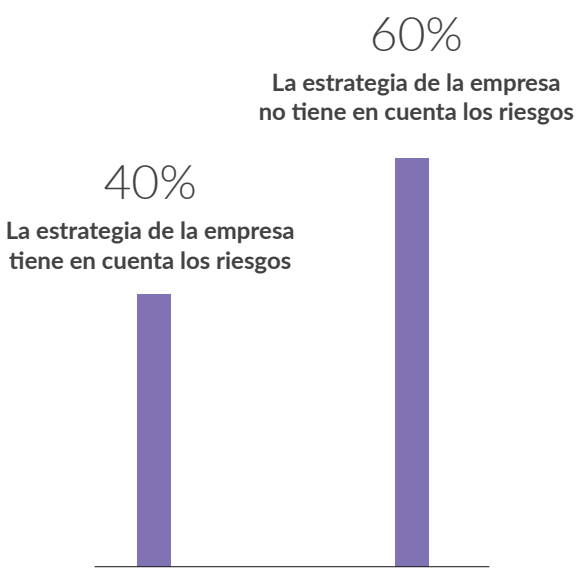
¿Cuál es el área geográfica sobre el que se proyecta su programa de concienciación de uso responsable de la tecnología en el entorno familiar?



RIESGOS

Una gran mayoría de las empresas no tienen en cuenta los riesgos procedentes de los ámbitos personales o familiares de los empleados.

Tiene en cuenta su empresa en su estrategia de ciberseguridad los posibles riesgos procedentes del ámbito personal/familiar de los empleados?



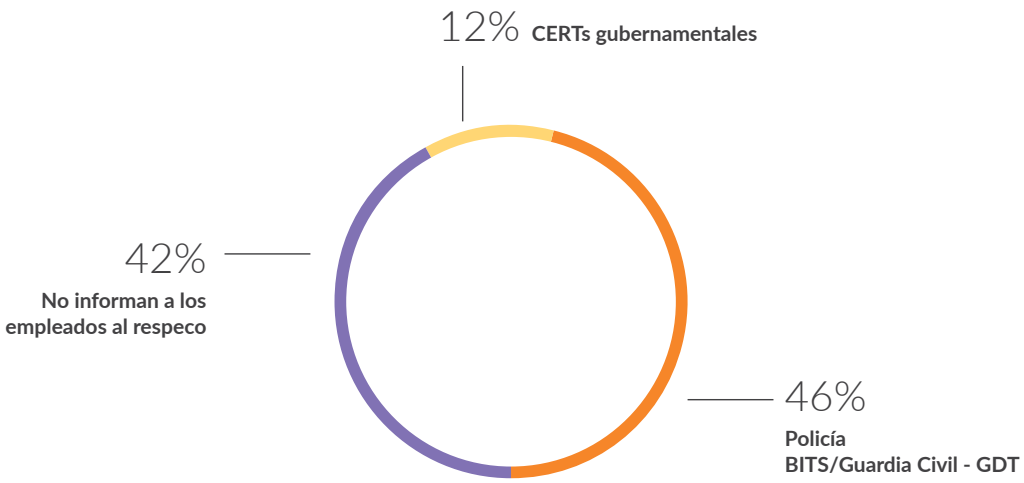
A pesar de esta cifra, las compañías si son conscientes de que hay ciertos riesgos imputables a la esfera personal o familiar de los empleados que puedan tener impacto en la estrategia global de ciberseguridad de la empresa.

Algunos de los riesgos detectados son:

- Descarga de *software* ilegal por menores en dispositivos corporativos, acceso a Internet no controlado, uso no profesional en sitios "desconocidos", uso de Wifi no seguras
- Utilización de herramientas del ámbito profesional para usos personales
- Uso de móviles y herramientas de trabajo desde el domicilio o lugares públicos
- Hábitos domésticos en el uso de las TI que pueden impactar en la red corporativa (visionado de contenidos multimedia, redes sociales, etc.), así como conductas de riesgo en la apertura de correos electrónicos fraudulentos
- Mal uso de los ordenadores/*Tablet*/*Smartphone* empresarial (virus, etc.)
- Mal uso/gestión de crisis en redes sociales
- Comentarios o información publicada por los empleados o sus familiares en redes sociales, relativos a asuntos de trabajo o en los que puedan ser identificados como empleados de la empresa

Las empresas, en concreto un 58% de ellas, informan a sus empleados sobre dónde pueden acudir en caso de incurrir en algún tipo de riesgo por presunta violación de su privacidad a través de Internet y por la cual sus familiares que se vean afectados. Recomiendan acudir a la Brigada Tecnológica de la Policía (Policía – BITS) o al Grupo de Delitos Telemáticos de la Guardia Civil (GDT Guardia Civil). Además el 12% de estas empresas recomiendan acudir al Centro Criptológico Nacional (CERT- Gubernamental).

¿Informa a los empleados a dónde deben acudir en caso de incurrir en algún tipo de riesgo por presunta violación de su privacidad a través de Internet y por lo cual sus familiares se hayan visto afectados?



ACTIVIDADES DE CONCIENCIACIÓN EN MATERIA DE USO RESPONSABLE DE LA TECNOLOGÍA EN EL ENTORNO FAMILIAR

TRASLADO DE BUENAS PRÁCTICAS

Una de las formas de concienciación de los empleados es trasladando buenas prácticas sobre el uso responsable de la tecnología en el entorno familiar. A través de la encuesta hemos descubierto los temas que son más relevantes para las empresas: protección de conexiones, protección de dispositivos y protección de identidad digital.

En su empresa trasladan buenas prácticas sobre uso responsable en el entorno familiar en cuanto a ....?

ACTIVIDADES DE VOLUNTARIADO

EL 21% de las empresas encuestadas realizan actividades de voluntariado en materia de uso responsable de la tecnología en el entorno familiar, convirtiéndose en una herramienta interesante a la hora de generar concienciación con los empleados.

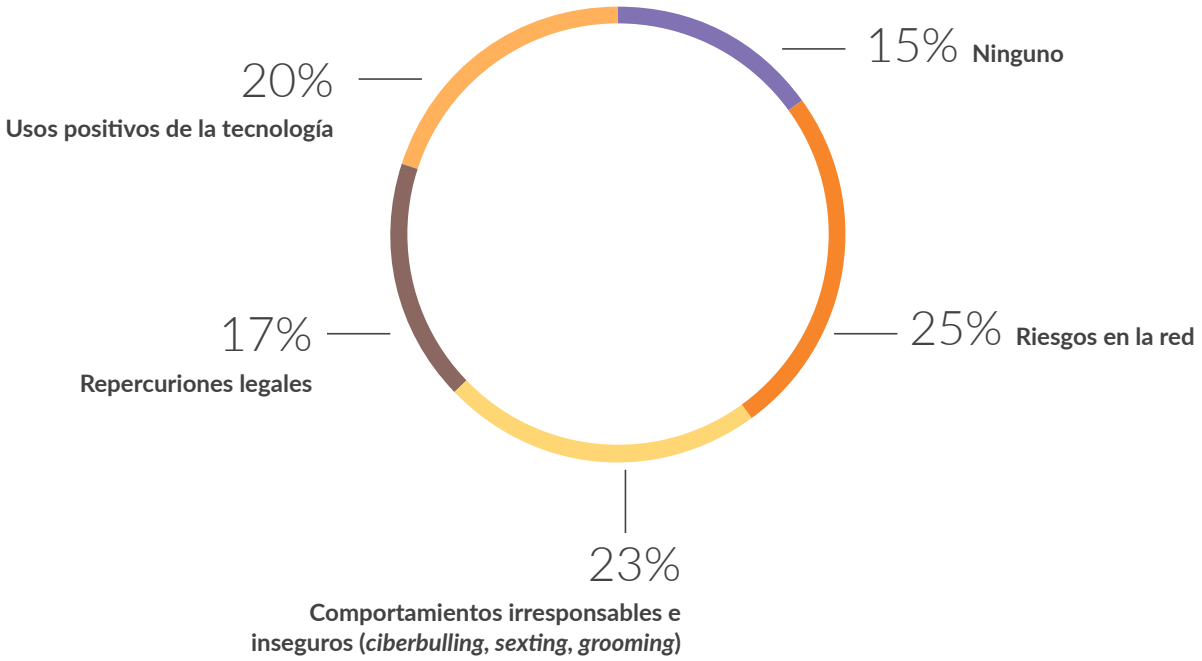
Las actividades que realizan son muy variadas, pero cabe destacar los siguientes programas:

- Colaboración con Centros Educativos concienciando a los menores/padres/educadores en el disfrute responsable y saludable de las TIC
- Formación específica sobre seguridad online para menores
- Concienciación a través del apoyo a la difusión de actividades e iniciativas dirigidas a este fin por medio de redes sociales
- Encuentros responsables sobre ciberseguridad y *bullying* escolar y *bullying* en el trabajo
- Charlas en colegios

TEMAS QUE TRATAN LAS EMPRESAS

Las empresas tratan varios temas en relación al uso responsable de la tecnología en el entorno familiar. Los más destacados son: Riesgos en la red, Comportamientos irresponsables e inseguros (*ciberbulling*, *sexting*, *grooming*), Repercusiones legales y usos positivos de la tecnología.

¿Cuáles son los temas que trata su empresa en relación con el uso responsable de la tecnología en el entorno familiar?



3.2. ESTRATEGIA EFICAZ DE CONCIENCIACIÓN

Concienciar a los empleados en el uso responsable de la tecnología no es una tarea en absoluto trivial. La concienciación tradicional impartida en las organizaciones suele tener muy poco calado entre los empleados que, por norma general, no son conscientes de la repercusión que puede tener el uso inadecuado o irresponsable de la tecnología que manejan y no lo consideran parte de su responsabilidad delegando esta por completo en los departamentos técnicos.

Queriendo arrojar algo de luz sobre el tipo de acciones que se realizan en este campo hemos descubierto que el 33% de las empresas conciencian a sus empleados sobre el uso responsable de la tecnología en el entorno familiar a través de charlas informativas. El 19% lo hacen a través de publicaciones. En cambio, el 11% realiza seminarios y formaciones y el 5% incluye artículos sobre el tema en sus revistas mensuales.

Para revertir este comportamiento es necesario abordar una estrategia de concienciación que haga que el empleado quiera implicarse de forma activa en el uso responsable de la tecnología.

Hoy en día, la barrera que separa la tecnología utilizada en el ámbito profesional, de la utilizada en el ámbito personal es muy difusa. Esta circunstancia nos permite definir una estrategia de concienciación que va más allá del entorno corporativo abordando también el personal, persiguiendo que las personas se sientan emocionalmente involucradas; combinando lo emocional con lo racional.

Es decir, una estrategia que NO se centra en concienciar a los "empleados de la organización", sino a las "personas que trabajan en la organización".

Si el empleado no ve la relación entre los mensajes que recibe y su ámbito más personal o familiar, es difícil que tome conciencia y se implique en hacer un uso responsable de la tecnología. Sin embargo, si ante una situación de mal uso o abuso de la tecnología, hacemos que recapacite y piense "eso me puede pasar a mí" o "eso le podría pasar a mi hijo o hija", la persona se identifica de manera instantánea con las malas prácticas y sus consecuencias. La conclusión es sencilla: ese podría ser yo.

Si conseguimos fomentar una cultura eficaz en el uso responsable de la tecnología en el ámbito familiar del empleado, este adoptará de manera natural las buenas prácticas en el ámbito corporativo.

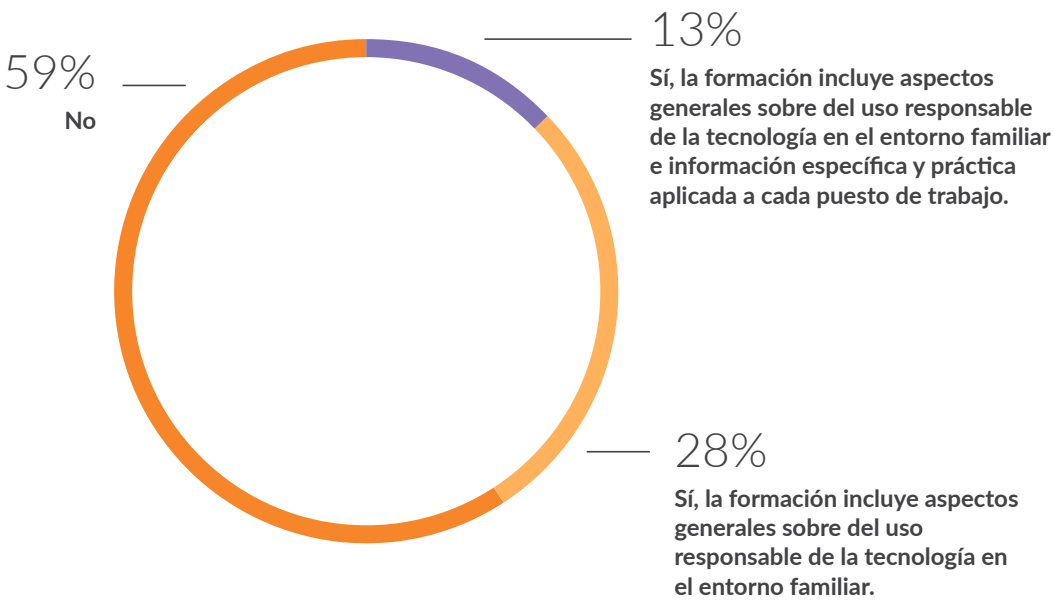
Sin perder de vista este objetivo, la estrategia propuesta establece un marco de trabajo con objetivos secundarios muy beneficiosos para el conjunto de personas que forman parte de las organizaciones y para la sociedad en la que desarrollan su actividad ofreciendo los siguientes objetivos colaterales:

- Concienciar a los más jóvenes sobre el uso responsable de las tecnologías, a todos los niveles.
- Humanizar los conceptos manejados al hablar de tecnología y por tanto reducir el "gap" entre los equipos técnicos y el resto del personal.
- Garantizar el mejor uso posible de la tecnología y, por tanto, incrementar la confianza en las mismas y la tranquilidad al utilizarlas no solo en el seno de la compañía sino también fuera de ella.
- Conocer y evitar los principales problemas derivados del mal uso o abuso de las tecnologías, proporcionándoles el conocimiento necesario para evitarlos.

3.3. PLAN ESTRATÉGICO DE CONCIENCIACIÓN

Para desplegar esta estrategia de concienciación es necesario diseñar e implementar un Plan Estratégico de Concienciación dirigido a todo el personal de todas las áreas de la empresa.

¿Tiene su empresa algún plan de concienciación para sus trabajadores sobre el uso responsable de la tecnología en el entorno familiar?



Es notorio que la mayoría de empresas encuestadas no disponen todavía de un Plan Estratégico de Concienciación, pero una gran parte de los que si lo han implantando incluyen también formación en el uso responsable tanto en el ámbito laboral como el familiar.

A continuación, se describen una serie de buenas prácticas en el diseño e implementación de un Plan Estratégico de Concienciación:

IDENTIFICACIÓN DE COLECTIVOS:

Previo a la implementación de acciones concretas de un Plan de Concienciación que impulse en las empresas el uso responsable de la tecnología, se debe llevar a cabo un trabajo de análisis de situación.

En el mismo, se debe identificar el público objetivo de la organización al que dirigir cada una de las acciones que compondrán el plan. En este punto, es importante identificar las necesidades concretas que tienen los distintos colectivos de personas que forman la organización. Para ello es aconsejable entrevistarse con los responsables de las distintas áreas para analizar y recopilar la información necesaria.

DEFINICIÓN DE CONTENIDOS

Posteriormente, se identificarán los contenidos más adecuados a trasladar a cada colectivo atendiendo a las necesidades de los mismos.

Los contenidos seleccionados serán orientados a generar impacto en el empleado con el objetivo de que este tome conciencia de la importancia de adoptar prácticas de uso responsable de la tecnología que maneja tanto a nivel personal como profesional.

Es importante que los contenidos sean trasladados en un lenguaje sencillo y sin tecnicismos mediante formatos atractivos que permitan una adecuada comprensión por todos los empleados: infografías, vídeos, post, soportes físicos, etc.

Un poco más de la mitad de las empresas encuestadas (52%) se han encontrado una serie de dificultades a la hora de gestionar el uso responsable de la tecnología en el entorno familiar. Algunas de ellas han sido:

- La necesidad de que el tema sea abordado en el currículo escolar del Ministerio de Educación
- Considerar que los dispositivos son para uso profesional
- La empresa no interfiere en el entorno familiar de los empleados
- El no retorno de si la información facilitada es aplicada
- Cómo trasladarlo a los niños
- Falta de tiempo, conocimiento y recursos

- Diferentes culturas y geografías
- Privacidad

Sin embargo, las soluciones que proponen las empresas que ya han pasado por las dificultades son:

- Actividades de colaboración con Comunidades Autónomas
- Charlas y concienciación
- Uso corporativo de los sistemas
- Establecer medidas
- Intercambio de ideas entre empleados
- Trabajo de concienciación
- Insistiendo y formando

DEFINICIÓN DE FORMATOS Y CANALES DE COMUNICACIÓN

Los contenidos podrán ser trasladados tanto mediante acciones presenciales como a través de canales online o plataformas de e-learning, pero es clave que lleguen a la totalidad de los empleados.

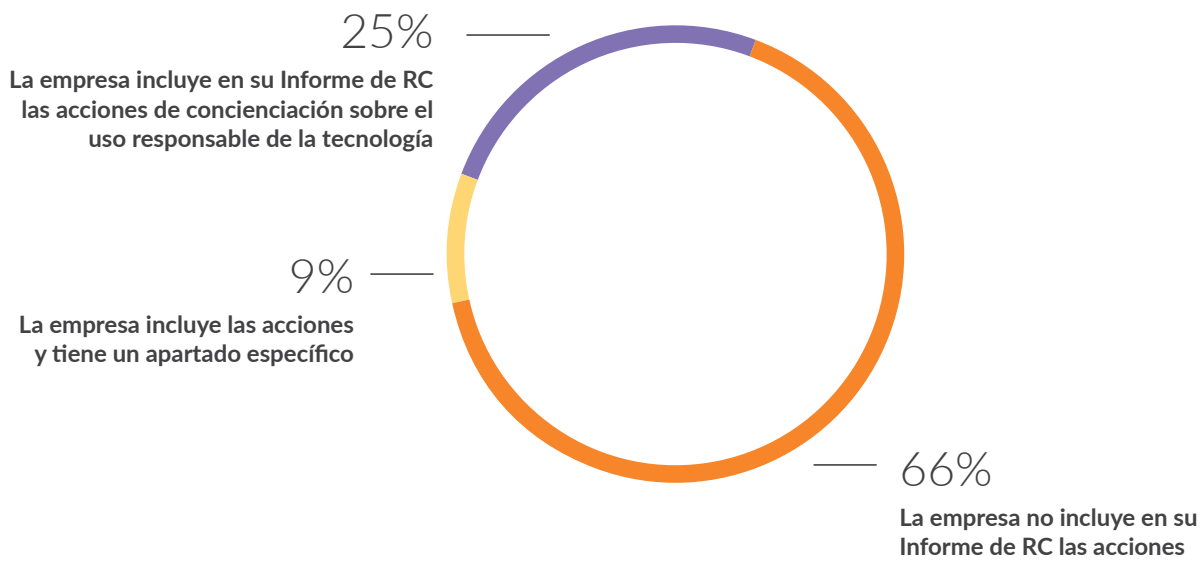
Aunque las acciones presenciales no permitan llegar a todos los empleados, tienen mucha importancia puesto que consiguen de forma muy eficaz impactar y generar interés en el uso responsable de la tecnología. Generamos un "caldo de cultivo" ideal para que los mensajes de concienciación enviados mediante los canales online tengan un mayor calado en la organización.

En este punto, es muy recomendable realizar acciones de concienciación presenciales específicas, dirigidas a la alta dirección de la organización abordando el uso responsable de las tecnologías que manejan tanto en su ámbito profesional como personal.

Para la comunicación por medios online pueden ser utilizados distintos canales como campus virtuales de formación, intranets, sitios web de concienciación, app de concienciación, blogs internos, correo electrónico, etc.

Más de un tercio de las empresas de las empresas incluyen en su Informe de RC las acciones de concienciación sobre el uso responsable de la tecnología. Además, un 9% del total incluye las acciones en un apartado específico.

¿La empresa refleja en su informe de sostenibilidad o de responsabilidad corporativa las acciones de concienciación orientadas al uso responsable de la tecnología en el entorno familiar?



DEFINICIÓN DE MÉTRICAS

Es imprescindible establecer métricas que permitan medir el calado y la eficacia de cada una de las acciones incluidas en el plan de concienciación así como el nivel de cultura en el uso responsable de la tecnología de la organización.

Para ello, será necesario identificar las distintas fuentes de información que permitan medir de forma eficaz el comportamiento de las personas en cuanto al uso responsable de la tecnología se refiere.

Las métricas definidas deben permitir establecer un ciclo de mejora continua a lo largo de todo el Plan de Concienciación.

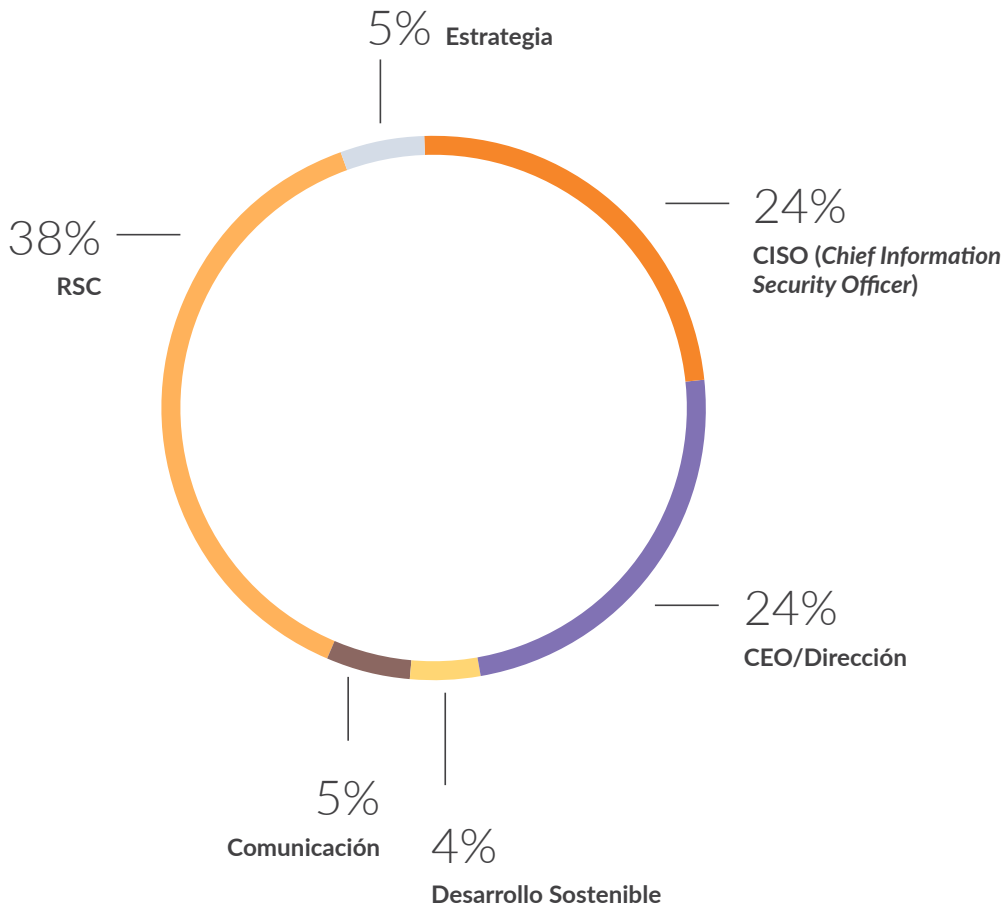
PRESENTACIÓN DEL PLAN A LA DIRECCIÓN

Involucrando desde el primer momento a la Dirección no solo como promotor de la iniciativa sino como receptor directo de la misma.

El área de Responsabilidad Corporativa o Recursos Humanos, así como, los departamentos técnicos de Tecnología, Seguridad o Auditoría podrían ser, en función de las circunstancias de cada organización, los más apropiados para impulsar el desarrollo del Plan de Concienciación.

En cuanto al responsable de las acciones de concienciación sobre el uso responsable de la tecnología en el entorno familiar, en el 38% de las empresas esta función recae sobre el departamento de RC. Caben destacar otros dos departamentos: Dirección (24%) y CISO (24%)

¿Qué función dentro de la organización es responsable de las acciones de concienciación/ sensibilización en el uso responsable de la tecnología en el entorno familiar?



El respaldo de la dirección es un punto clave en el éxito de cualquier plan de concienciación. Por este motivo, es importante dar visibilidad a todos los empleados de su apoyo mediante una presentación oficial del mismo.

La concienciación en el uso responsable de la tecnología no debe ser un proyecto aislado, sino una actividad continuada en las organizaciones. No es necesario abordar un plan de concienciación muy complejo como punto de partida, lo más importante es establecer una estrategia eficaz que permita incrementar poco a poco el grado de madurez de la cultura en el uso responsable de la tecnología entre las personas que forman parte de la cadena de valor de la organización; incluyendo en fases posteriores incluso a clientes, proveedores y en general, a todos los *stakeholders*.

4

Buenas prácticas empresariales para favorecer el uso responsable de la tecnología en el entorno familiar

ESET ESPAÑA

NOMBRE DE LA EMPRESA: **ESET ESPAÑA**

Nº DE EMPLEADOS: **50**

PÁGINA WEB INSTITUCIONAL: **www.eset.es**

DENOMINACIÓN DE LA PRÁCTICA: **¿Qué significan tus hijos para ti?**

LUGAR DE IMPLEMENTACIÓN: **Valencia**

OBJETIVOS

- Aumentar la concienciación social en la lucha contra el ciberacoso infantil.
- Fomentar el posicionamiento de la marca enfocado a la Responsabilidad Corporativa.
- Impulsar el desarrollo comercial.

RETO

Dar a conocer a los adultos los riesgos y amenazas que oculta Internet para ser capaces de identificarlos y saber aportar las medidas necesarias con el fin de proteger a los más pequeños de la casa.

DESCRIPCIÓN DE LA INICIATIVA

ESET ESPAÑA se une a la lucha contra el ciberacoso infantil a través de la creación de una serie de videos en los que los protagonistas son los empleados con hijos menores y a quienes se les pregunta sobre qué significan sus hijos para ellos y las acciones que llevarían a cabo si sus hijos estuvieran sufriendo un ciberacoso.

El objetivo de situar a sus empleados frente a una cámara y hacerles esta pregunta sin conocimiento anterior por parte de los mismos es el de captar reacciones auténticas para finalmente sugerir la siguiente reflexión: si nuestros hijos nos importan tanto, ¿por qué no les protegemos?

LOGRO DE RESULTADOS

- Concienciar sobre el ciberacoso entre menores a los empleados.
- Entender el uso responsable de la tecnología en el entorno familiar como un deber.
- Rendimiento positivo a la hora de confiar a nivel empresarial por la Responsabilidad Corporativa como parte de la estrategia de mercado.

Iberdrola

NOMBRE DE LA EMPRESA: **Iberdrola**

Nº DE EMPLEADOS: **28.395**

PÁGINA WEB INSTITUCIONAL: **www.iberdrola.es**

DENOMINACIÓN DE LA PRÁCTICA: **Protege a tus hijos**

LUGAR DE IMPLEMENTACIÓN: **Madrid, Bilbao, Valencia y Valladolid**

OBJETIVOS

- Concienciar a los menores sobre los riesgos y problemas de seguridad a los que se enfrentan debido al uso de las nuevas tecnologías e Internet.
- Conocer y evitar las principales amenazas proporcionando los conocimientos para hacerles frente.
- Conocer y aplicar las medidas de prevención básicas.

RETO

Sensibilizar a los empleados y sus familiares sobre la nueva realidad de la sociedad digital para que asuman un papel proactivo de protección y fomentar un uso responsable de las TIC en el ámbito familiar.

DESCRIPCIÓN DE LA INICIATIVA

“Protege a tus hijos” es la respuesta de Iberdrola a la necesidad de concienciar y formar a los niños en uso más seguro de Internet y a los empleados en cómo incidir y orientarles en la adopción de buenas prácticas para su seguridad.

Con este fin, Iberdrola pone a disposición de sus empleados y familias la realización de un taller práctico sobre seguridad de los menores en el uso de las TIC e internet. Durante las jornadas lúdico-formativas se representan ataques reales con el fin de que los niños aprendan que hay detrás de algunos comportamientos habituales en la red mientras los padres asisten a una sesión de concienciación con el objetivo de poder orientar a los menores en la adopción de buenas prácticas y seguridad en la red.

LOGRO DE RESULTADOS

- Mejora del uso responsable de la tecnología por parte de los empleados y sus familias.
- Fomento de la protección familiar y del clima laboral.
- Mayor concienciación sobre el uso responsable de las TIC.

MUTUA UNIVERSAL

NOMBRE DE LA EMPRESA: MUTUA UNIVERSAL

Nº DE EMPLEADOS: 1.800

PÁGINA WEB INSTITUCIONAL: www.mutuauniversal.net

DENOMINACIÓN DE LA PRÁCTICA: Comunidad Ciberseguridad Universal

LUGAR DE IMPLEMENTACIÓN: España

OBJETIVOS

» Aumentar el grado de concienciación en materia de ciberseguridad por parte de los empleados.

» Elevar el número de lectores habituales y lograr tanto su recomendación como la difusión de los mensajes sobre seguridad publicados en la Comunidad.

RETO

Concienciar a los empleados sobre la importancia de manejar correctamente la información especialmente protegida desde el punto de vista legal y de protección de datos.

DESCRIPCIÓN DE LA INICIATIVA

Bajo el lema "Ciberseguridad. Tu seguridad es la de tod@s", el equipo de ciberseguridad de MUTUA UNIVERSAL publica en el portal del empleado de forma semanal noticias de actualidad en este ámbito, así como consejos y prácticas para reforzar la seguridad tanto en el ámbito profesional como en el doméstico.

Asimismo, la Comunidad cuenta con un foro en el que cualquier empleado puede publicar sus dudas, así como, cualquier contenido de interés sobre la materia.

LOGRO DE RESULTADOS

» Mayor grado de percepción por parte de la empresa de los riesgos tecnológicos e incremento de la sensibilización ante las amenazas.

» Aumentado del conocimiento por parte de los empleados sobre las amenazas de ciberseguridad a las que pueden estar expuestos tanto a nivel profesional como personal.

ORANGE ESPAGNE

NOMBRE DE LA EMPRESA: ORANGE ESPAGNE

Nº DE EMPLEADOS: 2.684

PÁGINA WEB INSTITUCIONAL: www.orange.es

DENOMINACIÓN DE LA PRÁCTICA:

Promoción del uso seguro, responsable y positivo de Internet

LUGAR DE IMPLEMENTACIÓN: España

OBJETIVOS

- Acompañar a la sociedad (menores, padres y comunidad educativa) hacia un uso seguro y responsable de las TIC.
- Fomentar que los niños y jóvenes dejen de ser meros consumidores de contenidos educativos o de ocio, y que posean conocimiento para poder tener un papel activo en el desarrollo de dicha tecnología.

RETO

Implicación activa en la promoción del uso seguro, responsable y positivo de las TIC.

DESCRIPCIÓN DE LA INICIATIVA

Dentro de la línea estratégica de su política de Responsabilidad Social Corporativa ORANGE ESPAGNE ha lanzado diferentes proyectos enfocados al uso seguro de las nuevas tecnologías, como el voluntariados de empleados que una vez formados por Educalike dan charlas en los colegios de sus hijos con el objetivo de sensibilizar a los menores sobre el uso seguro de las TIC o la plataforma FamilyOn con actividades tecnológicas para adquirir competencias digitales en familia.

Educa Internet, para formar online a la comunidad docente sobre el uso de las TIC y crear sus propios recursos educativos digitales que incluyen un concurso escolar destinado a premiar las mejores prácticas y proyectos de aula sobre uso seguro y responsable de la tecnología. Asimismo, Educar para Proteger, servicio de ORANGE para asesorar y formar a los clientes, padres y madres, para que sus hijos puedan hacer un uso seguro y responsable de Internet.

Finalmente, Superprogramadores, programa de ayuda a las familias en el que les enseñan a disfrutar de la tecnología por medio de la programación y la creación de sus propios videojuegos y “Por un uso LOVE de la tecnología”, campaña de comunicación de ORANGE sobre los riesgos y las ventajas de Internet para los menores, con el objetivo de fomentar el debate y el diálogo entre padres e hijos y dar recomendaciones a los padres sobre la mejor fórmula para tratar estos temas en familia.

ORANGE ESPAGNE

LOGRO DE RESULTADOS

- Contribuir a la digitalización de la sociedad.
- Mejora de posicionamiento como marca comprometida por el uso de las TIC.
- Incremento del compromiso con los empleados.

RED ELÉCTRICA DE ESPAÑA

NOMBRE DE LA EMPRESA: **RED ELÉCTRICA DE ESPAÑA**

Nº DE EMPLEADOS: **1.700**

PÁGINA WEB INSTITUCIONAL: **www.ree.es**

DENOMINACIÓN DE LA PRÁCTICA: **Charlas concienciación en ciberseguridad para las familias**

LUGAR DE IMPLEMENTACIÓN: **Madrid, Barcelona y Sevilla**

OBJETIVOS

- Formar a los trabajadores para convertirlos en empleados seguros.
- Integrar a los empleados en la responsabilidad de la ciberseguridad de la empresa.
- Concienciar a los niños en el uso seguro de las tecnologías.

RETO

Acercar la ciberseguridad a los empleados a través del conocimiento de los riesgos del uso por parte de sus hijos de las nuevas tecnologías, ofreciéndoles recomendaciones y consejos de seguridad.

DESCRIPCIÓN DE LA INICIATIVA

Dentro de su plan de concienciación RED ELÉCTRICA DE ESPAÑA pone en marcha la realización de jornadas familiares en materia de ciberseguridad, con el fin de que padres e hijos tomen conciencia de la importancia de adoptar y promover buenos hábitos de comportamiento en la red, tanto en el ámbito laboral como doméstico, para su protección, así como para evitar ciberataques.

Durante las charlas divulgativas y con el objetivo de que los asistentes sean conscientes del riesgo real que suponen ciertos comportamientos en la red, se presentan situaciones cotidianas reflejo fiel de las rutinas diarias en el uso de las TIC, mostrando todas aquellas amenazas a las que se enfrentan cada día.

Para los más pequeños de la casa se prepara durante la jornada un taller de juegos en el que por medio de diferentes actividades lúdicas, superan diversos retos y pruebas relacionadas con la seguridad en Internet.

LOGRO DE RESULTADOS

- Aumento de la concienciación en ciberseguridad del empleado.
- Acercamiento a los riesgos a los que están expuestos sus hijos y obtención de soluciones a aplicar.

S2 GRUPO

NOMBRE DE LA EMPRESA: S2 GRUPO

Nº DE EMPLEADOS: 240

PÁGINA WEB INSTITUCIONAL: www.s2grupo.es

DENOMINACIÓN DE LA PRÁCTICA: Blog Hijos Digitales

LUGAR DE IMPLEMENTACIÓN: Alcance mundial

OBJETIVOS

- Recabar información sobre usos y prácticas de los usuarios a través de encuestas voluntarias sobre comportamientos de riesgo relacionados con la tecnología.
- Mejorar el acceso y la información de los usuarios hispanohablantes en países en desarrollo a información relacionada con la seguridad de la información.
- Resolver las dudas que los usuarios exponen a través de la web, y que son gestionadas por el personal al cargo del blog como por personal especializado, cuando es necesario.

RETO

Reducir la brecha tecnológica existente entre los menores, con un manejo y conocimiento amplio de las redes sociales y dispositivos tecnológicos (nativos digitales), y sus padres y madres, que tienen la necesidad de adaptarse a un nuevo entorno tecnológico (inmigrantes digitales) que presenta retos y riesgos desconocidos tanto para ellos como para sus hijos.

DESCRIPCIÓN DE LA INICIATIVA

S2 GRUPO edita dos blogs de difusión pública. Una herramienta de publicación muy flexible que se adapta a diferentes tipos de contenidos y grados de formalidad, a través de los que traslada a los lectores las noticias más relevantes en materia de seguridad de la información, nuevas herramientas, alertas y amenazas, investigaciones, etc. Y para el usuario final “de a pie”, S2 GRUPO publica Hijos Digitales, con una temática no especializada y más centrada en el día a día.

El objetivo principal del blog es crear un punto de encuentro entre dos generaciones: la de los “nativos digitales”, niños y jóvenes nacidos ya inmersos en la revolución de Internet y la de los “inmigrantes digitales”, aquellos que han sido testigos de cómo se incorporaban a sus vidas todos esos avances tecnológicos actuales, un lugar que sirva para que todos los actores que intervienen en este nuevo paradigma puedan conversar, intercambiar opiniones, resolver dudas, etc.

S2 GRUPO

LOGRO DE RESULTADOS

- Mejora del conocimiento de las necesidades de los usuarios finales e identificación de elementos de riesgo en los que es necesario seguir trabajando dentro de la línea de Responsabilidad Corporativa y otras iniciativas de prevención.
- Incremento de la seguridad al utilizar nuevas tecnologías por parte de los usuarios finales (adultos y menores).
- Acercar la tecnología a los colectivos con menor nivel de conocimiento.

UNICEF

NOMBRE DE LA EMPRESA: **UNICEF, FONDO DE NACIONES UNIDAS PARA LA INFANCIA**

PÁGINA WEB INSTITUCIONAL: **www.unicef.es**

DENOMINACIÓN DE LA PRÁCTICA:

Herramienta de Evaluación de la seguridad de la infancia On-line

LUGAR DE IMPLEMENTACIÓN: **Alcance mundial**

OBJETIVOS

- Asegurar que las empresas comprenden las cuestiones fundamentales y las repercusiones a tener en cuenta a la hora de evaluar su gestión de los derechos del niño e Internet.
- Ofrecer una autoevaluación completa de la gestión de una empresa sobre los derechos de los niños on-line y su impacto sobre la infancia.
- Detectar fortalezas y debilidades de las políticas y prácticas relativas a los derechos del niño, y elaborar planes correctivos necesarios para ajustar las prácticas de gestión.

RETO

Conocer el impacto de las empresas del sector TIC sobre los niños para poder asegurar la protección y el cumplimiento de los derechos de la infancia.

DESCRIPCIÓN DE LA INICIATIVA

Basándose en las Directrices para la protección de la infancia para la industria, UNICEF ha desarrollado una "Herramienta de Evaluación de la seguridad de la infancia *on-line*" con el fin de dar apoyo a las empresas del sector TIC en el proceso de integración de los derechos de los niños en sus operaciones. La herramienta pretende mejorar la capacidad de las empresas de reforzar sus políticas de protección infantil, sus códigos de conducta y los procesos de debida diligencia.

La herramienta está compuesta por un documento que deben cumplimentar las empresas del sector TIC que participan en esta iniciativa, y por una Guía de Implementación. Uno de los objetivos de la herramienta es la autoevaluación en materia de derechos de los niños *on-line* y su impacto sobre la infancia, para ello, la herramienta hace referencia a seis áreas en las que las TIC tienen más posibilidad de influir en la gestión de los derechos del niño: Área jurídica, derechos humanos y responsabilidad empresarial, recursos humanos, adquisiciones, desarrollo de productos y área comercial.

UNICEF

LOGRO DE RESULTADOS

- Promocionar la protección de los derechos de la infancia en un entorno especialmente sensible como son las TIC.
- Mejorar los sistemas de gestión de riesgo de las empresas del sector TIC.
- Dotar a las empresas TIC de un sistema de autoevaluación rápido, de fácil uso y adaptable a los diferentes ecosistemas empresariales.
- Permitir a las empresas TIC anticiparse a las regulaciones así como identificar oportunidades de autorregulación en materia de protección de derechos de la infancia.
- Construir imagen de marca y fortalecimiento del "social licence to operate" demostrando que los productos pueden tener un impacto positivo.
- Potenciar la motivación de los empleados.

UNIÓN DE MUTUAS MCSS 267

NOMBRE DE LA EMPRESA: UNIÓN DE MUTUAS MCSS 267

Nº DE EMPLEADOS: 650

PÁGINA WEB INSTITUCIONAL: www.uniondemutuas.es

DENOMINACIÓN DE LA PRÁCTICA: Blog de Seguridad Interno: Cuaderno de bitácora semanal

LUGAR DE IMPLEMENTACIÓN: España

OBJETIVOS

- Aumentar el número de posts del Blog de Seguridad Interno relacionados con buenas prácticas aplicables tanto al ámbito laboral como familiar.
- Incremento del número de visitas del Blog.

RETO

Reforzar la seguridad en el entorno laboral por medio de buenas praxis aplicables también al ámbito doméstico.

DESCRIPCIÓN DE LA INICIATIVA

Bajo la premisa "Educar a los que nos educan será fundamental para generar mejores ciudadanos en el entorno digital", UNIÓN DE MUTUAS MCSS 267 publica periódicamente en la intranet corporativa para el Blog de Seguridad Interno: Cuaderno de bitácora semanal.

Se trata de hacer accesible al personal de la empresa contenidos en materia de ciberseguridad: buenas prácticas, LOPD, educación para las redes sociales, menores en la red, novedades INCIBE, OSI, CNN-CERT, etc...

LOGRO DE RESULTADOS

- Mayor concienciación por parte de los empleados en materia de ciberseguridad y buenas prácticas.
- Mejora de la seguridad en el entorno laboral.

VODAFONE ESPAÑA

NOMBRE DE LA EMPRESA: VODAFONE ESPAÑA

Nº DE EMPLEADOS: 4.976

PÁGINA WEB INSTITUCIONAL: www.vodafone.es

DENOMINACIÓN DE LA PRÁCTICA: Programa Cibermentores

LUGAR DE IMPLEMENTACIÓN: Comunidad de Madrid

OBJETIVOS

- Promocionar el disfrute seguro de Internet y la ciudadanía digital responsable.
- Promover la convivencia positiva y prevenir el ciberacoso.
- Situar a los adolescentes como agentes activos y transformadores de la sociedad.

RETO

Sensibilizar a la sociedad ante determinados tipos de incidentes relacionados con el uso de internet por adolescentes y niños, especialmente en relación a los casos de ciberacoso escolar.

Concienciar sobre la necesidad de recursos internos en los centros educativos para la formación en el disfrute seguro y responsable de Internet.

DESCRIPCIÓN DE LA INICIATIVA

VODAFONE ESPAÑA promueve el disfrute seguro de internet a través de la creación del programa “Cibermentores” que convierte a los adolescentes en protagonistas y agentes activos de esta iniciativa.

En primer lugar se capacita a alumnos de 4º de ESO sobre el disfrute seguro, saludable y responsable de Internet (apps, redes sociales…), con énfasis en la convivencia positiva (prevención del ciberacoso) y en la igualdad.

En una segunda fase los alumnos previamente capacitados se convierten en Cibermentores de un alumnado de menor edad al que tienen la responsabilidad de transmitir los mensajes aprendidos en su capacitación, fomentando de esta manera el aprendizaje entre iguales.

Complementariamente, a través de este programa los Cibermentores realizan capacitaciones a personas adultas, ya sean padres o madres como personal docente.

LOGRO DE RESULTADOS

- Fomentar el disfrute seguro y responsable de Internet entre los menores.
- Aumento reputacional consecuencia de la decisión de invertir en Responsabilidad Social Corporativa.

ANEXOS

ABC Economía. (2014)
Siete de cada diez bebés de hoy trabajarán en profesiones que aún no existen

Instituto Nacional de Estadística (2017)
Uso de Internet en los últimos 3 meses por características demográficas y dispositivos utilizados para conectarse a Internet

Net Children Go Mobile. (2016)
Riesgos y oportunidades en internet y uso de dispositivos móviles entre menores españoles

Orange. (2011)
Estudio sobre hábitos seguros en el uso de Smartphones por los niños y adolescentes españoles

Park, Y. (2016)
8 digital life skills all children need – and a plan for teaching them

Roca, G. (2015)
Las nuevas tecnologías en niños y adolescentes. Guía para educar saludablemente en una sociedad digital

Rojas, M. (2016)
¿Cómo afectan las tecnologías al cerebro de los niños y jóvenes?

S2 Grupo. (2017)
Blog Hijos Digitales

Serrano, F. (2016)
Marcos de Competencia Digital en la Educación

Steffanie Zazulak. (2016)
Are all the children we teach really digital natives?

Tecnologías. (2013)
Oportunidades de las TIC

UE Estudio. (2017)
La educación psicodigital puede salvar tu Navidad

Indicadores encuesta “Guía sobre el uso responsable de la tecnología en el entorno familiar”

1 . ¿Su empresa aborda regularmente acciones de concienciación/sensibilización en materia de uso seguro y responsable de la tecnología en el entorno familiar?

Sí

No

Se han abordado con anterioridad pero se han discontinuado

2. ¿Las acciones de concienciación/sensibilización en materia de uso seguro y responsable de la tecnología abarcan también el ámbito personal/familiar de los empleados?

Sí

No

3. ¿Cuál es el área geográfica sobre el que se proyecta su programa de concienciación de uso responsable de la tecnología en el entorno familiar? (responder en caso que si exista sensibilización por parte de su empresa.

Local

Comunidad Autónoma

Nacional

Internacional

4. ¿La empresa refleja en su informe de sostenibilidad o de responsabilidad corporativa las acciones de concienciación orientadas al uso responsable de la tecnología en el entorno familiar?

Sí, y tiene un apartado específico sobre uso responsable de la tecnología en el entorno familiar

Sí

No

5. ¿Tiene en cuenta su empresa en su estrategia de ciberseguridad los posibles riesgos procedentes del ámbito personal/familiar de los empleados?

Sí

No

6. ¿Qué riesgos procedentes del entorno personal/familiar considera que pueden afectar a su actividad empresarial?

7. ¿En su empresa realizan actividades de voluntariado en materia de uso responsable e la tecnología en el entorno familiar?

Sí

No

8. Si su repuesta a la anterior pregunta es positiva, por favor cuéntenos ¿Cuáles son esas actividades de voluntariado en materia de uso responsable de la tecnología en el entorno familiar?

9. ¿Tiene su empresa algún plan de concienciación para sus trabajadores sobre el uso responsable de la tecnología en el entorno familiar?

Sí, la formación incluye aspectos generales sobre del uso responsable de la tecnología en el entorno familiar e información específica y práctica aplicada a cada puesto de trabajo.

Sí, la formación incluye aspectos generales sobre del uso responsable de la tecnología en el entorno familiar.

No

10 . ¿Cómo se fomenta en su empresa el uso responsable de la tecnología entre padres/madres e hijos? (escoja todas las que apliquen)

A través de publicaciones

Revistas mensuales

Seminarios y/o formaciones

Charlas informativas

Otro ¿Cuál?

11. ¿Cuáles son los temas que trata su empresa en relación del uso responsable de la tecnología en el entorno familiar?

Riegos en la red

Comportamientos irresponsable e inseguros (*ciberbulling*, *sexting*, *grooming*)?

Repercusiones legales

Denuncias

Usos positivos de la tecnología

Otras áreas ¿Cuáles?

12 . ¿Qué función dentro de la organización es responsable de las acciones de concienciación/sensibilización en el uso responsable de la tecnología en el entorno familiar?

CISO (Chief Information Security Officer

CEO/Dirección

Desarrollo Sostenible

IT

Comunicación

RSC

Estrategia

I+D+i

Operaciones

Otro

13. ¿Informa a los empleados a dónde deben acudir en caso de incurrir en algún tipo de riesgo por presunta violación de su privacidad a través de internet y que sus familiares se vean afectados?

Sí

CERTs gubernamentales

Policia – BITS / Guardia Civil – GDT

Otra, ¿Cúal?

No

14. ¿En su empresa trasladan buenas prácticas sobre uso responsable en el entorno familiar en cuanto a .....? Marque todas las que apliquen.

Protección de conexiones

Protección de dispositivos

Protección de identidad digital

Otra ¿Cuál?

15. ¿Conoce de indicadores para medir y valorar el nivel de concienciación/sensibilización en cuanto al uso responsable de la tecnología en el entorno familiar?

Sí (por favor describirlos brevemente)

No

16. Si su respuesta a la anterior pregunta fue "sí" , por favor mencione ¿Cuáles son los indicadores que conoce para medir y valorar el nivel de concienciación/sensibilización en cuanto al uso responsable de la tecnología en el entorno familiar

17. ¿Qué dificultades ha encontrado su empresa a la hora de gestionar el uso responsable de la tecnología en el entorno familiar?

18. ¿Como ha hecho frente su empresa a dichas problemáticas?

Diseño y maquetación
Amparo Fontanet

SOCIOS DEL CLUB

ABB · THE ADECCO GROUP · aena · GRUPO ANTOLIN · BASF We create chemistry

B/S/H/ BSH Electrodomésticos España, S.A. · CEMEX · Correos · endesa · FCC Servicios Ciudadanos

IBERDROLA · ISS · MAHOU SAN MIGUEL · orange · Placo SAINT-GOBAIN

RED ELÉCTRICA DE ESPAÑA · GROUPE RENAULT FUNDACIÓN PARA LA MOVILIDAD SOSTENIBLE · SEAT · vodafone

CLUB DE EXCELENCIA EN SOSTENIBILIDAD

CLUBSOSTENIBILIDAD.ORG | RESPONSABILIDADIMAS.ORG

C/ Serrano, 93 - 7°A. 28006 Madrid
Tel. 91 782 08 58 | info@clubsostenibilidad.org