cedec CENTRO NACIONAL DE DESARROLLO CURRICULAR EN SISTEMAS NO PROPIETARIOS

COMPORTAMIENTO EN RED Y GESTIÓN DE LA IDENTIDAD DIGITAL

NETIQUETA
Reglas básicas para relacionarnos y comunicarnos en Internet

A la hora de difundir nuestros materiales en Internet o en las redes sociales es necesario tener en cuenta una serie de reglas de comportamiento basadas en los principios de respeto y privacidad. Este **conjunto de normas relacionadas con la buena educación en Internet** recibe el nombre de netiqueta.

Algunas reglas básicas de netiqueta son las siguientes:

1. Respeta a los demás. No debemos olvidar que al otro lado de la pantalla hay un ser humano, por lo que debemos evitar el lenguaje ofensivo o hiriente, las provocaciones y el ciberacoso. Tratemos a los demás de la misma manera en la que nos gustaría que nos trataran a nosotros.
2. Mantén la privacidad. Evitemos compartir información de nuestra vida personal y privada con desconocidos. Y no compartamos tampoco información de otras personas sin su permiso.
3. Sé respetuoso con la propiedad. Internet no es un mercado libre de productos gratuitos. Respetemos los derechos de autor, evitemos las descargas ilegales o el uso de estratagemas para acceder gratuitamente a páginas que son de pago. En resumen: en el ciberespacio, al igual que en la vida real, debemos respetar la ley.
4. No utilices mayúsculas. En los chats y foros de Internet, escribir todas las palabras en mayúsculas equivale a gritar.
5. Cuida tu estilo. Vigila la ortografía y cuida la gramática y la expresión: la manera en la que escribimos dice mucho de nosotros.
6. Piénsalo dos veces antes de enviar. Antes de mandar un mensaje, una fotografía o cualquier otro tipo de material por Internet, es conveniente pensarlo bien porque, una vez enviado, ya no hay marcha atrás.
7. Evita malentendidos. En Internet las situaciones a veces se magnifican y es frecuente que surjan malentendidos como producto de una mala interpretación de los mensajes. Para evitarlo, es conveniente que cuidemos nuestra forma de expresarnos y, en caso de necesidad, recurramos a emoticonos para reforzar aquello que queremos transmitir.
8. No etiquetes sin permiso. Antes de etiquetar a una persona en una publicación, asegúrate de que no le molesta.
9. No compartas vídeos o fotografías de otras personas sin su consentimiento. Si estás pensando en publicar en una red social una fotografía o un vídeo en el que aparecen otras personas, ten en cuenta que, antes de hacerlo, debes pedirles permiso.
10. Respeta el tiempo de los demás. Aunque muchas veces podemos estar tentados de compartir vídeos e información con personas de nuestro entorno más cercano, es conveniente enviar archivos solo a las personas de nuestros contactos que creemos que podrían estar interesadas en ellos. No hagamos envíos masivos.

IDENTIDAD DIGITAL Y HUELLA DIGITAL
Qué son y cómo protegerlas

La **HUELLA DIGITAL** es el **rastro que dejamos** cuando navegamos **en Internet** y puede ser activa o pasiva. Así, la huella digital activa la forman los datos que compartimos de manera consciente (por ejemplo, cuando hacemos una publicación en redes sociales o en foros online, cuando nos registramos en páginas web…), mientras que la huella digital pasiva está formada por los datos recopilados sin que nosotros lo sepamos (un ejemplo de ello son las famosas *cookies* de las páginas web). Esta huella digital forma parte de la **IDENTIDAD DIGITAL**, que se define como el **conjunto de datos e información** sobre un individuo que existe **en Internet** (quién es, cuáles son sus gustos y aficiones…). Todos **estos datos determinan nuestra reputación digital**, es decir, la opinión que los demás tienen sobre nosotros en el mundo digital.

Por este motivo, es importante **cuidar nuestra identidad digital** de la misma manera en la que cuidamos la imagen que proyectamos en la vida real. Existen para ello unas pautas de seguridad online que pueden ayudar a minimizar las amenazas a las que diariamente está sometida nuestra identidad digital (robo de datos, suplantación de identidad…). He aquí algunas que pueden resultar muy útiles:

1. Limitar la información ofrecida en las redes sociales. Las redes sociales son un escaparate, pero un escaparate que puede llegar a ser peligroso si exponemos nuestra privacidad sin ningún tipo de filtro. Recordemos que, una vez que publicamos un contenido o una información en las redes sociales, perdemos el control sobre lo publicado y alguien podría utilizarlo en nuestra contra.
2. Configurar la privacidad. Por defecto, en la mayoría de las páginas web en las que nos registramos, podemos decidir con quién compartimos la información. Por lo tanto, es importante leer con atención las condiciones de uso y la política de privacidad de los sitios que visitamos y aprender a configurar esas opciones de privacidad de una manera consciente y prudente.
3. Proteger los dispositivos electrónicos con contraseñas seguras. Existen en el mercado una gran variedad de dispositivos móviles (tabletas, teléfonos inteligentes, ordenadores portátiles…) en los que almacenamos gran cantidad de información muy sensible (mensajes privados, fotografías, vídeos…). Si, a causa de una pérdida o un robo, alguien accediera a toda esa información, podría hacer un mal uso de ella, por lo que conviene proteger nuestros dispositivos electrónicos con contraseñas seguras, cambiarlas con cierta regularidad y no compartirlas con nadie.
4. Actualizar el *software* regularmente. Todos los sistemas operativos se actualizan con cierta frecuencia. En algunos casos esta actualización se produce de forma automática mientras que, en otros casos, aparece un aviso en nuestro ordenador en el que se nos pregunta si queremos proceder a actualizarlo. Cuando esto ocurre es importante no demorar el proceso de actualización de nuestro *software* ya que las nuevas actualizaciones siempre vienen con mejoras en cuanto a seguridad.

5. No conectarse a redes wifis públicas. Las redes gratuitas que ofrecen algunos lugares públicos (bares, restaurantes, cafeterías…) no suelen contar con elementos de protección, como contraseñas, lo que hace que nuestro dispositivo esté expuesto y visible a los demás usuarios. Esto puede provocar que los datos que tengamos almacenados puedan ser objeto de algún tipo de ataque por parte de cibercriminales. Por lo tanto, evitemos conectarnos a redes wifi no seguras y, en caso de que sea necesario hacerlo, no entremos en páginas especialmente comprometidas, como nuestro correo electrónico o nuestra banca online.
6. No utilizar páginas web desprotegidas. Es importante que naveguemos siempre por páginas web que sigan el Protocolo Seguro de Transferencia de Hipertexto o "https". Este protocolo hace que toda la información que circula por estas páginas web esté encriptada y, por lo tanto, nadie pueda interceptar el tráfico de datos y acceder a nuestra identidad digital.
7. Cerrar la sesión y borrar el historial de navegación. Cuando accedamos a nuestras cuentas privadas desde ordenadores ajenos (centros de enseñanza, bibliotecas…), es muy importante que no olvidemos cerrar la sesión. También es conveniente que borremos nuestro historial de navegación para que el siguiente usuario que acceda al ordenador no tenga datos sobre nosotros.
8. Hacer *egosurfing*. *Egosurfing* es el término inglés que se utiliza para hacer referencia a una práctica que consiste en buscar en Internet todo lo que está publicado sobre nosotros mismos. Es aconsejable realizar esta práctica de manera periódica ya que, de esta manera, podremos saber qué imagen estamos proyectando al exterior, tomar medidas en caso de encontrar información que no queramos que aparezca y proteger así nuestra identidad digital. De hecho, el TJUE (Tribunal de Justicia de la Unión Europea) en 2014, mediante sentencia, estableció que todas las personas físicas tienen derecho de supresión ("derecho al olvido"), es decir, que pueden a solicitar a los buscadores que retiren determinados resultados de las consultas realizadas con su nombre.
9. Denunciar en el caso de que la identidad digital haya sido suplantada o dañada. La suplantación de la identidad digital es uno de los ciberdelitos más frecuentes, aunque no es el único: la sextorsión, el ciberacoso, etc. son también delitos cibernéticos cada vez más habituales. Y todos estos delitos están perseguidos por la ley. Por este motivo, si sabemos o sospechamos que hemos sido víctimas de alguno de ellos, debemos presentar lo antes posible una denuncia ante las autoridades policiales para que puedan investigar y dar con el ciberdelincuente.

PARA SABER MÁS…

SOBRE NETIQUETA:

- BILIB - Centro de desarrollo de competencias digitales de Castilla-La Mancha: Avanzando en competencias digitales: netiqueta o normas de conducta en la web, qué es y para qué

sirve.

- CALVO FERNÁNDEZ, María: Netiqueta y Soft Skills: Mejorando la competencia digital del alumnado. Cedec.
- Eduteka: Las 10 reglas básicas de la "Netiqueta". Universidad ICESI.
- Pantallas Amigas: Netiqueta Joven para redes sociales.

SOBRE IDENTIDAD Y HUELLA DIGITAL:

- ÁLVAREZ DÍEZ, Vanesa; GONZÁLEZ ALONSO, Mª Dolores y PÉREZ GONZÁLEZ, Silverio, Seguridad en la red III. Consejería de Educación. Junta de Castilla y León.
- BBVA: Identidad y huella digital, ¿cuáles son sus diferencias?
- INCIBE (Instituto Nacional de Ciberseguridad): Privacidad, identidad digital y reputación online.
- INTEF: Identidad, reputación y huella digital.