Ciudadanía digital

El concepto de ciudadanía digital (también denominado ciberciudadanía o e-ciudadanía) viene empleándose con dos sentidos, partiendo desde dos ópticas y áreas de conocimiento distintas pero confluentes: por un lado, hay quien lo utiliza para referirse a la aplicación de los derechos humanos y derechos de ciudadanía a la sociedad de la información, y, por otro, quien lo limita a aquellas nuevas cuestiones relativas a los derechos y deberes de los ciudadanos que surgen en el entorno de las nuevas tecnologías. También existe un empleo menos riguroso que lo hace referente únicamente a la alfabetización digital de los ciudadanos, sin entrar en cuestiones éticas ni relativas al concepto de ciudadanía.

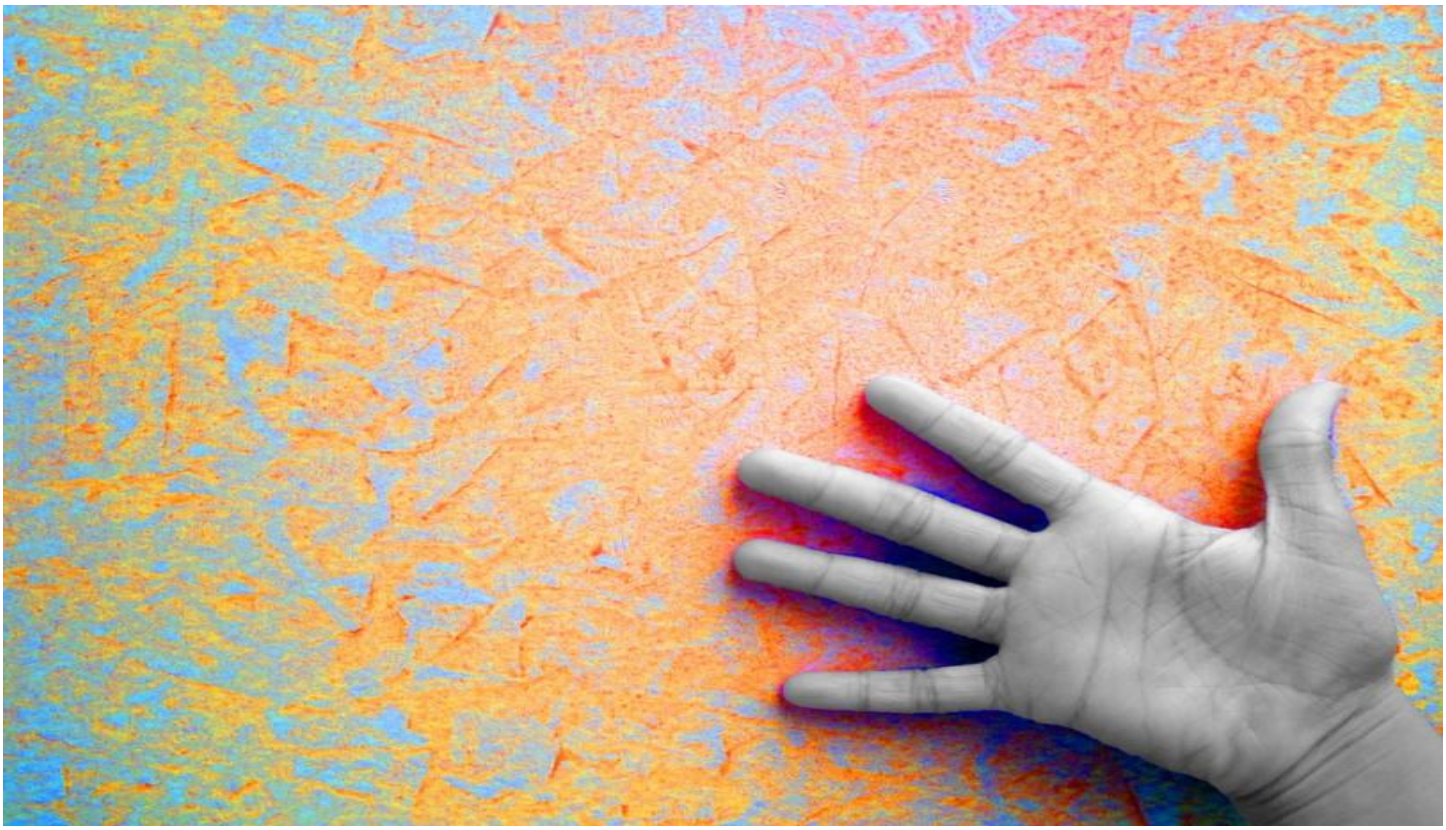
La ciudadanía digital comienza a plantear el manejo de algunas reglas escritas o normas sobre el comportamiento y el buen uso de estas tecnologías. En la actualidad cada vez se le da una mayor importancia a la enseñanza para una ciudadanía responsable, que nos ayude a prevenir los

riesgos que se pueden originar a partir del uso de las TIC cotidianamente, especialmente para los chicos. Hay algunas realidades, como el ciberbullyng o ciberacoso, que son demasiados peligrosos para los niños y adolescentes que usan internet. Ha sido definida como las normas de comportamiento que conciernen al uso de la tecnología, aunque el propio concepto se considera en proceso de definición permanente a medida que evolucionan las posibilidades de la tecnología.

¿Se consideraría a sí mismo un ciudadano digital? La respuesta inmediata para algunas personas es 'no'. Sin embargo, tras una reflexión posterior, y después de pensar en la participación diaria en el mundo digital: dedicando tiempo diariamente en la red, conectándose a través de uno o más dispositivos simultáneamente, estando en contacto con socios, familiares, compañeros o amigos principalmente a través de medios digitales, muchas personas probablemente reconsiderarían su respuesta y se darían cuenta de que son, de hecho, ciudadanos digitales.

Cuando se intenta definir la ciudadanía digital vienen a la mente tres pilares principales: ***pertenencia, implicación y protección***. Los ciudadanos digitales pertenecen a la sociedad digital y utilizan la tecnología para implicarse activamente en la sociedad y con la sociedad. La ciudadanía digital empodera a las personas para cosechar los beneficios de la tecnología digital de una forma segura y eficaz.

Yo pertenezco a aquí



La sociedad digital proporciona oportunidades para interactuar, aprender, trabajar, ser. Los ciudadanos y ciudadanas "trabajan para" y "se benefician de" su pertenencia a la sociedad, y los

mismos aspectos son aplicables a los ciudadanos y ciudadanas digitales. Muchas de nuestras interacciones se producen en línea, y por lo tanto, somos parte de una sociedad digital en la misma medida que somos parte de la sociedad (tangible) en la que vivimos. Todo el mundo tiene un sentimiento de pertenencia, de igual forma que todo el mundo necesita sentir que pertenece a algún sitio. Esto es especialmente cierto con los jóvenes, que están conformando los rasgos de su personalidad ajustándose al grupo (y a la sociedad) a la que pertenecen. En la negociación de derechos y deberes a la que inevitablemente se llega con el concepto de ciudadanía, un asunto que no hay que olvidar es el de disfrute, que está en la base misma del sentido de pertenencia. Disfrutamos siendo parte de una sociedad digital y nuestras obligaciones hacia esta sociedad no deberían ir en detrimento del disfrute por esa pertenencia.

Una participación completa en una sociedad digital requiere disponer de acceso. El acceso fue el primer criterio para explicar la brecha digital, un concepto que empezó a usarse en la década de 1990 para aludir a las diferencias en cuanto a inclusión digital. La inclusión digital ha mejorado drásticamente en la última década, estando el acceso a las tecnologías casi saturado en Europa. Sin embargo, sigue habiendo barreras relacionadas con el acceso de los menos privilegiados, o con el uso de tecnologías en el hogar. Por ejemplo, las mujeres, en especial las madres, son con frecuencia las últimas en disponer de acceso y en utilizar en la familia un dispositivo digital compartido. Podríamos argumentar que, si hace un siglo Virginia Wolf reclamaba para todas las mujeres “su propio espacio” para estudiar y tener acceso a la educación, hoy en día deseamos para todas las personas su propio espacio y su propio dispositivo digital.

El comportamiento individual de cada persona como miembro de una sociedad digital conformará el entorno digital al que pertenece el conjunto total de individuos.

Estoy implicado

La participación en el dominio digital ha dejado de ser una cuestión de "tener" o "no tener", como ya hemos visto antes, sino más bien de "poder" o "no poder". Si la participación digital depende del acceso y del uso, depende aún más de las actitudes. La participación puede tener diferentes grados, que van de la expectación al apoyo. Se puede participar simplemente navegando por la red, o se puede tener voz (y una voz fuerte).

Durante mucho tiempo los ciudadanos digitales han sido considerados como usuarios de tecnologías (meros receptores, consumidores). Ahora vemos que los ciudadanos y ciudadanas digitales también pueden convertirse en participantes activos. **Su implicación no solo se traduce en el consumo de productos digitales y contenido digital, sino que también se manifiesta en la creación de contenido digital, herramientas, aplicaciones, códigos y prácticas.**

Los jóvenes son productores prolíficos de contenido digital: toman y comparten imágenes, vídeos, multimedia, textos y opiniones. Ser productores en lugar de consumidores permite a los ciudadanos y ciudadanas digitales contribuir al panorama de la sociedad digital y a comprenderla mejor. Cuando hablamos, por ejemplo, sobre programación y sobre sus beneficios para la educación, esgrimimos siempre el argumento de que la programación permite a los estudiantes crear y no solo usar. Algo que es cierto. Sin embargo, implicándose en la codificación y en la programación también aprenderán cómo se mueve la sociedad digital en la que se zambullen todos los días. Pueden captar mejor la lógica de los algoritmos implicados en el motor de búsqueda y otras herramientas en línea en línea que utilizan.

Podríamos considerar la participación digital como un proceso de cuatro escalas. **Estarían quienes se mantienen expectantes**, observando, mirando, usando el mundo digital como consumidores y espectadores. **Están quienes participan compartiendo información y contenido**, conectando a las personas, compartiendo ideas que merece la pena difundir. En la tercera escala, **estarían quienes crean nuevo contenido, nuevas prácticas, nuevas herramientas**, quienes propician una nueva forma de implicarse con otros ciudadanos o ciudadanas digitales, y formar parte de una sociedad digital. **Y en la escala más alta estarían quienes aprovechan el potencial de la tecnología para conseguir una sociedad mejor**. Esta cuarta escala incluye a quienes quieren implicarse en dar forma al futuro de la web, así como a quienes conforman el futuro de la sociedad como un todo a través de medios digitales. Deberíamos reconocer la importancia de la participación de la juventud en los debates de gobernanza de Internet de una forma más sistemática y regular, adquiriendo por nosotros mismos las destrezas y conocimientos adecuados tanto para facilitar la comprensión como la formación de opiniones personales en temas relacionados con la forma en que funciona el ecosistema de Internet. Los jóvenes pueden ser empoderados para conformar una Internet mejor o, si no desean llegar a la escala superior, para poder seguir teniendo influencia en un entorno digital mejor promocionando valores y comportamientos positivos. Al mismo tiempo, deberíamos reconocer el papel de la juventud en la implicación en la sociedad y con la sociedad como ciudadanos digitales. Vemos cómo procesos tales como las peticiones en línea, por ejemplo,

reclaman ahora espacio para la implicación cívica. Las herramientas y medios digitales también se utilizan para apoyar la 'transparencia' en la elaboración de políticas, permitiendo que los ciudadanos puedan reunirse de nuevas formas.

Estoy protegido y protejo

Por definición, los ciudadanos están protegidos por el país al que pertenecen. La protección es parte también de los derechos que tienen las personas cuando están en red. Las tecnologías ofrecen oportunidades y riesgos. Aunque el riesgo no implica inevitablemente un daño, el daño puede ir en detrimento del disfrute de la ciudadanía digital.

El acceso digital no solo expone a los jóvenes a posibles riesgos, sino que también mejora su educación digital y sus habilidades de seguridad. Esto significa que es más probable que los usuarios activos se conviertan en usuarios de tecnología resilientes. Por lo tanto, los responsables de la elaboración de las políticas, los educadores, los padres y otros cuidadores deben implementar estrategias específicas para garantizar los derechos de los niños y niñas a la protección, sin menoscabo de sus derechos a la participación.

Muchos jóvenes son expertos en decirle a los adultos lo que tienen que hacer para mantenerse en condiciones de seguridad en la red, sin embargo, no queda garantizado que esto se traduzca en cambios en su comportamiento. Una estrategia sensata y eficaz es animar a los niños, niñas y jóvenes a ser usuarios responsables no solo en sus acciones en línea sino también en la forma en que prestan apoyo a otras personas. Si preguntamos a un grupo de personas (no solo a jóvenes) cuántas de ellas han visto algo inapropiado en línea muchas de ellas responderán

afirmativamente. Si preguntamos al mismo grupo de personas cuántas de ellas han informado de este contenido al proveedor de servicios o a un adulto el número de quienes respondan afirmativamente será mucho menor. Del mismo modo, cabría preguntarse si los centros escolares y los padres están debidamente preparados para tomar acciones preventivas o correctivas cuando las cosas no vayan bien.

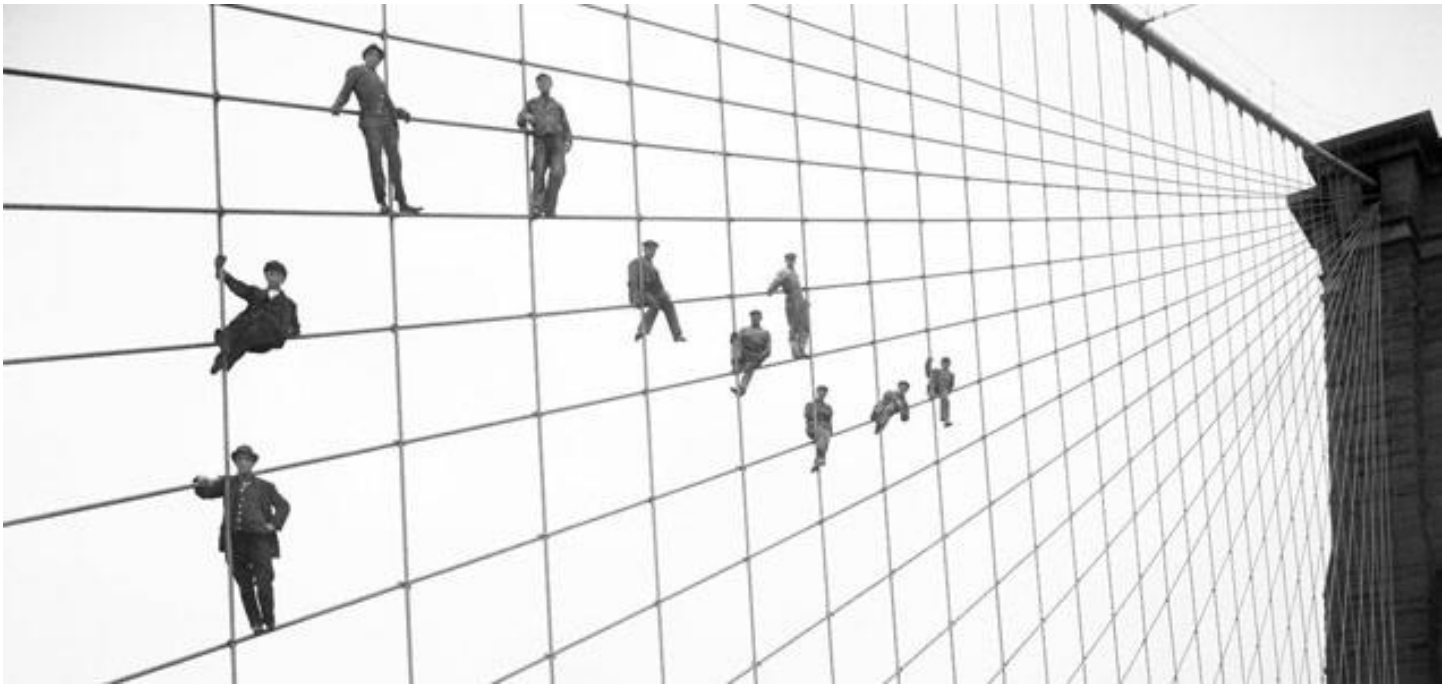
Los niños, niñas y jóvenes tienen necesidades específicas y se merecen protección y salvaguardia. Como en el mundo real, es necesario establecer ciertas medidas protectoras. Los niños, niñas y jóvenes también deberían tener margen para experimentar y aprender de sus errores, sin que se siga o rastree todo clic o todo me gusta. Se les debe alentar a respetar y salvaguardar el derecho de los demás. Esta es una enorme responsabilidad que compartimos entre todos y todas.

Poseo destreza digital

En el punto de inflexión de la ciudadanía digital, las destrezas digitales proporcionan el punto de entrada a este país virtual. En una sociedad cada vez más digitalizada, podemos considerar la ciudadanía digital como un derecho. Las habilidades digitales nos permiten ejercer este derecho.

Sin embargo, no deberíamos considerar las habilidades digitales como la simple capacidad para utilizar dispositivos. Se considera que la concienciación y la tolerancia, los valores y responsabilidades democráticas forman parte, todos ellos, de las habilidades necesarias para ser y convertirse en ciudadanos y ciudadanas digitales. Dentro de este contexto, la educación tiene que jugar un papel crucial, ya que está en una buena posición para conformar, desde una temprana edad, el futuro de una generación conectada. Como estudiantes de EMS deben desarrollar habilidades digitales, empoderándose para pertenecer a la sociedad digital, con un sentido de implicación seguro, responsable y creativo.

Áreas de la ciudadanía digital



Según las diversas definiciones, hay una serie de áreas que se suelen abarcar dentro del concepto de ciudadanía digital:

Netiqueta: normas de comportamiento cívico en la Red.

Educación: aprendizaje del uso de las TIC (alfabetización y competencias digitales) y mediante el uso de las TIC.

Acceso y participación: brecha digital, derecho de acceso a Internet, democracia electrónica...

Consumo: defensa del ciberconsumidor.

Salud y riesgo: ergonomía y otros riesgos de las TIC.

A su vez esas áreas se pueden subdividir en una serie de derechos y deberes de los ciudadanos digitales (ciberderechos y ciberdeberes). Una tendencia en auge de especial relevancia es la vinculación de la educación para una ciberciudadanía responsable con la prevención de riesgos

de las TIC, principalmente para los menores. Ello es debido a que fenómenos como el ciberbullying son considerados como uno de los principales riesgos que niños y adolescentes afrontan como usuarios de Internet y otras nuevas tecnologías.

Netiqueta

Netiquette (o netiqueta en su versión castellana) es una palabra derivada del francés étiquette y del inglés net (red) o network y vendría a designar el conjunto de reglas que regulan el comportamiento de un usuario en un grupo de noticias (newsgroup en inglés), una lista de correo, un foro de discusiones o al usar el correo electrónico. Por extensión, se utiliza también para referirse al conjunto de normas de comportamiento general en Internet. La Netiqueta no es más que una adaptación de las reglas de etiqueta del mundo real a las tecnologías y el ambiente virtual. Aunque normalmente las tendencias de etiqueta han evolucionado hasta llegar a formar incluso parte de las reglas de ciertos sistemas, es bastante común que las reglas de etiqueta se basen en un sistema de “honor”; es decir, que el infractor no recibe siquiera una reprimenda. De la misma manera que existe un protocolo para los encuentros físicos con personas, la así llamada netiquette describe un protocolo que se debe utilizar al hacer "contacto" electrónico.

Funciones de la netiqueta

La Netiqueta comprende todas las formas de interacción directa e indirecta de un usuario con otro.

Entre estas, podemos destacar:

- ✓ El comportamiento en el correo electrónico: la forma en que nos dirigimos a la persona, el contenido del mensaje (publicidad, spam, cadenas, etc.), el contenido de los archivos adjuntos (si aplica), el uso de mayúsculas, etc.
- ✓ El comportamiento en los foros: el nivel de lenguaje utilizado, el formato del mensaje, distinción de ambiente, etc.
- ✓ El comportamiento en los blogs: comentarios formales o informales, concordancia del comentario con el tema, respeto hacia las otras opiniones, etc.
- ✓ El comportamiento en el chat: conciencia de las capacidades del servidor (flooding, tamaño de los ficheros), respecto de la temática del chat, uso de íconos moderado, etc.

Normas Netiqueta

Regla 1: Nunca olvide que la persona que lee el mensaje es en efecto humano con sentimientos que pueden ser lastimados.

Regla 2: Adhiérase a los mismos estándares de comportamiento en línea que usted sigue en la vida real.

Regla 3: Escribir todo en mayúsculas se considera como gritar y, además, dificulta la lectura.

Regla 4: Respete el tiempo y el ancho de banda de otras personas.

Regla 5: Muestre el lado bueno de su persona mientras se mantenga en línea.

Regla 6: Comparta su conocimiento con la comunidad.

Regla 7: Ayude a mantener los debates en un ambiente sano y educativo.

Regla 8: Respete la privacidad de terceras personas, hacer un grupo contra una persona está mal.

Regla 9: No abuse de su poder.

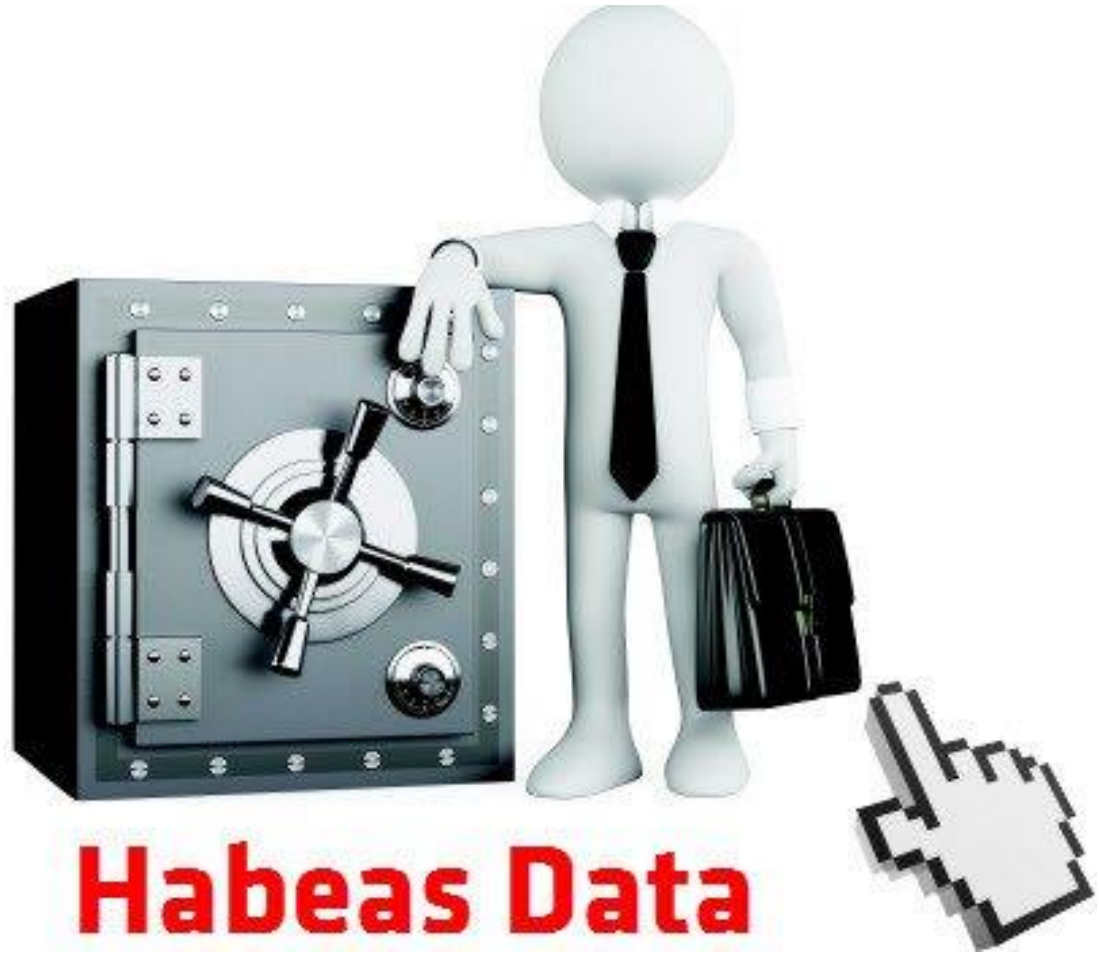
Regla 10: Ser objetivo sobre temas cuyo bien primordial no afecte el general.

Código de buena conducta en Internet

Los bien llamados "**códigos de buena conducta**" (Netiqueta) no han sido impuestos por nadie sino por el sentido común. Las personas que llevan mucho tiempo navegando por la red han ido asumiendo responsabilidades de comportamiento que facilitan el uso de la misma, rápido y satisfactorio. Cada comunidad tiene sus propias reglas culturales, normativas, educativas, reglas que influyen en el comportamiento de las personas. Cuando un individuo ajeno a una comunidad pretende integrarse en ella debe conocer previamente estas normas de comportamiento por la continua actualización y ampliación que tiene la Red. Por ello la importancia de estas.

Si bien es cierto que dirigirse a las personas con respeto y con sumo tacto de forma verbal es importante para equilibrar las ideas a transmitir ya sea como emisor o como receptor; de igual manera es importante tener cuidado cuando utilizamos la herramienta número uno en el mundo en cuanto a investigación, recreación y educación entre otras cosas. Además, por cómo es internet, las netiquetas nos ayudaran en nuestra interacción y al buen entendimiento con nuestros semejantes.

Habeas data



Habeas data frase legal en latín; la traducción más literal de tal frase es: **tener datos presentes** siendo hábeas la segunda persona singular del presente de subjuntivo del verbo latino habere (en este caso entendido como “tener”). Esto es; en ejercicio de una acción constitucional o legal, que tiene cualquier persona que figura en un registro o banco de datos, de acceder a tal registro para conocer qué información existe sobre su persona, y de solicitar la corrección o eliminación de esa información si le causara algún perjuicio. También puede aplicarse al derecho al olvido, esto es, el derecho a eliminar información que se considera obsoleta por el transcurso del tiempo y ha perdido relevancia para seguir siendo informada.

Este derecho se fue expandiendo y comenzó a ser reglamentado tanto por leyes de habeas data como por normas de protección de datos personales (que suelen tener un capítulo procesal donde se escribe el objeto de la acción de habeas data, la legitimación pasiva y activa, y la prueba y la sentencia).

También se encomendó a organismos de control la vigilancia sobre la aplicación de estas normas. Así existen en diversos países (como Argentina, España, Francia y Uruguay etc.) organismos de control que tienen por misión supervisar el tratamiento de datos personales por parte de

empresas e instituciones públicas. También se suele exigir una declaración de los ficheros de carácter personal para generar transparencia sobre su existencia.

Constituciones que reconocen este derecho

Argentina, Bolivia, Brasil, Colombia, Ecuador, España, Panamá, **México**, Paraguay, Perú, República Dominicana, Uruguay, Venezuela.

Responsabilidades de emisión de datos e información en el ciberespacio

Los avances tecnológicos, llevan necesariamente a tener que resignificar las transformaciones sufridas por estos últimos. Analizando el fenómeno de Internet, podemos observar, tres constantes dentro de la estructura que sostiene su desarrollo.

La primera se encuentra configurada por la conectividad; sin ésta no podríamos estar hablando del impacto de Internet en la actualidad. La segunda, es consecuencia de la anterior, es decir, la conexión se produce por distintas acciones representadas en la interactividad, a través de la cual, se ponen en funcionamiento nuevas formas de relaciones a escala mundial. Y, por último, la tercera constante, que se produce cuando la información se configura por la hipermedialidad, es decir, el acceso interactivo a cualquier componente informacional dentro de la Red, desde cualquier parte.

El ciberespacio es una nueva forma de perspectiva. No coincide con la perspectiva audiovisual que ya conocemos. Es una perspectiva completamente nueva, libre de cualquier referencia previa: es una perspectiva táctil. Ver a distancia, oír a distancia: esa fue la esencia de la antigua perspectiva audiovisual.

Pero tocar a distancia, sentir a distancia, equivale a cambiar la perspectiva hacia un dominio que todavía no se abarca: el del contacto, el contacto a distancia, el telecontacto.

Robo de identidad

El robo o usurpación de identidad es el hecho de apropiarse la identidad de una persona haciéndose pasar por ella, llegando a asumir su identidad ante otras personas, en un lugar público o privado, en general para acceder a ciertos recursos o la obtención de créditos y otros beneficios en nombre de esa persona. Por otro lado, el robo de identidad también es utilizado con el fin de perjudicar a una persona, es decir difamarlo o manchar su nombre con diversos fines que el criminal busque. El caso más común hoy en día se da cuando un atacante, por medios informáticos o personales, obtiene su información personal y la utiliza ilegalmente.

El robo de identidad es el delito de más rápido crecimiento en el mundo. Hasta no hace mucho tiempo, cuando un ladrón nos robaba la billetera o porta documentos, el dinero era lo único que pretendía.

Eso está cambiando, ahora lo más valioso es el número de su documento, tarjeta de crédito, de débito, cheques y cualquier otro documento que contenga sus datos personales.

En el transcurso de un día normal, usted divulga esta información al hacer transacciones en persona, por teléfono y online para efectuar la compra de productos y servicios. Si esta información confidencial cae en manos de un delincuente, podría utilizarse para robarle su identidad financiera y realizar muchas de las actividades en nombre suyo. Nadie está a salvo de este delito ni podemos tener la certeza de que nunca le robarán su identidad, lo importante es conocer los métodos existentes para reducir las probabilidades de que usted se convierta en una víctima y qué medidas puede tomar si llegara a ocurrir. Lamentablemente, la mayoría de las personas no se enteran que han sido víctimas de robo de identidad hasta que solicitan un crédito y se los niegan, quieren contratar el servicio de telefonía celular y no pueden y en la mayoría de los casos, cuando aparecen cobros sospechosos en los resúmenes de las tarjetas de crédito. Con el desarrollo de las nuevas tecnologías, el robo de identidad se ha convertido en la modalidad delictiva que más ha crecido en los últimos años.

Métodos utilizados

Existen varios métodos para obtener datos de su información personal:

Phishing y correos falsos. Esta técnica permite pasar a un atacante por una organización, banco o empresa verdaderas para obtener información que garantice acceso a algún recurso que usted utilice en esa organización, banco o empresa.

Personal. Cualquier persona maliciosa podría obtener información que escuchó o vio de parte suya que le garantice acceso a algún recurso valioso.

Ataque organizado. Cualquier atacante podría intentar superar la seguridad de un banco, empresa u organización para obtener información personal de los clientes para luego acceder a algún recurso de esa empresa.

Cibercultura

Cibercultura es la cultura que emerge, o está emergiendo, del uso del ordenador para la comunicación, el entretenimiento y el mercadeo electrónico. Cultura nacida de la utilización de las nuevas tecnologías de la información y comunicación como internet. Cultura basad a en las ventajas y desventajas de la libertad absoluta, el anonimato, y ciberciudadanos con derechos y obligaciones.

Es un neologismo que combina las palabras cultura y el prefijo ciber, en relación con la cibernética, así como lo relacionado con la realidad virtual. Son las Tecnologías de la información y la comunicación las que han generado una gran revolución en la manera de acceder, apropiarse y transmitir la información, generando nuevos desarrollos sociales, políticos y económicos, que es lo que el común de la gente interpreta como cibercultura. Según Derrick de Kerckhove, es desde el computador donde se ha configurado un lenguaje universal: el digital. La cibercultura se puede apreciar desde tres puntos de vista:

a) **Interactividad**, que es la relación entre la persona y el entorno digital definido por el hardware que los conecta a los dos;

b) **Hipertextualidad**: que es el acceso interactivo a cualquier cosa desde cualquier parte. Es una nueva condición de almacenamiento y entrega de contenidos;

c) **Conectividad**: que es lo potenciado por la tecnología, por ejemplo, internet.

Manifestaciones de la cibercultura

La cibercultura incluye varias interacciones humanas mediadas por la red de computadores, como son actividades, ocupaciones, juegos, lugares y metáforas, e incluyen una variedad de

aplicaciones informáticas. Algunas son ofrecidas por especialistas en software y otras son protocolos propios de internet:

Blogs	Juegos de rol	Pornografía
Redes sociales	Televisión interactiva	Foros de discusión
Wikis	Agregadores noticias	
Juegos en línea	Comercio electrónico	

Ergonomía

Ergonomía es el estudio de todas las condiciones de adaptación recíproca del hombre y su trabajo, o del hombre y una máquina o vehículo. En particular, ergonomía computacional es el estudio de las condiciones de comodidad en las que el hombre trabaja con una computadora y la adaptación y facilidades que ésta aporta para una mayor comodidad del hombre.

En nuestro caso el uso de la computadora como una herramienta más de trabajo ha tenido un crecimiento explosivo en los últimos años. Es por eso que, si pasamos varias horas frente a la computadora, lo más probable es que se sienta algún tipo de molestia en la espalda, los ojos o en otras partes del cuerpo, para evitarlo es aconsejable tomar ciertas precauciones como utilizar productos ergonómicos, por ejemplo: el teclado, el monitor, la silla, etc. Cuando se diseñan productos informáticos esto se realiza de acuerdo con las normas ergonómicas, para adaptarse al hombre ya que el ser humano, no está preparado para trabajar con luz artificial; o para sentarse frente a un monitor varias horas al día; esto puede perjudicar la salud, trayendo como consecuencias: dolor de hombros, espalda, muñecas, manos y fatiga visual si no se toman las medidas adecuadas. Podemos prevenir estos problemas si considerásemos por lo menos:

- Situar el monitor en línea recta a la línea de visión del usuario, para que la pantalla se encuentre la misma altura de los ojos. De esta manera no tendrá que doblar el cuello para mirarla.
- Mantener una distancia de 50 o 60 cm. entre la persona y el monitor o a una distancia equivalente a la longitud de su brazo.
- Bajar el brillo del monitor para no tener que forzar la vista.
- Evitar que la luz del ambiente produzca reflejos sobre la pantalla; en todo caso, cambiar la posición del monitor, o disminuir la iluminación del ambiente.
- El asiento debe tener una altura que mantenga un ángulo de 90°, evitando así el dolor en las cervicales, lumbagos o problemas de disco; además debe tener un respaldo que permita apoyarse correctamente.
- Al digitar, los antebrazos y las muñecas deben formar una misma línea y los codos tienen que estar a ambos lados del cuerpo.
- Es bueno hacer un descanso de 5 minutos por cada hora de trabajo y hacer una serie de ejercicios sencillos como por ejemplo pararse derecho y levantar los hombros lentamente varias veces; o para relajar el cuello inclinar la cabeza hacia la izquierda y la derecha, intentando tocar el hombro con la oreja.

Resguardo de Identidad

Contraseñas seguras

Contraseñas muy comunes y poco seguras.

• 123456
• Password
• 1234
• 12345678
• Qwerty
• Football
• Dragon
• 111111
• Abc123

¿Qué notan de estas contraseñas?
¿Cuántas sólo contienen números? ¿Cuántas sólo letras?
¿Cuán extensas son estas contraseñas?
¿Pueden sugerir otras malas contraseñas?
¿Cuáles son las ventajas y desventajas de crear contraseñas fáciles de recordar o contraseñas difíciles de adivinar?
¿Crees que es seguro usar la misma contraseña para todas las cuentas? ¿Por qué no?

Elementos a tener en cuenta para crear buenas contraseñas a partir de la información que se presenta en la tabla:

SI	NO
Usa al menos 6 caracteres, idealmente 8.	No uses información de tu identidad en la contraseña (nombre, dirección, correo electrónico, número de teléfono o de documento.
Combina letras, números, símbolos, mayúsculas y minúsculas.	No uses una contraseña fácil de adivinar como el nombre de tu mascota o tu fecha de nacimiento
Usa contraseñas distintas para cada cuenta importante que tengas.	No compartas tus contraseñas con nadie, excepto tus padres o adultos de confianza.
Intenta cambiar tu contraseña con regularidad, en lo posible, cada 6 meses	No escribas tu contraseña para recordarla y, si vas a hacerlo, guarda el papel en un lugar seguro.

Métodos para crear contraseñas fuertes y fáciles de recordar:

Método 1 (nivel básico)

1. Piensa en una frase que te resulte divertida y fácil de recordar. Puedes utilizar el título de tu canción, libro o película favorita, tu equipo de fútbol, etc.

2. Toma la primera letra de cada palabra en la frase.

3. Cambia algunas letras por símbolos

4. Usa algunas letras mayúsculas y otras minúsculas.

A continuación, un ejemplo:

Frase: Mi prima Laura tiene dos perros y un gato

Contraseña: MpLt2P&1g

Método 2 (nivel avanzado)

1. Piensa en una contraseña maestra súper fuerte basada en una frase

2. Modifícala para cada sitio o aplicación que uses...de una forma que sólo vos sepas.

A continuación, un ejemplo:

Frase: Mis papás juegan cartas dos veces por semana

Contraseña maestra: mPjC#2vS

Sitio web: Gmail

Contraseña para Gmail: mPjC#2vGMsAIL

Engaño virtual

Cómo reconocer un engaño virtual	
¿Ofrece algo de manera gratuita?	Las ofertas gratuitas o demasiado buenas para ser ciertas suelen ser un engaño para acceder a tu información personal. Por ejemplo, los "tests de personalidad" son una forma de conocer información sobre vos para que resulte más fácil adivinar tu usuario y contraseña.
¿Solicita el envío de datos personales?	La mayoría de los negocios legítimos nunca solicitan el envío de información personal (números de cuenta, contraseñas, identificación, etc.) por correo electrónico.
¿Se trata de un mensaje en cadena?	Los mensajes en cadena pueden ponerte en riesgo. No los reenvíes a tus contactos.

Cómo evitar un engaño virtual	
Piensa antes de hacer clic.	No hagas clic en ningún enlace o archivo adjunto en un correo que parezca sospechoso.
Evita los concursos en los mensajes emergentes (pop-ups).	Es improbable que ganes el concurso. Por lo general, estos mensajes buscan recolectar información personal o infectar tu computadora con software malicioso.
No respondas correos que solicitan el envío de información personal.	Realiza una búsqueda del nombre de la empresa en la web antes de dar cualquier información personal.
Lee la letra chica.	la página puede decir que ganaste una Tablet pero si lees la letra chica verás que hay que pagar $200 al mes para obtenerla.

¡Oh, no! caí en la trampa. ¿Qué debo hacer?	
Avisa a un adulto de confianza.	Mientras más demores, más graves pueden ser las consecuencias.
Si estás preocupado por tu cuenta bancaria o tarjeta de crédito.	Contacta al banco o la tarjeta de crédito inmediatamente por teléfono.
Si recibiste una estafa por correo electrónico o en tu red social	Márcala como “correo basura” o “spam” en tu correo o repórtala en tu red social.

Encriptación

Encriptación: consiste en cifrar la información de manera tal que sólo quien tiene acceso al código secreto puede leerla. la encriptación es un método muy antiguo y se ha utilizado con diversos fines. Por ejemplo, la leyenda cuenta que en la Antigua Grecia cada vez que un general deseaba enviar un mensaje secreto a la ciudad, solicitaba rasurar la cabeza de un soldado para escribir el mensaje en su cuero cabelludo. Tan pronto el cabello crecía, el mensaje quedaba oculto en la cabeza del soldado. De esta forma, cuando llegaba a la ciudad, el oficial sabía cuál era el “código secreto”: rasurar la cabeza del soldado para revelar el contenido del mensaje.

Hoy en día, la encriptación es fundamental para el comercio electrónico y el inicio de sesión porque permite enviar información confidencial de manera segura entre servidores. los sitios web encriptan la información mediante un método llamado ‘SSL’ (en inglés: Secure Socket layer). Puedes identificarlo cuando aparece un candado verde en el margen izquierdo de la barra del navegador y la URL comienza con la leyenda HTTPS:// (‘S’ significa seguro).

NIVELES DE CONEXIÓN	
 Candado verde	La conexión está encriptada y la identidad del sitio fue verificada.
 Candado gris o ausencia de candado	La conexión al sitio puede estar encriptada, pero Google Chrome encontró algo en la página, como imágenes inapropiadas o anuncios. Se recomienda no ingresar información personal.

 Candado rojo	Hay problemas con el certificado del sitio. Procede con cautela porque alguien en la red (por ejemplo: alguien que usa tú mismo WiFi) podría poner tu información en peligro. Si ingresas información personal en el sitio, como tu tarjeta de crédito o contraseña, otras personas podrían verla.

Actividad: Realizar el apunte correspondiente, en su libreta de apuntes, cuidando de la ortografía y gramática, utilice ilustraciones elaboradas por usted para acompañar al texto. Sumado, se le invita a realizar la lectura en tres ocasiones o más para que pueda comprenderla ya que será el medio para elaborar una serie de cuestionamientos. El apunte será entregado y revisado en la sesión más próxima.

¡Excelente descanso!

No hagas para pensar, piensa para hacer