1.1. Conceptos básicos

En la actualidad los centros escolares utilizan para la creación, procesamiento, transmisión y almacenamiento de su información las ventajas de las Tecnologías de la Información y las Comunicaciones - TIC. Debido a esto, el número de amenazas se incrementa y obliga a que garantizar la disponibilidad, confidencialidad e integridad de la información signifique un aspecto de primer orden sobre el cual invertir para evitar las amenazas, las pérdidas, modificación o robo de los activos informáticos.

La falta de control y deficiencia de una política de seguridad informática son un atractivo para los cibercriminales. Los centros educativos mantienen depósitos de datos sensibles, incluyendo información financiera y estadística. Gracias a la falta de personal capacitado, la falta de inversión y la no adecuada implementación de soluciones de seguridad. La información académica es bastante atractiva para alguien que quisiera atacar a los Docentes y Estudiantes: (Notas, número de cédula, tipos de financiación y en general información sensible).

De acuerdo con el reporte "Internet Security Threat Report" Symantec, el sector educativo se encuentra en el tercer puesto de reporte de brechas de seguridad y en noveno lugar de entidades expuestas a brechas. Los ataques informáticos más importantes se deben principalmente a aspectos como las vulnerabilidades de software, malware, dispositivos móviles, personal interno y hackers, los cuales acaparan alrededor del 69% del total de las incidencias de seguridad atendidas por los especialistas encuestados, según un estudio de International Information Systems Security Certification Consortium (ISC2) (SUBY, 2013).

Cada vez más docentes solicitan información para comprender lo que está ocurriendo y diseñar estrategias de abordaje, porque advierten que los chicos desconocen los riesgos de la sobreexposición e ignoran el uso que las empresas de software hacen con los datos que se "regalan" al postear. En ámbitos educativos advierten, también, situaciones angustiantes de niños que son víctimas de hackers que los inducen, bajo amenaza, a la autoflagelación (como ocurrió con el juego de la Ballena Azul o de Momo, un personaje en el chat de juegos infantiles).

Las escuelas, donde se concentra la población más vulnerable a las redes y a los delitos sexuales virtuales, se sienten solas a la hora de trabajar estos tópicos, ya que la currícula obligatoria no incluye los conceptos de programación para comprender y prevenir. El gran número de casos de cibercrímenes contra niños y jóvenes, la escasa formación de los docentes en el tema, la poca oferta formativa en las escuelas y una sociedad que aún debate la legitimidad de formar en educación sexual.

Se entiende la seguridad como un proceso que nunca termina ya que los riesgos nunca se eliminan, pero se pueden gestionar. De los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica, y por ese motivo nunca se eliminan en su totalidad, su impacto se minimiza.

La seguridad siempre busca la gestión de riesgos, esto quiere decir que se tenga siempre una forma de evitarlo o prevenirlo y que se pueda realizar ciertas acciones para evitar esas situaciones de la mejor forma. Se definió que la seguridad podría ser catalogada como la ausencia de riesgo, la definición de este término involucra cuatro acciones que siempre están inmersas en cualquier asunto de seguridad como son:

- Prevención del riesgo.
- Transferir el riesgo
- Mitigar el riesgo
- Aceptar el riesgo

La seguridad informática se encarga de la seguridad del medio informático, según varios autores la informática es la ciencia encargada de los procesos, técnicas y métodos que buscan procesar almacenar y transmitir la información, mientras tanto la seguridad de la información no se preocupa sólo por el medio informático, se preocupa por todo aquello que pueda contener información, en resumen, esto quiere decir que se preocupa por casi todo, lo que conlleva a afirmar que existen varias diferencias, pero lo más relevante es el universo que manejan cada uno de los conceptos en el medio informático.

Según Aguilera (2011), se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad.

La principal tarea de la seguridad informática es la de minimizar los riesgos, en este caso provienen de muchas partes, puede ser de la entrada de datos, del medio que transporta la información, del hardware que es usado para transmitir y recibir, los mismos usuarios y hasta por los mismos protocolos que se están implementando, pero siempre la tarea principal es minimizar los riesgos para obtener mejor y mayor seguridad.

Lo que debe contemplar la seguridad informática se puede clasificar en tres partes como son los siguientes: los usuarios, La información, y La infraestructura.

Los usuarios son considerados como el eslabón más débil de la cadena, ya que a las personas es imposible de controlar, un usuario puede un día cometer un error y olvidar algo o tener un accidente y este suceso puede echar a perder el trabajo de mucho tiempo, en muchos casos el sistema y la información deben de protegerse del mismo usuario.

La información se considera como el oro de la seguridad informática ya que es lo que se desea proteger y lo que tiene que estar a salvo, en otras palabras, se le dice que es el principal activo. La seguridad de la información consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, también pueden estar involucradas otras propiedades, como la autenticidad, responsabilidad, la confiabilidad y el no repudio.

Existen tres principios que debe respetar la gestión de la información en cualquier empresa para poder cumplir, de forma correcta, los criterios de eficiencia y eficacia. Un sistema de información se define como seguro, según la regla ISO 27002, si cumple con los elementos básicos de la seguridad informática: integridad confidencialidad, y disponibilidad, ver imagen 1.

La integridad de los datos: supone que la información se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización. El objetivo de la integridad es prevenir modificaciones no autorizadas de la información.

La disponibilidad del sistema: supone que el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información deberá permanecer accesible a elementos autorizados.

La confidencialidad: requiere que la información sea accesible de forma única a las personas que se encuentran autorizadas. Es necesario acceder a la información mediante autorización y control. La confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos. El objetivo de la confidencialidad es, prevenir la divulgación no autorizada de la información sobre nuestra organización.

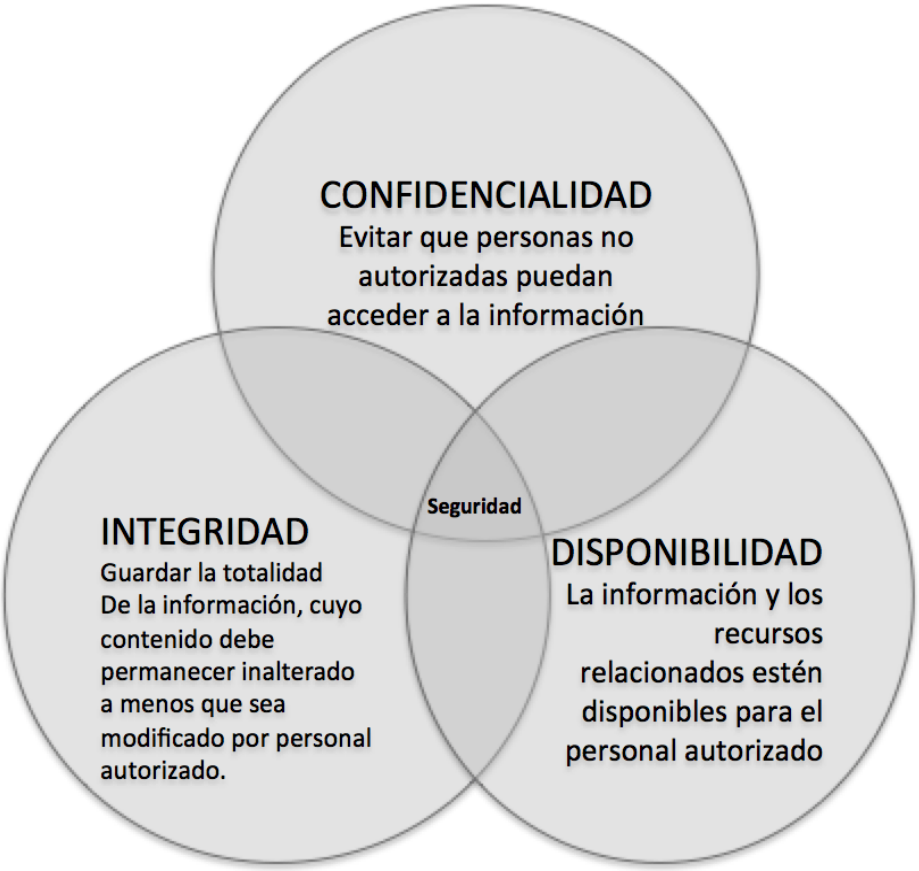

Imagen 1. Seguridad de la información
Fuente: Elaboración propia

Por último, está la infraestructura esté puede ser uno de los medios más controlados, pero eso no implica que sea el que corre menos riesgos, siempre dependerá de los procesos que se manejan. Se deben de considerar problemas complejos, como los de un acceso no permitido, robo de identidad, hasta los daños más comunes, por ejemplo, robo del equipo, inundaciones, incendios o cualquier otro desastre natural que puede tener el material físico del sistema de la organización.

Aguirre (2006), también afirma que la seguridad informática puede definirse como el conjunto de métodos y de varias herramientas para proteger el principal activo de una organización como lo es la información o los sistemas ante una eventual amenaza que se pueda suscitar.

Se puede decir que un sistema es fiable si funciona correctamente, es decir, realiza las funciones para las que fue diseñado, es confidencial si la información es accesible solamente para las personas autorizadas, íntegro si el contenido de la información transmitida no se altera o se altera solamente por personal autorizado, y está disponible si el sistema funciona y si los usuarios tienen acceso a todos los componentes del sistema, aunque sea con diferentes niveles de seguridad.

Otra cualidad que debe cumplir un sistema seguro es el de no repudio. Esta cualidad se puede aplicar tanto en origen como en destino. Por una parte, debe garantizar al emisor que la información fue entregada al receptor (no repudio en destino) y por otra, ofrece una prueba al receptor del origen de la información recibida, el emisor no puede negar que emitió el mensaje (no repudio en origen).

Esta cualidad es muy importante en el comercio electrónico para garantizar las transacciones realizadas y las entidades participantes, aplicándose en los dos lados de la comunicación, no poder rechazar la autoría de un mensaje, ni negar su recepción.

1.2. Identidad digital

Debemos a Timothy John Berners-Lee que hoy en día podamos navegar a través de Internet, la autopista de la información. Berners-Lee ideó las líneas maestras sobre las cuales se sustenta la navegación web, gracias a su protocolo HTTP (Hypertext Transfer Protocol) que hace posible la visualización de las páginas web, y al lenguaje HTML (Hypertext Markup Language) con el que se programan esas páginas; estos nos permiten viajar por internet tal como lo conocemos hoy.

Al principio de la era de Internet, las páginas web eran sitios en los que la información sólo corría de forma unidireccional; es decir que tanto los contenidos como la información eran desarrollados por los administradores de las páginas web, llamados webmasters, quienes decidían, en primera y última instancia, cómo serían el contenido y la información que se mostraría en cada página web, de modo que solo existían dos roles en Internet: los webmaster y los usuarios o consumidores de la información que contenía la red. Ver tabla 1.

En la última década del siglo XX y principios de siglo XXI asistimos a una auténtica revolución. La dictadura de los webmaster ha sido quebrada, la revolución de los internautas ha generado un cambio actitudinal y surge un nuevo concepto, "Web 2.0", acuñado por Tim O´Reilly, quien lo basa en siete principios fundamentales que explica durante una conferencia en 2004 (Velich, Huel, Bastidas, & Fernández, 2010).

Tabla 1. Evolución de la Internet

Web 1.0	Web 2.0	Web 3.0	Web 4.0
Páginas estáticas para el usuario que la visita El uso de framesets o marcos. Extensiones propias del HTML como el parpadeo y las marquesinas, etiquetas introducidas durante la guerra de los navegadores. Libros de visitas en línea o guestbook Botones gif. Formularios HTML enviados vía email.	La Web es una plataforma La información es lo que mueve Internet Los efectos de Internet son a su vez movidos por la participación (Identidad digital) Las distintas características de la red pueden desarrollarse de manera independiente	Está relacionada con una visión en tres dimensiones de la web, abriendo nuevas formas de comunicación y colaboración utilizando espacios tridimensionales. Ya no solo se accede a la web desde el navegador, sino que se hace uso de otros dispositivos y tecnología inteligente. En la web 3.0 el contenido y el conocimiento se relacionan de manera más eficiente.	Comprensión del lenguaje cotidiano o natural. Comunicación entre dispositivos (m2m, máquina a máquina). Uso de información relacionada (GPS, sensores de temperatura, etc.). Nuevas formas de interacción con el usuario.

Desde las últimas décadas del siglo pasado, se ha producido una revolución tecnológica a escala mundial que ha dado paso a una sociedad informacional, definida por la generación, la gestión y el uso de datos. La revolución actual gira en torno a las tecnologías del procesamiento de la información y la comunicación, que, cada vez más, se usan en la mayoría de ámbitos de nuestra vida (Castells, 2003). Con la eclosión de Internet y sobre todo de la denominada web 2.0, la cantidad de datos personales existentes en la red es muy elevada y contribuye a crear nuevas identidades personales en el entorno digital que, como veremos, pueden coincidir o no con la identidad analógica, es decir, con las características que se pueden atribuir a una determinada persona en su vida fuera de la red o offline. La irrupción de Internet ha ofrecido una gama amplísima de nuevas herramientas para la creación de contenidos y de comunicación cambiando las condiciones tradicionales de gestión de la identidad (Zhao et al., 2008).

Actualmente, la capacidad de enviar y gestionar datos aumenta y el consumo informativo no sólo es ingente en empresas y en el ámbito comercial, sino que la cantidad de datos que un individuo genera, gestiona, edita o comparte cada día es difícilmente calculable. Ante la gran abundancia de información y de la sobreexposición a los demás, el individuo queda desprotegido. Es por ello que recientemente se ha reactivado el debate sobre la necesidad de formar a las personas en nuevas alfabetizaciones (Livingstone, 2004), informacionales y digitales, que se convierten en clave para los ciudadanos de hoy.

La Identidad Digital es el conjunto de informaciones publicadas en Internet sobre mí y que componen la imagen que los demás tienen de mí: datos personales, imágenes, noticias, comentarios, gustos, amistades, aficiones, etc. Todos estos datos me describen en Internet ante los demás y determina mi reputación digital, es decir, la opinión que los demás tienen de mí en la red. Esta identidad puede construirse sin que se corresponda exactamente con la realidad. Sin embargo, lo que se hace bajo esa identidad digital tiene sus consecuencias en el mundo real y viceversa.

Más aún, la presente revolución comunicativa también ha generado una traslación de nuestras relaciones sociales al ambiente digital, a Internet. Hemos dispuesto retazos de nuestra personalidad, a veces más de los necesarios, en Internet. Hoy en día es tan importante establecer relaciones sociales en el mundo digital como lo es en el físico

INTECO (Instituto Nacional de Tecnologías de la Comunicación): "conjunto de la información sobre un individuo o una organización expuesta en Internet (datos, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha persona en el plano digital" (INTECO, 2012a, pág. 5).

Identidad digital e Identidad 2.0 (ID) es el conjunto de métodos para generar una presencia en la web de una persona o empresa en Internet. Esa presencia podría reflejarse en cualquier tipo de contenido que se refiere a la persona o negocio. Esto incluye noticias, la participación en blogs y foros, sitios web personales, presencia en Social Media, imágenes, vídeo, etc.

Características de la identidad digital:

- **Social.** Se construye navegando por las redes sociales a partir del reconocimiento de los demás sin ni siquiera llegar a comprobar si esa identidad es real o no.
- **Subjetiva.** Depende de cómo los demás perciban a esa persona a través de las informaciones que genera.
- **Valiosa.** A veces personas y empresas navegan por las redes sociales para investigar la identidad digital de un candidato y tomar decisiones sobre él/ella.
- **Indirecta.** No permite conocer a la persona directamente sino las referencias publicadas de esa persona.
- **Compuesta.** La identidad digital se construye por las aportaciones de la misma persona y también por otras personas sin la participación o consentimiento del mismo.
- **Real.** La información de la identidad digital puede producir efectos positivos y negativos en el mundo real.
- **Dinámica.** La identidad digital no es una foto instantánea, sino que está en constante cambio o modificación.

Además, la Identidad 2.0, también llamada identidad digital, es la revolución anticipada de la verificación de la identidad en línea, utilizando tecnologías emergentes centradas en el usuario tales como el standard OpenID o Microsoft Windows CardSpace. Se encuentra dentro de la teoría de la Web 2.0, donde destaca de un modo simple y abierto los métodos de identificación en transacciones cuyos procesos sean similares al mundo real, como por ejemplo un carnet de conducir.

Un sistema de identidad 2.0 permitiría a los usuarios usar una única ID, transparente y flexible en vez de usar múltiples nombres de usuario y contraseñas para registrarse en sitios web. La identidad 2.0 está centrada en el usuario. Requiere transacciones identificadas entre usuarios y agentes (páginas web) usando datos verificables, proporcionando así transacciones a las que sea más fácil seguir el rastro.

¿Por qué debo tener una identidad digital?

Los especialistas en marcas (branding) te dirán que todos somos marcas. Internet nos permite estar 24 horas on-line, ofreciendo nuestros productos o servicios. Imagina que eres un escritor o artista y tus libros u obras están a la venta durante 24 horas, los 7 días de la semana. ¡Fantástico!, ¿verdad? Tener una identidad digital también es rentable por el hecho de que cada vez más nos buscan por Internet.

¿Para qué debo tener una identidad digital?

Entre los principales objetivos está maximizar nuestra presencia y ofrecer referencias on-line positivas sobre una persona o empresa específica, dirigidas no sólo a los usuarios que buscan activamente a esa persona en cualquier motor de búsqueda, sino también a los que eventualmente pueden llegar a hacer referencia a una persona mientras navega por la web.

Reputación on-line

¿Qué se dice de nosotros? ¿Dónde? ¿Por qué? Es importante saber qué sucede y qué se comenta respecto a nuestra empresa. Esta información nos ayudará a saber qué estamos haciendo y poder potenciarlo o corregirlo. En ocasiones no estaremos de acuerdo, y aunque lo más importante es que nos van a citar, sin embargo, tenemos que saber en parte y de qué modo está ocurriendo.

¿Cómo proteger nuestra identidad digital?

El robo de identidades digitales es uno de los ciberdelitos más frecuentes. Si te roban tu identidad digital, además de que el ciberdelincuente puede acceder a tus cuentas bancarias o realizar compras en tu nombre, también puede dañar tu reputación en las redes sociales.

Para proteger tu identidad personal en la red, primero debes de ser muy consciente de que el robo de identidades digitales está a la orden del día. Mañana podría pasarte a ti. Y segundo, es muy recomendable que pongas en práctica los siguientes consejos:

1. No utilices redes wi-fi desprotegidas o públicas. Las redes wi-fi gratuitas, que ofrecen en bares, restaurantes o cafeterías, o las redes wi-fi públicas no suelen tener cifrado WPA o WEP, con lo cual no son seguras. Por eso, si tienes que conectarte a algún tipo de servicio que contenga tus datos personales, o información personal sensible, no utilices estas redes. Si debes hacerlo, al menos asegúrate de que puedes navegar de forma segura, accediendo sólo a páginas que usen el protocolo https.

2. No utilices páginas web desprotegidas. A pesar de que puedas estar usando una WI-FI privada, también es importante que sólo navegues por páginas web que utilicen el protocolo https (Protocolo Seguro de Transferencia de Hipertexto). Este protocolo significa que la información que circula a través de estas páginas web está encriptada, con lo cual nadie la pueden interceptar.

3. Utiliza contraseñas seguras y cámbialas regularmente. Para todos quienes tenemos conocimientos básicos de informática, las contraseñas son nuestro principal recurso para proteger nuestra identidad digital. Y quizás no les damos la relevancia que tienen. Las contraseñas seguras deben tener como mínimo 16 caracteres, combinar mayúsculas, minúsculas y caracteres alfanuméricos. Y no se debe utilizar la misma contraseña para dos servicios distintos.

Como es difícil memorizar todas las contraseñas que utilizamos, sobre todo si empezamos a utilizar contraseñas seguras, es muy recomendable utilizar un gestor de contraseñas.

4. Actualiza tu software regularmente. Tanto si utilizas Windows como Mac, los sistemas operativos se actualizan con cierta frecuencia. Cada vez que se lanza una nueva actualización de software, aparece un aviso en tu ordenador que te pregunta si quieres proceder a actualizarlo. (En algunos casos se actualiza de forma automática). Es importante no demorar el proceso de actualización del software de tu ordenador, aunque ello suponga tener que reiniciarlo y esperar unos minutos. Cada actualización supone una versión del software mejorada, incluyendo un refuerzo en su seguridad.

5. Repasa los permisos y las políticas de privacidad. Todas las redes sociales que utilizas tienen su política de privacidad, y actualmente todas te permiten que controles lo que quieres que se publique sobre ti. Repasa esas políticas de privacidad y revisa los permisos que concedes a cada red social. Quizás no te interesa tener perfil público en Instagram o quizás quieres aprobar cada foto en la que se te etiqueta en Facebook, para decidir si aparece o no en tu muro.

6. Monitoriza tu nombre regularmente. Seguramente ya habrás buscado alguna vez tu nombre en Google para ver lo que el buscador sabe sobre ti (y lo que puede saber todo el mundo). Es recomendable monitorizar tu nombre en Google cada cierto tiempo, para comprobar que tú sigues teniendo el control de todo lo que aparece sobre ti en la red. Es decir, que tú has permitido que aparezca. Esto está muy relacionado con el punto anterior.

7. La gestión de la identidad digital. En una sociedad intensamente informatizada, uno de los peligros existentes es la diferencia entre los que tienen acceso a las nuevas tecnologías y los que no, así como el abismo entre los que saben utilizarlas y los que no. Estos últimos se convierten en el nuevo sector en riesgo de exclusión social, fenómeno denominado brecha digital.

Para evitar la marginación que esta fractura conlleva es necesario que los ciudadanos desarrollen habilidades informacionales y digitales. Podemos diferenciar entre las habilidades más básicas, como saber leer o gestionar un documento digital, y las habilidades más avanzadas, como coordinar un equipo de trabajo que no puede reunirse presencialmente o hacer trámites a través de la administración electrónica. Entre las nuevas competencias que el ciudadano del siglo xxi debe adquirir, está la competencia de gestionar eficazmente la propia identidad digital.

¿Cómo se construye una identidad digital? De forma activa, se realiza aportando textos, imágenes y vídeos a Internet, participando, en definitiva, del mundo web. En los sitios de redes sociales1, se construye a partir de un perfil de usuario, que a menudo se enlaza a perfiles de otros usuarios o contactos. Una identidad digital bien gestionada y homogénea con la identidad analógica no sólo repercute en una vida más activa en todos los ámbitos, sino que también tiende a consolidar un entramado social más sólido fuera de Internet. Sin embargo, la construcción de la identidad digital está ineludiblemente ligada al desarrollo de habilidades tecnológicas, informacionales y una actitud activa en la red, participativa, abierta y colaborativa.

La identidad digital se puede configurar de muchas maneras y una misma persona puede tener diferentes identidades utilizando herramientas diversas o tener sólo una. A partir de Gamero (2009) se presentan una serie de herramientas gratuitas y accesibles en la red, a través de las cuales cualquier persona puede vertebrar una identidad digital. Ver imagen 1.

- Blogs.

El nombre de blog o bitácora proviene de la navegación y se refiere al diario de un barco. Extrapolado a nuestros días, un blog ha pasado a ser un diario que tanto puede ser personal como corporativo. Un ejemplo de blog que contribuye a construir la identidad de su autor es el de Genís Roca.

- Microblogs.

Es una herramienta similar al blog, con la diferencia que tienen un número limitado de caracteres y que se pueden publicar a través de diversas aplicaciones, como vía SMS o por correo electrónico. Los usuarios de los microblogs, aparte de escribir micromensajes, pueden seguir a otras personas y conocer lo que hacen y comentan. Un ejemplo de un microblog con fuerte repercusión y vinculado a una persona física es el del presidente de Estados Unidos, Barack Obama, que tiene más de dos millones de seguidores. Ahí explica en qué está trabajando, qué está haciendo y qué piensa. Es un ejemplo de marketing y consolidación de su identidad digital en la red.

- Portales de noticias y sitios web.

Cualquier página web puede ser una plataforma a partir de la cual construir una identidad digital. Un ejemplo es el prestigioso portal de noticias y revista Wired, el cual permite a cualquier lector comentar una noticia. Estos comentarios son firmados (a menudo con pseudónimos) y pueden ser recuperados posteriormente en la red ya que buscadores como Google los indexan. Cuando se aportan comentarios y opiniones en Internet, hay que tener presente que estos mensajes se pueden encontrar a través de los buscadores y que difícilmente desaparecen de la red.

- Sitios de redes sociales genéricas o especializadas.

tales como Facebook, LinkedIn, XING o Pleiteando (esta última especializada en el mundo jurídico). El uso de las redes sociales se está extendiendo con rapidez. Sin embargo, el dominio sobre todos los aspectos que implican su uso no es generalizado. En relación a la gestión de la propia identidad, muchos sitios de redes sociales permiten que no se muestren algunos de los datos del perfil. Del mismo modo, la red Facebook permite restringir el acceso a ciertas informaciones, a usuarios concretos o a grupos de usuarios mediante la configuración de cada perfil.

- Textos, fotografías o vídeos en la red.

Con Google Docs, Picasa, Flickr, YouTube o Vimeo Todas las actividades en la red (visitas a la web, clics en un enlace, comentarios en un blog, colgar una foto o un vídeo...) quedan registradas y difícilmente se borran. El conjunto de todos estos pasos en Internet forma parte de la identidad digital de una persona, de quien posteriormente se pueden buscar y recuperar gran parte de las acciones, comentarios y opiniones que ha dejado en la red.

- El correo electrónico

Del mismo modo que no se borra el rastro a la red, en general, tampoco se borran los mensajes de correo electrónico, a pesar de que estén protegidos con una contraseña. Hay proveedores de correo electrónico que personalizan la publicidad que aparece en pantalla a partir el contenido de los mensajes electrónicos. Por ejemplo, si dentro del texto de un mensaje aparece la palabra "Londres" la publicidad personalizada podrá ser "Vuelos a Londres" o "Hoteles en Londres".

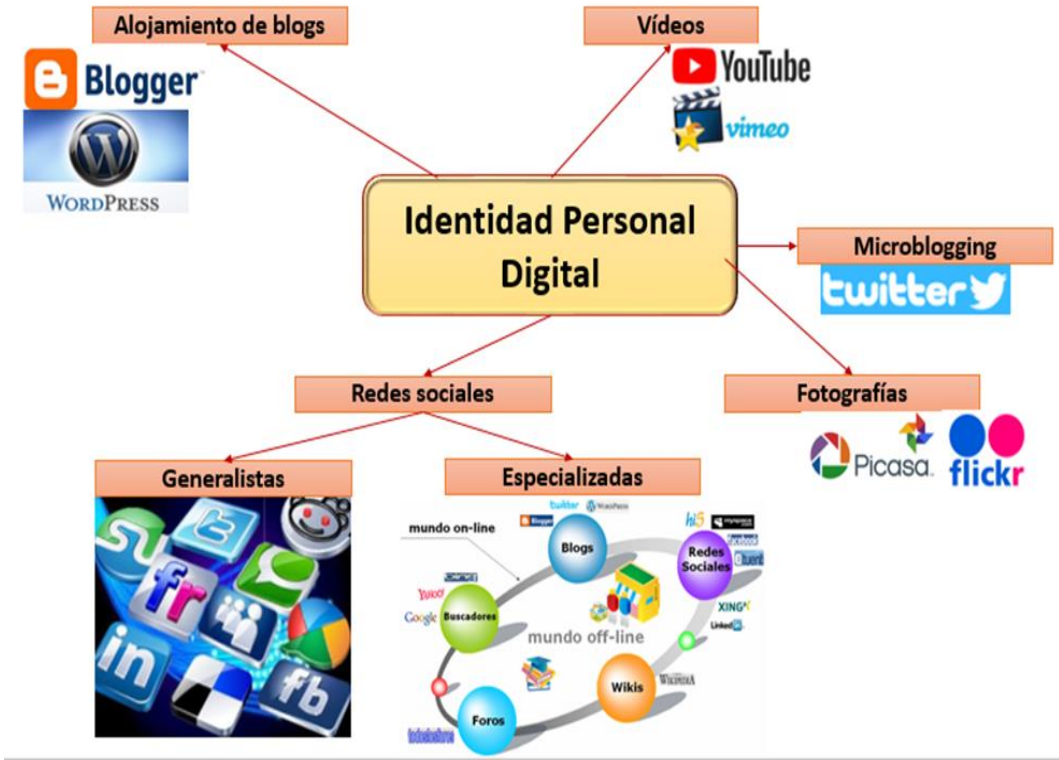

Imagen 1. Ejemplo de identidades digitales
Fuente: Elaboración propia

Ejemplos de herramientas y webs 2.0 con respecto a la identidad digital. En este apartado se muestran diferentes herramientas y sitios de la Web 2.0 estrechamente ligados con la identidad digital.

a) Herramientas para homogeneizar la propia presencia en la red

OpenID es una manera de autenticarse en las páginas web sin la necesidad de tener un usuario para cada una de las plataformas. Es así como permite que el usuario gestione su identidad digital de manera centralizada, evitando la esquizofrenia digital de utilizar diferentes identidades y que se tengan que memorizar grandes cantidades de información para identificarse en los diferentes servicios en línea. OpenID es abierto y defiende la autenticación única de los usuarios en la red. Hay empresas que al detectar también estas deficiencias han creado los propios servicios de autenticación, pero simplificando y mejorando la experiencia del OpenID.

Hay que tener cuidado, no obstante, porque el hecho de tener unificada la identidad digital hace que sea más vulnerable en caso de que alguien averigüe la contraseña de acceso

Facebook Connect es un gestor de identidades aplicable a diferentes páginas web a partir del cual cuando un usuario deja un comentario puede hacer que automáticamente quede reflejado también en su perfil de Facebook. De este modo puede compartir la información que encuentre de interés con los contactos de Facebook.

Google Friend Connect es un módulo ofrecido por Google para añadir una capa social en cualquier blog (parecido a Facebook Connect), al mismo tiempo también añade una autenticación desde otra cuenta como la de Twitter, de modo que los visitantes del blog podrán utilizarlo para twittear sin tener que salir del bloque.

b) Identificar perfiles de personas concretas. Estas herramientas sirven para autentificar que la persona es realmente quien dice que es.

Identify: agregado de Firefox para investigar personas
Identify es un complemento del navegador Firefox que busca todos los perfiles de un usuario a todos los sitios de redes sociales y los aglutina en una única interfaz (es preciso que el usuario haya elegido previamente un mismo nombre para identificarse). Una vez instalada la aplicación en el navegador Firefox, si se busca Oprah Winfrey, nombre de la popular presentadora americana, aparece como primer resultado su Twitter y se puede ver como Identify lo marca como "perfil verificado". Ciertamente, es su verdadero perfil por el número de seguidores que tiene, pero se encuentran más resultados si se busca por el mismo nombre, la mayoría de los cuales son identidades falsificadas de la popular presentadora.

c) Integrar mensajes de una plataforma a otra

Twit This ofrece una manera fácil de publicar una noticia de un blog en el canal de Twitter. Para hacerlo, es necesario que el blog o la web incluya la opción Twit This y sólo hay que hacer clic e identificarse en Twitter. Una vez hecho esto, el mensaje de un blog se puede publicar en el propio canal de Twitter y así hacerlo visible a todos los contactos de este canal. Además del Twit This, Twitter también ofrece un buscador que permite buscar en cada momento qué se dice sobre un tema en concreto. Los resultados son un conjunto de comentarios hechos por diferentes usuarios donde sale la palabra de búsqueda indicada. Hay también el Tweet Beep, un servicio de alertas al correo electrónico de todos los micromissatges que escriben los usuarios que lo siguen o el Tweet Later para hacer que los micromissatges lleguen más tarde a los usuarios. El uso se ha extendido hasta el punto de que hay gobiernos como el de Australia que alientan la población a utilizar herramientas como el Twitter o el Facebook en caso de alarmas de incendios o emergencias.

d) Integración de sitios de redes sociales

Friendfeed es una herramienta que permite desde un mismo lugar agregar toda la actividad en línea: las fotos que subimos, los vídeos, los posts que se escriben, los eventos donde nos apuntamos, la música que escuchamos como favorita, los enlaces que guardamos, etc. todo lo que sea susceptible de hacerse mediante una aplicación en línea. A todo esto, se le añade una capa social, con el que se puede seguir lo que hacen los demás usuarios y viceversa, filtrando las actividades que nos interesan y las que no.

e) Ejemplos de sitios de redes sociales

Sitios de redes sociales: Facebook, Tuenti, etc.

Los sitios de redes sociales se han popularizado muchísimo por ser herramientas que permiten mantener el contacto con los "amigos" que físicamente es difícil de mantener. Ha sido un fenómeno bastante generalizado en cuanto a edades y que ha afectado a todo el planeta. Los hay de genéricas (como Facebook o Tuenti) y especializadas. Entre las especializadas hay temáticas, como Pleiteando, red de personas relacionadas con el mundo de la justicia, de geográficas, como Migente, que incluye hispanos que viven en Estados Unidos; redes en que se comparten gustos musicales, como Last.fm, o videos, como YouTube. Lo que tienen en común todos estos sitios de redes sociales es que para registrarse el usuario crea el perfil digital. Últimamente, Facebook ofrece la posibilidad de personalizar el perfil de usuario, de manera que no aparezca una retahíla de números y letras sino una dirección URL más corta, más amigable, que contiene el nombre del usuario y que, por tanto, es más fácil de recordar.

Buscadores de identidades (Pipl.com, yasni.com o 123people.es)

Se han creado también sistemas que funcionan como buscadores, en los que poniendo el nombre de la persona que nos interesa el sistema busca todas las identidades que tenga en la web, ya sean vídeos, sitios de redes sociales, blogs, etc. Hay que tener presente, sin embargo, que en los buscadores de entidades como los mencionados surge el problema del ruido en la recuperación de nombres y apellidos comunes, ya que a menudo no hay una correspondencia unívoca entre el nombre y la identidad.

1.3. Robo de información

El robo de datos informáticos, ya se trate de robo de datos personales o de otra índole, independientemente del tipo de delito informático de que se trate, se producen como consecuencia de la falta de protección de esos datos que deben ser objeto de protección.

Los datos que se contengan en ficheros informáticos, personales, bajo la protección de la Ley de Protección de Datos Personales, o de otra índole de datos privados, por ejemplo, datos relacionados con un proyecto empresarial, mediciones, estructuras, etc., que son privados, pero no entran dentro del ámbito de la Ley de Protección de Datos, pero que evidentemente, por el interés de la empresa que los desarrolla, también los debe de considerar de gran importancia y por consiguiente proteger y confidencializar.

El robo de identidad o usurpación de identidad es la apropiación de la identidad de una persona: hacerse pasar por esa persona, asumir su identidad ante otras personas en público o en privado, en general para acceder a ciertos recursos o para la obtención de créditos y otros beneficios en nombre de esa persona.

:

Los ciberdelincuentes consiguen acceder a datos sensibles de muchas maneras y no siempre como consecuencia de un usuario imprudente: a veces los trucos son tan refinados que incluso un usuario especialmente concienciado y cuidadoso puede ser víctima de este tipo de delitos. Algunos de sus mecanismos incluyen:

Ataques de hackers: Las noticias sobre robos a gran escala de datos de usuarios y de datos bancarios no dejan de estar de actualidad. Incluso los usuarios más prudentes pueden ser víctimas de esta clase de delitos. Para algunos hackers es muy fácil acceder a cuentas protegidas con una contraseña débil, así como a aquellas cuentas que usan una misma contraseña. Algunos criminales pueden pasar de un perfil en las redes sociales a una cuenta en una tienda online donde se compre habitualmente, o donde se guarden datos bancarios.

Correos phishing o phishing E-Mails: La suplantación de identidad a través del correo electrónico es una de las variantes favoritas de los cibercriminales. Se trata de una forma de correo spam en la que el destinatario es "invitado" a pinchar en un enlace que le lleva a una copia de la página original, donde se le pedirán datos de acceso. De ser introducidos, estos pasarán directamente a manos de los estafadores.

Troyanos: Al descargar programas gratuitos u otra clase de archivos se corre el riesgo de infectar el ordenador con este tipo de virus; que se encargan principalmente de transferir datos privados a terceros. A menudo se esconden también en archivos adjuntos de correos spam.

Ingeniería social: esta práctica especialmente deshonesta consiste en manipular a un usuario para conseguir información confidencial que luego pueda ser utilizada con fines delictivos. De la misma manera que alguien se puede hacer pasar por el nieto de un anciano con problemas de memoria para hacerse con información sobre sus finanzas, también es posible, ganarse la confianza de otros usuarios en las redes sociales por medio de perfiles falsos para obtener acceso a datos confidenciales.

Un ejemplo de robo de información es el Robo de Identidad que se produce cuando una persona adquiere, transfiere, posee o utiliza información personal de una persona física o jurídica de forma no autorizada, con la intención de efectuar o vincularlo con algún fraude u otro delito. El robo de identidad es un delito grave. El robo de identidad se produce cuando alguien usa su información sin su permiso. Los ladrones de identidad podrían usar:

- Su nombre y domicilio.
- Los números de su cuenta bancaria o de tarjeta de crédito.
- Su número de Seguro Social.
- Los números de su cuenta de seguro médico.

¿Por qué debería preocuparme si alguien me roba la identidad?

Porque usted será responsable de lo que haga el ladrón mientras use su información personal. Usted podría tener que pagar lo que compre el ladrón. Esto es cierto aunque usted no sepa nada sobre las facturas.

¿Cómo puede suceder?

- Un ladrón podría obtener una tarjeta de crédito usando su nombre.
- El ladrón cambia el domicilio.
- Las facturas le llegan al ladrón, pero él nunca las paga.
- Eso significa que la compañía de tarjeta de crédito piensa que usted no está pagando las facturas.
- Eso dañará su crédito.

Tu correo a menudo contiene información delicada: si no tienes cuidad los delincuentes podrían obtenerla simplemente revisando tu basura. Es importante destruir todos los documentos que contengan información personal, antes de depositarlos en la caneca.

El robo de identidad también ocurre como resultado de la pérdida o el hurto de una billetera o de artículos personales, entre los que puede haber tarjetas de crédito o débito, pasaportes, licencias de conducción, cheques, cédulas de ciudadanía, etc. Si esto llegase a ocurrir, es importante denunciar la pérdida ante la policía, y reportar a los bancos o entidades crediticias.

Otra forma de robo de información incluye el uso de malware o spyware para obtener ilícitamente información de computadores, piratear redes, bases de datos, o como medio para suplantar organizaciones confiables, con el fin de obtener información personal. Activa contraseñas de acceso y usa un antivirus confiable para todos tus dispositivos.

Evita compartir información personal o números de cuenta por teléfono o en línea a través de chats o correo electrónico. Recuerda borrar toda la información personal de tus dispositivos tecnológicos antes de donarlos o venderlos.

¿Qué es lo que puede hacer un ladrón con mi información personal?

- Comprar cosas con sus tarjetas de crédito.
- Obtener nuevas tarjetas de crédito.
- Abrir una cuenta de teléfono, electricidad o gas
- Robarle su rembolso de impuestos.
- Obtener atención médica.
- Hacerse pasar por usted si lo arrestan.
- Pueden conseguir un empleo usando su número de Seguridad Social.
- Pueden alquilar una vivienda u obtener servicios médicos usando su nombre.
- Pueden darle información personal suya a la policía durante un arresto. Si no se presentan ante la justicia el día de su citación, una orden de arresto es emitida a su nombre.

¿Cómo puedo saber si alguien me robó la identidad?

- Lea sus facturas. ¿Ve algún cargo por cosas que usted no compró?
- Revise el resumen de su cuenta bancaria. ¿Hay algún retiro que usted no hizo? ¿Hay algún cambio inesperado?
- Esté atento a su correspondencia. ¿Dejó de llegarle una factura? ¿O empezó a recibir una factura nueva de la que no sabía nada?
- Obtenga su informe de crédito. ¿Hay alguna cuenta u otra información que no reconoce?

¿Qué hago si mi identidad ha sido robada?

Si sospechas que alguien ha robado tu identidad, hay varias cosas que debe hacer:

•Denuncia el robo de identidad a la policía, la fiscalía o a los organismos competentes. En el caso de entidades bancarias, puedes comunicarte con las defensorías del consumidor financiero y la superintendencia financiera.

•Si abrieron un producto a tu nombre, ponte en contacto con la compañía donde ocurrió el fraude e infórmales que se ha abierto una cuenta falsa que tú no solicitaste.

•Pon una alerta en tu reporte de crédito: contacta a burós de crédito para informar la situación. La alerta de fraude hará que las entidades sean más precavidas si alguien intenta abrir un crédito o solicitar un producto a tu nombre.

•Comunícate con el banco. Informa de la situación a los departamentos de fraude de las entidades crediticias o con las que tengas productos vigentes.

1.4. Protección de datos.

La Ley de Protección de Datos Personales reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada. En cumplimiento con lo dispuesto en la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la Protección de Datos Personales y por el decreto 1377 de 2013 que reglamenta dicha ley.

¿Qué son Datos Personales?

Cuando hablamos de datos personales nos referimos a toda aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos.

¿Cómo se recogen los datos personales?

Los datos personales conforman la información necesaria para que una persona pueda interactuar con otras o con una o más empresas y/o entidades para que sea plenamente individualizada del resto de la sociedad, haciendo posible la generación de flujos de información que contribuyen con el crecimiento económico y el mejoramiento de bienes y servicios. Así, por ejemplo, cuando hacemos una solicitud de crédito ante una entidad financiera, se requiere diligenciar formularios con nuestra información personal, o cuando realizamos una compra y para realizar la factura de venta solicitan datos como el número de documento de identidad, correo electrónico, dirección y teléfono de contacto, entre otros.

¿Qué tipos de datos hay?

Las disposiciones sobre protección de datos, establecen tipologías de datos según el mayor o menor grado de aceptabilidad de la divulgación:

- Dato Público: es el dato que la ley o la Constitución Política determina como tal, así como todos aquellos que no sean semiprivados o privados.
- Dato Semiprivado: es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas.

- Dato Semiprivado: es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas.
- Dato Privado: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información.
- Dato Sensible: es el dato que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación.

¿A qué datos personales no se aplica la ley?

- A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.
- Las que tengan por finalidad la seguridad y defensa nacional la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.
- Las que tengan como fin y contengan información de inteligencia y contrainteligencia.
- Las que contengan información periodística y otros contenidos editoriales
- Las bases de datos con información financiera, crediticia, comercial y de servicios, y de los censos de población y vivienda.

Tratamiento de datos personales a través de las Cookies

Las cookies son archivos que recogen información a través de una página web sobre los hábitos de navegación de un usuario o de su equipo y eventualmente podrían conformar una base de datos de acuerdo a la definición legal de la Ley 1581 de 2012 al recolectar datos personales conforme a las siguientes características: (i) están referidos a aspectos exclusivos y propios de una persona natural, ii) permiten identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación; caso en el cual, el responsable deberá ceñirse por las normas sobre protección de datos vigentes en Colombia, en especial la aplicación de los principios rectores para la administración de datos de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad consagrados en el artículo 4 de la Ley 1581 de 2012.

1.5. Criptografía básica

La criptografía clásica viene desde la antigüedad hasta 1949. Su seguridad radica en el desconocimiento del algoritmo utilizado. El cifrado de textos es una actividad que ha sido ampliamente usada a lo largo de la historia humana, sobre todo en el campo militar y en aquellos otros en los que es necesario enviar mensajes con información confidencial y sensible a través de medios no seguros. Dos técnicas engloban las manifestaciones más relevantes de la criptografía clásica:

La sustitución consiste en cambiar los caracteres componentes del mensaje original en otros según una regla determinada de posición natural en el alfabeto.

La trasposición consiste en cambiar los caracteres componentes del mensaje original en otros según una regla determinada de posición en el orden del mensaje.

La palabra criptografía proviene del griego κριπτός (kryptós = recubierto, oculto), γραφειν (grafein = escribir), y el sufijo -ia (usada para crear sustantivos abstractos). El mensaje cifrado en sí está a la vista. Se puede leer, pero su significado está oculto. Así, podemos decir que mediante la criptografía una persona puede ocultar un texto o una información, para que solo el emisor y el receptor puedan interpretarlo. La criptografía es, en líneas generales, el arte y la técnica de crear mensajes codificados con procedimientos o claves secretas con el objeto de que no pueda ser descifrado salvo por la persona a quien está dirigido o que detenta la clave.

La Criptografía es una rama de las matemáticas que, al orientarse al mundo de los mensajes digitales, proporciona las herramientas idóneas para solucionar los problemas relacionados con la autenticidad y la confiabilidad. El problema de la confidencialidad se vincula comúnmente con técnicas denominadas de "encripción" y la autenticidad con técnicas denominadas de "firma digital", aunque la solución de ambos, en realidad, se reduce a la aplicación de procedimientos criptográficos de encripción y desencripción.

El objetivo de la criptografía es, pues, proteger la información enviada, de modo que solamente el destinatario o las personas que posean la clave, puedan leer el mensaje de manera correcta. Para ello, se diseñan sistemas de cifrado que solo son conocidos por las personas autorizadas.

Criptosistemas de clave pública y privada puede definirse formalmente un criptosistema como una quíntupla (M, C, K, E, D), donde:

- **M** representa el conjunto de todos los mensajes sin cifrar (lo que se denomina texto claro, o plaintext) que pueden ser enviados.
- **C** representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
- **K** representa el conjunto de claves que se pueden emplear en el criptosistema.
- **E** es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de M para obtener un elemento de C. Existe una transformación diferente Ek para cada valor posible de la clave k.
- **D** es el conjunto de transformaciones de descifrado, análogo a E.

Todo criptosistema ha de cumplir la siguiente condición, es decir, que, si tenemos un mensaje m, lo ciframos empleando la clave **K** y luego lo desciframos empleando la misma clave, obtenemos de nuevo el mensaje original **M**

Dk (Ek (m)) = m

Tipos de criptografía

Como mencionamos al inicio, la criptografía puede ser simétrica o asimétrica, según el tipo de clave que emplee. Veamos esto con más detalles.

Simétrica

También conocida como criptografía de clave privada. Este es el tipo de criptografía que se ha empleado desde los inicios de la historia y por muchísimo tiempo. También es llamada criptografía de clave privada o criptografía de una clave. Para llevarla a cabo y poder cifrar y descifrar un mensaje, se emplea una única clave que tanto el emisor como el receptor deben conocer previamente. Este es el punto débil de este método, ya que hay más probabilidad de que un tercero intercepte la clave cuando el emisor se la transmita al receptor, ver imagen 2.

En la criptografía simétrica se debe emplear una clave muy difícil de adivinar, debido a que los ordenadores actuales pueden adivinar claves muy rápidamente. Por ello, debemos considerar que como los algoritmos criptográficos son públicos, se debe garantizar que su fortaleza depende de su complejidad interna y de la longitud de la clave empleada, para evitar los ataques de fuerza bruta.

Método en el cual se emplea la misma clave para encriptar y descifrar mensajes, por lo cual ambas partes, tanto el emisor como el receptor, han de tener la misma clave. Por ejemplo: la autenticación de un celular de tecnología GSM.

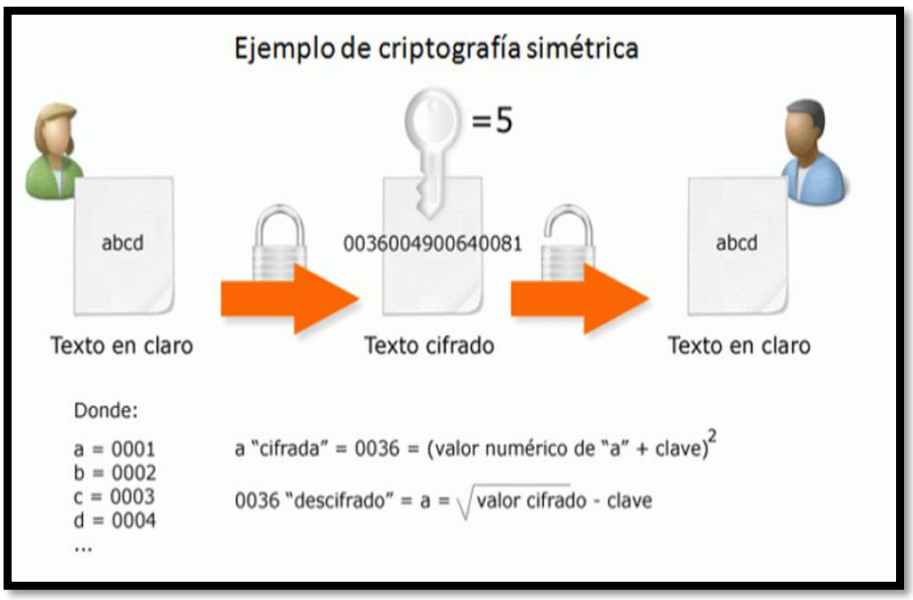

Imagen 2. Criptografía simétrica
Fuente: https://securityhacklabs.net/articulo/criptografia-simetrica-asimetrica-e-hibrida

Son aquellos que emplean una misma clave k tanto para cifrar como para descifrar. Presentan el inconveniente de que para ser empleados en comunicaciones la clave k debe estar en posesión tanto en el emisor como en el receptor, lo cual nos lleva preguntarnos cómo transmitirles a los participantes en la comunicación esa clave de forma segura.

Asimétrica

También conocida como criptografía de clave pública. Este método hace uso de dos claves, una pública y una privada; por lo que no es necesario conocer una clave previamente. La clave pública puede ser enviada y dada a conocer a cualquier persona, mientras que la clave privada es la que no se debe compartir con nadie. Cuando un emisor desea enviar un mensaje, éste usa la clave pública para cifrar el mensaje y lo envía. Y solo el receptor con su clave privada puede descifrar el mensaje, ver imagen 3.

La criptografía asimétrica brinda un nivel de seguridad extraordinario, al punto de que ni siquiera la persona que cifró el mensaje, puede descifrarlo sin la clave privada. Este es el método utilizado en las criptomonedas, y es una pieza fundamental en la blockchain para poder realizar operaciones e intercambios de información entre iguales con total seguridad y sin necesidad de confiar entre sí.

Es un método en el cual son empleadas dos claves, una pública y otra privada. A la clave pública cualquier persona puede acceder, mientras que a la privada solo tiene acceso su propietario.

Imagen 3: Criptografía asimétrica
Fuente: https://securityhacklabs.net/articulo/criptografia-simetrica-asimetrica-e-hibrida

Emplean una doble clave (kp, kP). kp se la conoce como clave privada y kP se la conoce como clave pública. Una de ellas sirve para la transformación o función E de cifrado y la otra para la transformación D de descifrado. En muchos casos son intercambiables, esto es, si empleamos una para cifrar la otra sirve para descifrar y viceversa. Estos criptosistemas deben cumplir además que el conocimiento de la clave pública kP no permita calcular la clave privada kp. Ofrecen un abanico superior de posibilidades, pudiendo emplearse para establecer comunicaciones seguras por canales inseguros puesto que únicamente viaja por el canal la clave pública, que sólo sirve para cifrar, o para llevar a cabo autenticaciones. Sin la clave privada (que no es deducible a partir de la clave pública) un observador no autorizado del canal de comunicación será incapaz de descifrar el mensaje cifrado.

Híbrida

Es un método que usa tanto un cifrado simétrico como un asimétrico. Empleando el cifrado de clave pública para compartir una clave para el cifrado simétrico.

Conociendo los conceptos básicos de la criptografía simétrica y la criptografía asimétrica, podemos darnos cuenta de cuál es su mayor diferencia. La seguridad que aporta la primera es de un nivel muy bajo comparado con la seguridad que aporta la segunda. Pero, la rapidez con que la criptografía simétrica cifra y descifra un mensaje es superior a la de la criptografía asimétrica. Por lo que de allí surge la criptografía híbrida.

El cifrado César y otros cifrados de sustitución monoalfabeto

El sistema César o desplazamientos César es una de las técnicas de criptografía más simples y mayormente difundidas. Fue el primero que se utilizó del cual se tienen registros y ese es quizás su principal valor, o sea, el valor histórico de haber sido el primero. No obstante, por su sencillez y facilidad de aplicación, tiene mucha aplicabilidad.

En un sistema César la encriptación se hace por sustitución, cada carácter del mensaje original será reemplazado por un carácter en el mensaje cifrado, el carácter cifrado se obtiene avanzando 'k' pasos en el alfabeto a partir del carácter original. Obviamente 'k' es la clave. Con nuestro alfabeto el sistema quedaría así:

Alfabeto en claro:

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

Alfabeto cifrado:

D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A B C

Tabla 2. Cifrado por desplazamiento

Por ejemplo, si se quiere enviar el mensaje ATACARALAMANECER, lo que se escribirá realmente es DWDFDUDÑDODPHFHU

El receptor del mensaje conocía la clave secreta de éste (es decir, que estaba escrito con un alfabeto desplazado tres posiciones a la derecha), y podía descifrarlo fácilmente haciendo el desplazamiento inverso con cada letra del mensaje. Pero para el resto de la gente que pudiese accidentalmente llegar a ver el mensaje, el texto carecía de ningún sentido.

Aparentemente es un cifrado muy débil y poco seguro, pero en la época de Julio César no era de conocimiento general la idea de ocultar el significado de un texto mediante cifrado. De hecho, que un mensaje estuviese por escrito ya era un modo de asegurar la confidencialidad frente a la mayoría de la población analfabeta de la época.

Como dato curioso, más de 1500 años después, un cifrado similar al de César fue utilizado por la reina María Estuardo de Escocia, para conspirar junto con los españoles contra su prima Isabel I (en realidad, fue incitada a conspirar por agentes al servicio de Isabel I; una trampa bien urdida.) Los mensajes cifrados de María fueron fácilmente descifrados mediante sencillos análisis estadísticos por los agentes de Isabel I, y así pues quedó al descubierto la conspiración de la reina escocesa. Junto con la pérdida del secreto de la comunicación, María perdió la cabeza en su ejecución el 8 de febrero de 1587. Después de esto el cifrado César quedó definitivamente descartado como método de cifrado seguro para los gobernantes del mundo. Desde entonces a hoy, los cifrados usados por los estados para preservar sus secretos han mejorado considerablemente.

Lo que a nosotros nos interesa del cifrado César es que es un claro ejemplo de utilización de la aritmética modular para garantizar la confidencialidad de la información mediante el cifrado o encriptación. Matemáticamente, podemos describir el método usado por Julio César como una función lineal del tipo

$E(x)=x+3 \pmod{27}$

Para un alfabeto con 27 caracteres como el español. La x indica la posición que la letra "en claro" ocupa en alfabeto. E(x) indica la posición de la letra cifrada correspondiente a x en el alfabeto. Según esto, E(0) =3, y E(26) =2 (esto es, la a se cifra como d, y la z como c)

Para descifrar se emplea la función $D(x)=x-3 \pmod{27}$ Para cifrar y descifrar el mensaje los comunicantes han de conocer y usar una misma clave secreta, que en este caso es el desplazamiento aplicado sobre el alfabeto (desplazamiento=3). Por eso el cifrado César pertenece a los cifrados de clave privada, también llamados cifrados simétricos.