

**Conceptos Clave**

1

**Cultura y Apropiación**

**Ministerio de Tecnologías de la Información y las Comunicaciones**



### Acceso a las TIC

Condiciones y medios de acercamiento a las TIC por parte de los Grupo de Interés (Infraestructura, servicios, aplicaciones, políticas, programas...).

### Activismo Digital

Ejercicio de la ciudadanía y del compromiso social mediante la participación activa en redes sociales de personas naturales o jurídicas creando dinámicas de información, sensibilización, educación y movilización social usando la web.

### Activo

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

### Alfabetización Digital

Proceso de formación de competencias básicas para el uso de las TIC y, particularmente relacionada con el manejo de un computador, el software de oficina y de la navegación en Internet.

### Amenaza

Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

### Amenaza Externa

Amenaza que se origina fuera de una organización.

### Amenaza Interna

Amenaza que se origina en una organización.

### Análisis de Riesgo

Uso sistemático de la información para identificar las fuentes y estimar el riesgo NTC-ISO /IEC 27001.

### Analizador

Herramienta de configuración automatizada que analiza una red en busca de sistemas activos y actúa como guía durante el proceso de definición de los sistemas que desea supervisar y de las firmas de ataques que desea asociar con cada sistema.

### Antivirus

Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

### Aplicaciones engañosas

Las aplicaciones engañosas son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los usuarios divulguen información personal confidencial. Un ejemplo es el software de seguridad fraudulento, que también se denomina scareware.

### Aprovechamiento de las TIC

Emplear útilmente las TIC, hacerlas provechosas o sacarles el máximo rendimiento.

### Arquitectura abierta de red

Es el conjunto de características técnicas de las redes de telecomunicaciones que les permite interconectarse entre sí a nivel físico y lógico, de tal manera que exista interoperabilidad entre ellas. (Decreto 2870 de 2007, Artículo 2º).

### Ataques Web

Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

### Automatizar

Hace referencia a la incorporación de herramientas tecnológicas a un proceso o sistema.

### Back Office

En términos empresariales, hace referencia a la parte donde tienen lugar las tareas destinadas a la gestión de la propia empresa y con las cuales el cliente no tiene un contacto directo. En el ámbito tecnológico, se refiere a los sistemas automáticos que respaldan las acciones que acompañan a una transacción.

### Blacklisting o Lista Negra

La lista negra es el proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos.

### B-Learning

Educación flexibilizada mediante metodologías semi-presenciales y apoyadas en canales electrónicos (las nuevas redes de comunicación, en especial Internet), utilizando además de los espacios presenciales, herramientas o aplicaciones de hipertexto (correo electrónico, páginas web, foros de discusión, mensajería instantánea, plataformas de formación -que aúnan varios de los anteriores ejemplos de aplicaciones-, etc.) como soporte de los procesos de enseñanza-aprendizaje.

### Botnet

Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Estos equipos normalmente se distribuyen a través de Internet y se utilizan para actividades malintencionadas, como el envío de spam y ataques distribuidos de negación de servicio. Las botnet se crean al infectar las computadoras con malware, lo cual da al atacante acceso a las máquinas. Los propietarios de computadoras infectadas generalmente ignoran que su máquina forma parte de una botnet, a menos que tengan software de seguridad que les informe acerca de la infección.

### Brecha Digital

Hace referencia a la diferencia socioeconómica entre aquellas comunidades que tienen accesibilidad a las TIC y aquellas que no, y también hace referencia a las diferencias que hay entre grupos según su capacidad para utilizar las TIC de forma eficaz, debido a los distintos niveles de alfabetización y capacidad tecnológica.

### Brigada Digital

Estrategia de apropiación TIC, de uso responsable y solidario de las destrezas digitales de los usuarios de redes sociales, que propicia espacios de colaborativos y la intervención en temas de interés para el desarrollo de las personas, las comunidades y el país.

### Bucle de abonado

Son todos los elementos de red (físicos y/o lógicos) que permiten el establecimiento del enlace entre el terminal del abonado y la red del servicio. Va desde el Punto de Terminal de Red (punto de conexión en los predios de abonado) hasta el nodo de la red en donde se encuentra conectado el usuario.

### Caballo de Troya

Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de Troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos. Por lo general, también tienen un componente de puerta trasera, que le permite al atacante descargar amenazas adicionales en un equipo infectado. Normalmente se propagan a través de descargas inadvertidas, archivos adjuntos de correo electrónico o al descargar o ejecutar voluntariamente un archivo de Internet, generalmente después de que un atacante ha utilizado ingeniería social para convencer al usuario de que lo haga.

### Cadena de Trámites

La relación que se establece entre los trámites en función de los requisitos exigidos para su realización, los cuales se cumplen a través de otros trámites o servicios prestados por otras entidades, genera las cadenas de trámites.

### Certificado

Los sistemas criptográficos utilizan este archivo como prueba de identidad. Contiene el nombre del usuario y la clave pública.

### Chief Technology Officer (CTO)

Dentro de una organización, es el encargado de realizar procesos de transformación de procesos y recursos en tecnología con el fin de apoyar el cumplimiento de los objetivos de la misma. Usualmente combina un fuerte conocimiento técnico y científico con habilidades gerenciales e involucra la realización de actividades de investigación y desarrollo tecnológico y la formulación de estrategias de largo plazo.

### Ciberacoso (cyberbullying)

Es un tipo de agresión psicológica que se da usando las nuevas tecnologías: teléfonos celulares e Internet. Por medio de correos, mensajes o imágenes que se envían se busca herir o intimidar a otra persona. Este tipo de acoso no se hace de frente, por ello la víctima desconoce la identidad de su agresor.

### Cibercrímen (delito cibernético)

Conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio.

### Ciberseguridad

Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

### Ciberterrorismo

Es el uso del Ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o estado trayendo como consecuencia una violación a la voluntad de las personas.

### Ciudadanía Digital

Programa que ejecuta el Ministerio de las TIC que busca certificar en competencias TIC a servidores (as) y docentes públicos de todo el país, para promover e incrementar los niveles de incorporación, adaptación e integración de las tecnologías de la información y las comunicaciones en los servicios del Gobierno y sector educativo.

### Ciudadano / Ciudadana Digital

Persona que ha adquirido destrezas y competencias para el manejo y aprovechamiento de las TIC, que aplica dichas competencias en su vida cotidiana y que puede llegar a certificarse como tal mediante el programa de Ciudadanía Digital del MINTIC.

### Competencias TIC

Habilidades o destrezas que se adquieren a través de formación o capacitación frente el uso y apropiación de tecnologías de la información y las comunicaciones.

### Comunidades organizadas (D.1981-03)

Se entiende por comunidad organizada a la asociación de derecho, sin ánimo de lucro, integrada por personas naturales y/o jurídicas, en la que sus integrantes estén unidos por lazos de vecindad y colaboración mutuos en beneficio del desarrollo local y la participación comunitaria.

### Confidencialidad

Propiedad de la información que determina que esté disponible a personas autorizadas.

### Conjunto de Datos

Es un conjunto de variables y datos asociados.

### Crimeware

Software que realiza acciones ilegales no previstas por un usuario que ejecuta el software. Estas acciones buscan producir beneficios económicos al distribuidor del software.

Cuarentena Aislar archivos sospechosos de contener algún virus, de modo que no se pueden abrir ni ejecutar.

### Cultura

Aunque el término designa todo lo que produce significados en una sociedad, se refiere al conjunto de instituciones, prácticas y objetos que constituyen el universo simbólico de una sociedad, en relación con los cuales se socializan los sujetos y grupos, y que rigen las creencias y el comportamiento de estos.

### Datos Abiertos

Son todos aquellos datos primarios (sin procesar) que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos. Las principales características de los datos abiertos son:

* Completos: Los datos públicos no deben estar sujetos a privacidad u otras limitaciones. Además, deben estar electrónicamente almacenados.
* Primarios: Significa que debe haber una disponibilidad de la fuente primaria, sin procesamientos y sin formas agregadas.
* Oportunos: Ello para preservar su valor.
* Accesibles: La disponibilidad debe ser lo más amplia posible para los usuarios y para propósitos diversos.
* Procesables: Deben estar razonablemente estructurados para permitir su automatización por diversas herramientas.
* Acceso indiscriminado: Implica su disponibilidad para cualquier usuario, sin necesidad de su registro.
* No-propietarios: Deben estar disponibles en un formato donde nadie deba tener la exclusividad de su control.
* Libres de licencias: No deben estar sujetos a copyright, patentes, o regulaciones secretas. Una razonable privacidad, seguridad y restricciones puede ser aplicada por el gobierno u otros estamentos. Datos Abiertos corresponde a una filosofía y práctica que persigue que determinados datos de los Gobiernos estén disponibles de forma libre a todo el mundo, sin restricciones de copyright, patentes u otros mecanismos de control, permitiendo el impulso del crecimiento económico, salvaguardar los derechos de ciudadanos y empresas, así como, delimitar las obligaciones de las administraciones.

### Derecho a la Información

Derecho constitucionalmente reconocido que tiene toda persona de buscar, recibir y difundir información. Las Naciones Unidas, en una de sus primeras asambleas generales afirmó que: "la libertad de información es un derecho fundamental y... la piedra angular de todas las libertades a las que están consagradas las Naciones Unidas". En otras palabras, es un derecho instrumental que puede ser utilizado para garantizar el cumplimiento de otros derechos esenciales del ser humano.

### E-Learning (aprendizaje electrónico)

Educación a distancia completamente virtualizada a través de los nuevos canales electrónicos (las nuevas redes de comunicación, en especial Internet), utilizando para ello herramientas o aplicaciones de hipertexto (correo electrónico, páginas web, foros de discusión, mensajería instantánea, plataformas de formación -que aúnan varios de los anteriores ejemplos de aplicaciones-, etc.) como soporte de los procesos de enseñanza-aprendizaje.

### Enfoque Diferencial

Tipo de abordaje político para el diseño de planes, estrategias, programas y proyectos tomando en cuenta la diversidad social y poblacional y particularmente reconociendo la necesidad de establecer mecanismos de priorización y focalización en atención a esas diferencias para la promoción de la equiparación de oportunidades.

### Entorno digital

Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web.

### Entorno digital abierto

Entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica.

### Evaluación del riesgo

Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. NTC-ISO /IEC 27001.

### Exelearning

Es un programa tipo open source (recursos libres o gratuitos); una creación de aplicación que permite a profesores y académicos la publicación de contenidos didácticos en soportes informáticos (CD, memorias USB, en la web), sin necesidad de ser ni convertirse en expertos en HTML o XML.

### Firewall

Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

### Firma digital o electrónica

Es el valor numérico que se adhiere a un mensaje de datos y que utiliza un procedimiento matemático conocido vinculado a la clave del iniciador y al texto del mensaje para determinar que este valor se haya obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no haya sido modificado después de efectuada la transformación. (Ley 527 de 1999).

### Front Office

Es el lugar donde el usuario entra en contacto con la entidad y se refiere al conjunto de estructuras que gestionan la interacción con dicho ciudadano o usuario.

### Hackear

Es el ingreso ilegal a computadores, páginas y redes sociales con el objetivo de robar información, suplantar la identidad del dueño, beneficiarse económicamente o protestar.

### Indicadores de gestión (R. 087-97)

Son medidas objetivas de resultados alrededor de diversos objetivos, utilizadas para asegurar su mejoramiento y evaluación y medir el desempeño. Información. (U.I.T. recomendación B 13)

### Instancias de participación ciudadana

Son escenarios de representación de la sociedad civil, de encuentro e interacción entre actores sociales o entre éstos y las autoridades públicas, a través de los cuales se canalizan iniciativas, se delibera en torno a los asuntos relacionados con temas específicos y se construyen y se hace seguimiento a acuerdos. Las instancias de participación ciudadana pueden ser formales e informales.

### Integridad

Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento deben ser exactos.

### Interoperabilidad

Habilidad de transferir y utilizar información de manera uniforme y eficiente entre varias organizaciones y sistemas de información. (Gobierno de Australia). Habilidad de dos o más sistemas (computadoras, medios de comunicación, redes, software y otros componentes de tecnología de la información) de interactuar y de intercambiar datos de acuerdo con un método definido, con el fin de obtener los resultados esperados. (ISO). El ejercicio de colaboración entre organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio, con el propósito de facilitar la entrega de servicios en línea a ciudadanos, empresas y a otras entidades. (Marco de Interoperabilidad para el Gobierno en línea, Versión 2010).

### Interoperabilidad de los servicios (R. 087-97)

Es el correcto funcionamiento de los servicios que se prestan sobre dos redes intercontectadas.

### IPv6

El Protocolo de Internet versión 6, es la versión del Protocolo de Internet (IP por sus siglas en inglés) que fue diseñada para suceder al Protocolo versión 4. Ipv6 ha sido desarrollado por la Internet Engineering Task Force (IETF -www.ietf.org), para hacer frente al agotamiento de las direcciones Ipv4, y se describe en el documento estándar de Internet RFC 2460, publicado en diciembre de 1998. Aunque Ipv4 de 32 bits permite una dirección de Protocolo de Internet, y por lo tanto puede soportar 232 direcciones, Ipv6 utiliza direcciones de 128 bits, por lo que el nuevo espacio de direcciones compatible con 2128. Esta expansión permite muchos más dispositivos y usuarios en Internet, así como una mayor flexibilidad en la asignación de direcciones y la eficiencia para el direccionamiento de tráfico.

### M-Learning

Educación a distancia virtualizada a través de dispositivos móviles, utilizando para ello herramientas o aplicaciones apropiadas para el desarrollo de procesos de enseñanza-aprendizaje.

### Neutralidad Tecnológica

Es la libertad que tienen los proveedores de redes y servicios de usar las tecnologías para la prestación de todos los servicios sin restricción distinta a las posibles interferencias perjudiciales y el uso eficiente de los recursos escasos.

### Ofimática

Herramientas de oficina usadas en las entidades como lo son hojas de cálculo, procesamiento de texto, entre otros.

### Open Data

Datos Abiertos corresponde a una filosofía y práctica que persigue que determinados datos de los Gobiernos estén disponibles de forma libre a todo el mundo, sin restricciones de copyright, patentes u otros mecanismos de control, permitiendo el impulso del crecimiento económico, salvaguardar los derechos de ciudadanos y empresas, así como, delimitar las obligaciones de las administraciones.

### PACO

Punto de Atención al Ciudadano y al Operador

### Participación Ciudadana

Es el derecho que tienen las personas y las organizaciones civiles, sin distingo alguno, a incidir, a través de diversas acciones, en la elaboración, ejecución y seguimiento de las decisiones relacionadas con el manejo de los asuntos públicos, cuando les asista interés o puedan resultar afectados por ellas. Es un derecho inherente a las personas y un deber consagrado en la Constitución. La participación ciudadana puede tener distintos alcances: la información, la consulta, la iniciativa, la deliberación, la decisión y el control de la gestión pública.

### Pharming

Método de ataque que tiene como objetivo redirigir el tráfico de un sitio Web a otro sitio falso, generalmente diseñado para imitar el sitio legítimo. El objetivo es que los usuarios permanezcan ignorantes del re-direccionamiento e ingresen información personal, como la información bancaria en línea, en el sitio fraudulento.

### Phishing

Método más utilizado por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

### Racionalizar

Organizar los trámites, procesos y procedimientos de tal manera que se reduzcan a su mínima expresión, con el menor esfuerzo y costo para el ciudadano, a través de estrategias efectivas de simplificación, estandarización, mejoramiento continuo, supresión y automatización de los mismos.

### Regla de Negocio

Es una condición, validación o norma que se debe cumplir y controlar dentro de la organización y que es definida de acuerdo al comportamiento esperado del negocio y de la organización.

Riesgo El riesgo es el efecto de la incertidumbre sobre los objetivos.

### Rootkits

Componente de malware que utiliza la clandestinidad para mantener una presencia persistente e indetectable en un equipo. Las acciones realizadas por un rootkit, como la instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o consentimiento del usuario final.

### Servicio en Línea

Servicio que puede ser prestado por medios electrónicos a través del portal de una entidad.

Simplificar Adoptar estrategias que implican: reducción de costos operativos en la entidad, reducción de costos para el usuario, reducción de documentos, reducción de pasos, reducción de pasos en el trámite interno, reducción de requisitos, reducción del tiempo de duración del trámite, reducción del tiempo en los puntos de atención, aumento en la vigencia del trámite, aumento de puntos de atención, fusión del trámite.

### Sistema de detección de intrusos

Un sistema de detección de intrusos es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red. Un sistema de detección de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

### Sistema de Gestión Documental (SGD)

Se refiere a un repositorio de documentos de una entidad, este repositorio cuenta con índices e información que permite el uso, localización y almacenamiento de los documentos.

### Sistema de prevención de intrusos

Un sistema de prevención de intrusos es un dispositivo (hardware o software) que supervisa las actividades de la red o del sistema en busca de comportamiento no deseado o malicioso y puede reaccionar en tiempo real para bloquear o evitar esas actividades. Un sistema de prevención de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

### Sistema Único de Información de Trámites - SUIT

Es un sistema electrónico de administración de información de trámites y servicios de la administración pública Colombiana que opera a través del Portal del Estado Colombiano y cuyo funcionamiento es coordinado por el Departamento Administrativo de la Función Pública, por mandato legal. Este sistema permite integrar la información y actualización de los trámites y servicios de las entidades de la administración pública para facilitar a los ciudadanos la consulta de manera centralizada y en línea.

### Smishing

Es una variante del phising, pero a diferencia de este, usa mensajes de texto para engañar a los usuarios, pidiéndoles información privada e invitándolos a que se dirijan a sitios web falsos que tienen spywares y softwares maliciosos que se descargan automáticamente, sin que el usuario lo note.

### Sociedad de la Información

La sociedad de la información es aquella en la cual las tecnologías que facilitan la creación, distribución y manipulación de la información juegan un papel importante en las actividades sociales, culturales y económicas debe estar centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida.

### Spam

También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing.

### Spyware o Software Espía

El software espía consta de un paquete de software que realiza un seguimiento y envía información confidencial o personal a terceros. La información personal es información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial incluye datos que la mayoría de las personas no desearía compartir con otras, como detalles bancarios, números de tarjetas de créditos y contraseñas. Terceros puede hacer referencia a sistemas remotos o partes con acceso local.

### Tecnologías de la Información (TI)

Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia de negocio.

### Tecnologías de la Información y las Comunicaciones (TIC)

Las Tecnologías de la Información y las Comunicaciones (TIC), son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes (Art. 6 Ley 1341 de 2009).

### Telecomunicación (L. 72-89)

Se entiende por telecomunicaciones toda transmisión, emisión o recepción de signos, señales, escritos y sonidos, datos o información de cualquier naturaleza, por hilo, radio, medios visuales u otros sistemas electromagnéticos.

### TIC para el Desarrollo

Aplicación de las Tecnologías de la Información y las Comunicaciones -TIC en apoyo a medidas nacionales para la superación de la pobreza, el aumento de la competitividad y la superación de problemáticas en diferentes poblaciones, sectores y territorios (en inglés ICT4D).

### Trámite

Conjunto o serie de pasos o acciones reguladas por el Estado, que deben efectuar los usuarios para adquirir un derecho o cumplir con una obligación prevista o autorizada por la ley. El trámite se inicia cuando ese particular activa el aparato público a través de una petición o solicitud expresa y termina (como trámite) cuando la administración pública se pronuncia sobre éste, aceptando o denegando la solicitud.

### Trámite en Línea

Trámite que puede ser realizado por medios electrónicos a través del portal de una entidad, ya sea de manera parcial, en alguno de sus pasos o etapas, o total, hasta obtener completamente el resultado requerido.

### Trazabilidad

La trazabilidad es la capacidad para rastrear un elemento del proyecto hasta otros elementos del proyecto relacionados, especialmente los que están relacionados con requerimientos. Los elementos del proyecto implicados en la trazabilidad se llaman elementos de trazabilidad. Entre los elementos de trazabilidad típico se incluyen diferentes tipos de requerimientos, elementos de modelos de análisis y diseño, artefactos de prueba y material de formación y documentación de soporte al usuario final.

### Usabilidad

La usabilidad es un atributo relacionado con la facilidad de uso. Más específicamente, se refiere a la rapidez con que se puede aprender a utilizar algo, la eficiencia al utilizarlo, cuán memorable es, cuál es su grado de propensión al error, y cuánto le gusta a los usuarios. Si una característica no se puede utilizar o no se utiliza es como si no existiera. (Nielsen)

### Uso de las TIC

Capacidad y/o competencia del Grupo de Interés para utilizar efectivamente las TIC.

### Ventanilla Única Virtual

Sitio virtual desde el cual se gestiona de manera integrada la realización de trámites que están en cabeza de una o varias entidades, proveyendo la solución completa al interesado.

### Virus

Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios: Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa. Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red. Muchos de los virus actuales están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos. Otros menoscaban el equipo dañando los programas, eliminando archivos o volviendo a formatear el disco duro. Aún existen otros que no están diseñados para causar daño, aunque simplemente se reproducen y hacen manifiestan su presencia presentando mensajes de texto, video y audio, aunque este tipo de ataques de notoriedad no son tan comunes, puesto que los autores de virus y demás malware tiene como fin obtener ganancias ilegales.

### Vulnerabilidad

Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:

* Permitir que un atacante ejecute comandos como otro usuario
* Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos
* Permitir a un atacante hacerse pasar por otra entidad - Permitir a un atacante realizar una negación de servicio

### XML

Extensible Markup Language (Lenguaje extendido de tags). Se refiere a un lenguaje estructurado basado en tags que permiten la definición y entendimiento de una máquina del contenido del documento.