

**Conceptos Clave**

1

**Seguridad y Privacidad de la Información**

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



### Accesibilidad

Acceso universal a la Web, independientemente del tipo de hardware, software, infraestructura de red, idioma, cultura, localización geográfica y capacidades de los usuarios (W3C World Wide Web Consortium). En el contexto colombiano, ha venido asumiéndose como las condiciones que se incorporan en sitios y herramientas web que favorecen el que usuarios en condiciones de deficiencia tecnológica, física o sensorial o en condiciones particulares de entornos difíciles o no apropiados, puedan hacer uso de estos recursos de la Web.

### Acceso a las TIC

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

### Acceso a la Información Pública

 Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

### Activo

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

### Activos de Información y recursos

Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).

### Advertencia

Mensaje que comunica al usuario que una acción puede ocasionar u ocasionara la pérdida de datos del sistema del usuario.

### Alerta

Notificación automática de un suceso o un error.

### 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.

### Antispam

Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.

### 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.

### Archivo

 Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

### Amenazas

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

### Análisis de Riesgo

Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).

### 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.

### Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

### Autorización

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

### Automatizar

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

### Bases de Datos Personales

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

### 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.

### 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.

### 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.

### Certificado

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

### CERT (Computer Emergency Response Team)

Equipo de Respuesta a Emergencias cibernéticas. Se refiere a una institución definida y concreta con capacidad centralizada para la coordinación de gestión de incidentes. (Universidad Carnegie Mellon).

### Ciberseguridad

Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

### Ciberdelito / Delito cibernético

Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia).

### Ciberespacio

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

### 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.

### Ciberlavado

Es el uso del Ciberespacio, en cualquiera de sus formas, para dar apariencia de legalidad a bienes obtenidos ilícitamente o para ocultar dicha ilicitud ante las autoridades.

### 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.

### Confidencialidad

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

### Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

### 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.

### CSIRT

Equipo de Respuesta a Incidentes de Seguridad cibernética, por su sigla en inglés. Se refiere a una institución definida y concreta que tiene la responsabilidad de proveer capacidades de gestión de incidentes a una organización/sector en especial. Su objetivo es minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta y recuperación efectiva, así como trabajar en pro de prevenir la ocurrencia de futuros incidentes.

### Cyberstalking

Es el acoso, espionaje o persecución que se da a una persona o grupo usando Internet u otro dispositivo electrónico. Este acoso puede darse con investigación constante de información sobre la persona, acusaciones falsas, espionaje, amenazas, robo de identidad, y daño a la información o el equipo que la almacena.

### 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.

### 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.

### Datos Abiertos

 Son todos aquellos datos primarios o 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 o privadas que cumplen con funciones 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 (Ley 1712 de 2014, art 6)

### Datos Personales

 Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

### Datos Personales Públicos

 Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

### Datos Personales Privados

 Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

### Datos Personales Mixtos

Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

### Datos Personales Sensibles

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

### Derecho a la Intimidad

Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

### Descubridor

Se trata de aquella parte interesada que tiene conocimiento de la existencia una vulnerabilidad propia o de uno o varios terceros.

### Divulgación responsable

Es cuando un descubridor revela una vulnerabilidad a la(s) parte(s) interesada(s) que la posee o a las autoridades competentes, con la intención que se proceda a su corrección o a la toma de medidas al respecto. Esta divulgación no se entiende de carácter público, hasta que la(s) parte(s) interesada(s) que posee(n) la vulnerabilidad o las autoridades competentes lo consideren conveniente, sea para generar alarmas oportunas, para efectos estadísticos o para la documentación del caso.

### Encargado del Tratamiento de Datos

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

### Entorno digital

Ambiente, tanto físico como virtual sobre el cual se soportan las interacciones del futuro digital, tales como la economía digital.

### 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).

### Gestión de incidentes de seguridad de la información

 Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

### 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.

### Incidente

Cualquier evento adverso real o sospechado, intencionado o no intencionado, que puede cambiar el curso esperado de una actividad en el entorno digital.

### 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).

### Infraestructura crítica

 es el conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar en la seguridad de la economía, salud pública, o la combinación de ellas, en una nación. (Resolución CRC 2258 de 2009).

### Infraestructura crítica cibernética nacional

Se entiende por aquella infraestructura soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.

### Información Pública Clasificada

 Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

### Información Pública Reservada

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

### Ingeniería Social

Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social.

### 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.

### Keystroke Logger o Programa de captura de teclado (Keylogger)

Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.

### Ley de Habeas Data

Se refiere a la Ley Estatutaria 1266 de 2008.

### Ley de Transparencia y Acceso a la Información Pública

Se refiere a la Ley Estatutaria 1712 de 2014.

### Mecanismos de protección de datos personales

Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

### Malware

El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer acciones delictivas.

### 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.

### Partes interesadas (Stakeholder)

 Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

### Plan de continuidad del negocio

 Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

### Plan de tratamiento de riesgos

Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

### 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.

### Registro Nacional de Bases de Datos

Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

### Responsabilidad Demostrada

Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

### Responsable del Tratamiento de Datos

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

### Riesgo

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

### Riesgo

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

### 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.

### Seguridad de la información

Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio

### Seguridad digital

Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

### 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.

### 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.

### Titulares de la información

Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

### Tratamiento de Datos Personales

Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

### 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.

### 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.

### Trazabilidad

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).

### Uso de las TIC

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

### 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

### Vulnerabilidad

Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).