



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

Establecer las políticas de seguridad y privacidad de la información de la Unidad con el fin de regular la gestión de la seguridad de la información al interior de la misma.

Este documento relaciona los lineamientos y aspectos de la capa transversal de seguridad relacionados en la Arquitectura Tecnológica de Referencia y las mejores prácticas que permiten a la Unidad prestar de manera segura los servicios relacionados en el Catálogo de servicios de TI.

Es muy importante para la Unidad contar con estas políticas de seguridad documentadas ya que son ellas quienes guiarán el comportamiento personal y profesional sobre la información capturada, integrada y dispuesta por la Unidad, así mismo permitirán a la Unidad trabajar bajo las mejores prácticas de seguridad y facilitarán el cumplimiento de los requisitos legales a los cuales esté obligada en torno a esta materia.

Estas políticas en términos generales abarcan los temas de:

2.1 POLÍTICA DE CONTROL DE ACCESO

El acceso de los funcionarios, contratistas, personal que labore en las instalaciones vinculado con un proveedor de la UAECD o personal externo (empresa o entidad externa) a la información y a los recursos tecnológicos de la UAECD debe ser debidamente solicitado y autorizado por el responsable de dicho recurso, basado en la premisa “Todo está restringido, a menos que esté expresamente permitido”.

2.2 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

Establecer los lineamientos básicos bajo los cuales se debe mantener protegida la información ubicada en los puestos de trabajo/oficinas y desplegada en las pantallas de las terminales/equipos de cómputo de la Unidad, independiente del medio en que se encuentre depositada o almacenada.

2.3 POLÍTICA PARA EL TRATAMIENTO DE DATOS PERSONALES

Esta política permite dar cumplimiento a la Ley 1581 de 2012 "por la cual se dictan disposiciones generales para la protección de datos personales", reglamentada parcialmente a través del Decreto N° 1377 de 2013 “por el cual se reglamenta parcialmente la Ley 1581 de 2012”, con el propósito de que todas las personas puedan conocer, actualizar



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

y rectificar los datos que se hayan recogido sobre ellas en las bases de datos o archivos que sean susceptibles de tratamiento por parte de la UAECD.

2.4 POLÍTICA DE INSTALACIÓN Y USO DE SOFTWARE

En las últimas décadas el software se ha situado en el núcleo de la revolución tecnológica, impulsando la innovación a un ritmo acelerado, facilitando la difusión del conocimiento y la comunicación global.

Por lo anterior, es imprescindible una protección jurídica clara, eficaz y completa en defensa de los derechos de propiedad intelectual de los desarrolladores de software y la atención adecuada a las brechas de seguridad que se puedan presentar por instalaciones de software libre no controladas que puedan introducir software infectado o vulnerable exponiendo la información de la Unidad.

La presente política permitirá a la UAECD disponer de lineamientos para controlar las instalaciones/actualizaciones/desinstalaciones de software en la Unidad, tanto para el software libre como para el software licenciado o privativo.

2.5 POLÍTICA DE USO ACEPTABLE

Los funcionarios, contratistas, personal que labora en las instalaciones vinculado con un proveedor de la UAECD o personal externo (empresa o entidad externa) a la Unidad deben conocer los requisitos de seguridad tanto de la información de la Unidad como de los activos asociados con los servicios de procesamiento de dicha información.

2.6 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

En muchas oportunidades la información que gestiona la Unidad es transferida entre dependencias, a proveedores o terceras partes, a otras entidades públicas o a organizaciones o individuos, ya que es información valiosa para su gestión y adicionalmente es de su competencia el conocerla para el ejercicio de sus funciones. Estas transferencias de información son realizadas utilizando varios mecanismos de envío (por correo electrónico, transferencia electrónica de datos, a través de medios removibles, por correspondencia física o en la mano, por teléfono o dispositivo móvil, transmisión por sitios o páginas colaborativas o internet, transmisión por mensajes de texto SMS¹ o mensajería instantánea), ya sea que se trate de información en medio electrónico o en medio físico (papel), hay un riesgo de que la información se pierda, sea alterada, sea entregada de



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

manera no apropiada o accidentalmente sea entregada a personas no autorizadas. Para mantener la confidencialidad de la información, la protección de los datos personales, el cumplimiento de la legislación y normatividad vigentes y la confianza de nuestros ciudadanos, es esencial que la transferencia sea realizada protegiendo adecuadamente la información. En esta política se presentan los requerimientos mínimos de seguridad para proteger la información durante su transferencia evitando así su interceptación, copiado, modificación, enrutado y destrucción.

2.7 POLÍTICA DE COPIAS DE RESPALDO Y RECUPERACION

La información digital y electrónica que reside en los diferentes recursos tecnológicos de almacenamiento de la Unidad Administrativa Especial de Catastro Distrital- UAECD no está exenta de eventos o situaciones (fallas técnicas, eventos naturales, daño físico, acciones no autorizadas, acciones malintencionadas, entre otros) que puedan afectar su operación normal, por lo que debemos prepararnos y reducir el impacto ante este tipo de eventos o situaciones a través de la generación y ejecución del plan de copias de respaldo de la información, teniendo en cuenta los siguientes aspectos: a. Identificar los registros exactos y completos de la información a respaldar de las diferentes bases de datos misionales y administrativas de la Unidad. b. Contar con un procedimiento de copias de respaldo de la información documentado. c. Contar con un procedimiento de recuperación de copias de respaldo documentado. d. Definir el tipo de copias de respaldo, por ejemplo: copias de respaldo completas, incrementales o diferenciales, dependiendo de la criticidad de la información a respaldar y/o de la frecuencia de su actualización. e. Determinar la frecuencia con que se realicen el respaldo de información de acuerdo con las necesidades de los responsables del proceso, por ejemplo: diaria, mensual, semestral, anual, entre otras. f. Determinar la retención de las copias de respaldo de acuerdo con los requisitos normativos plasmados en las tablas de retención documental de los procesos de la Unidad. g. Cumplir con los requisitos de seguridad de la información para la protección adecuada de los medios utilizados durante su almacenamiento y transferencia (transporte), de acuerdo con la criticidad de la información respaldada. En este documento se encontrarán los lineamientos que rigen el Plan de copias de respaldo y recuperación de la UAECD y los procedimientos de copias de respaldo y recuperación, los cuales deben estar alineados con los Subsistemas de Gestión de Seguridad de la información y de Continuidad del Negocio, que hacen parte del Sistema de Gestión Integral - SGI de la UAECD.

2.8 POLÍTICA PARA DISPOSITIVOS MÓVILES



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

Los dispositivos móviles facilitan el acceso y transferencia de la información de la Unidad, por tanto, se deben establecer lineamientos para mitigar los riesgos asociados al acceso, pérdida y divulgación no autorizados de la información de la Unidad. Dada la tendencia de llevar su propio dispositivo móvil² como apoyo al desarrollo de las actividades asignadas por la Unidad, permitiendo una flexibilidad en el trabajo al facilitar que los funcionarios, contratistas y personal que labora en las instalaciones vinculado con un proveedor de la UAEDC, puedan acceder a la información de la Unidad a través de estos dispositivos, se deben cumplir en todo momento los controles de seguridad de la información aplicables a ellos, tales como: asignación privilegios de acceso, borrado seguro de la información y aplicación de técnicas de cifrado.

2.9 POLÍTICA PARA LA RELACIÓN CON PROVEEDORES EN LA ETAPA PRECONTRACTUAL Y CONTRATISTAS.

Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores en la etapa precontractual y contratistas a los activos de información de la Unidad se deben acordar durante las etapas de planeación (que inicia con la identificación de la necesidad y finaliza con la elaboración de los estudios previos) y precontractual del proceso de contratación que recae en el establecimiento de la relación contractual con un proveedor a través de la inclusión de cláusulas en los estudios previos y técnicos que den cumplimiento a los requisitos de seguridad de la información conforme a la norma ISO27001:2013.

2.10 POLÍTICA PARA LA GESTIÓN DE LA SEGURIDAD DE LAS REDES.

La gestión de la seguridad de las redes le permite a la Unidad prestar de manera segura los servicios de red. Los beneficios que puede traer para la Unidad son:

- a. Aumento de la productividad como resultado de una red más confiable e íntegra y con menos indicadores de no disponibilidad.
- b. Cumplimiento con los acuerdos de niveles de servicio propuestos por la Subgerencia de Infraestructura Tecnológica.
- c. Mejora de la imagen y reputación comercial al estar disponibles los portales y servicios que son provistos para el uso de los ciudadanos.



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

2.11 TÉRMINOS Y DEFINICIONES ASOCIADOS

a. 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 Unidad. (ISO/IEC 27000). Ver

http://www.mintic.gov.co/gestionti/615/articles-482_G11_Analisis_Impacto.pdf al 2016-11-10

y <http://www.iso27000.es/glosario.html#section10> al 2016-11-10.

Cualquier componente que tenga valor para la Unidad. Esto puede incluir activos físicos tales como instalaciones, maquinaria y equipos, o bien recursos humanos, propiedad intelectual, imagen interna y externa y reputación. Ver https://drii.org/assets/glossary_doc/Glossary_Spanish.pdf al 2016-11-15.

b. Administrador de plataforma: o custodio del recurso tecnológico. Es una parte designada de la Unidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. Ver

http://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf al 2016-11-15.

c. Amenaza: situación o condición natural u ocasionada por el hombre que puede causar una interrupción de las operaciones o servicios de la Unidad. Ver https://drii.org/assets/glossary_doc/Glossary_Spanish.pdf al 2016-11-15.

d. Arquitectura de referencia: es un diseño de alto nivel, sin detalles tecnológicos o de productos, que se utiliza como una plantilla para guiar el bosquejo de otras arquitecturas más específicas. Esta plantilla incluye los principios de diseño que la guían, las decisiones de alto nivel que se deben respetar, los componentes que hacen parte de la solución, sus relaciones tanto estáticas como dinámicas, las recomendaciones tecnológicas y de desarrollo, las herramientas específicas de apoyo a la construcción y los componentes existentes reutilizables. El concepto de Arquitectura de Referencia se puede utilizar como base del diseño detallado de arquitecturas de solución, de software, de información o de plataforma tecnológica. Ver

<http://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html> al 2016-08-26.



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

e. Autorización: consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales. Ver <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981> al 2016-11-15.

f. Base de datos: conjunto organizado de datos personales que sea objeto de tratamiento. Ver Ley Estatutaria N° 1581 de 2016-11-15 publicado en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981> al 2016-11-15.

g. Bombas de correo electrónico: es una forma de abuso por internet que consiste en el envío de grandes cantidades de correos a una cuenta de correo con el objetivo de desbordar la casilla o saturar el servidor de correos de la Unidad en un ataque de denegación de servicio. Ver: http://www.alegsa.com.ar/Dic/bomba_de_email.php al 2016-11-23.

h. Caballo de troya: los troyanos informáticos son una clase de virus que se caracteriza por engañar a los funcionarios, contratistas, personal que labora en las instalaciones vinculado con un proveedor de la UAECD o personal externo (empresa o entidad externa) a la Unidad, disfrazándose de programas o archivos legítimos/benignos (fotos, archivos de música, archivos de correo, etc.), con el objeto de infectar y causar daño. Ver: <http://www.seguridadpc.net/troyanos.htm> al 2016-11-23.

i. Cifrado: en criptografía, el cifrado es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) transforma un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo. Ver [https://es.wikipedia.org/wiki/Cifrado_\(criptograf%C3%ADa\)](https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa)) al 2016-12-08

j. Cintoteca: recopilación de medios magnéticos, cuya finalidad es la preservación, protección y custodia de la información que estos almacenen. Entre los tipos de medios que reposan en una Cintoteca están: Disquetes, Láminas de Zinc, Cintas de 9 tracks, Cinta magnéticas, casetes, cartuchos, Discos removibles, Disco compacto [CD, DVD, Bluray], Discos Duros externos, Memorias USB, Memorias SD y micro SD. Las cintas y otros soportes han de ser guardados de un determinado modo, para proteger la información que contienen de elementos externos, preservándolos de humedad, calor, campos magnéticos y hasta el contacto humano hasta donde sea posible. Ver <https://es.wikipedia.org/wiki/Cintoteca> al 2016-11-23.

k. Confidencialidad: La información no se pone a disposición ni se revela a personas, entidades o procesos no autorizados. Por ejemplo, la asignación de cuentas de usuario con su respectiva contraseña, se autoriza el acceso a un recurso tecnológico.



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

Ver http://www.iso27000.es/download/doc_sgsi_all.pdf al 2016-08-26.

I. Copia de respaldo: una "copia de respaldo", "copia de seguridad" o también llamado "backup" (su nombre en inglés) es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas.

Ver https://es.wikipedia.org/wiki/Copia_de_seguridad al 2016-11-08. Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Ver https://drii.org/assets/glossary_doc/Glossary_Spanish.pdf al 2016-11-15.

m. Copia de respaldo completo: realiza una copia íntegra de los archivos. Ver <http://www.palentino.es/blog/pormenores-de-las-copias-de-seguridad-analizando-el-backup-pyme/> al 2016-11-08.

n. Copia de respaldo diferencial: realiza una copia creando un archivo sólo con las modificaciones desde la fecha de la última copia de respaldo completo. Es decir, si haces copia de respaldo completo el domingo por la noche y modificas el archivo el lunes en la mañana, por la noche se ejecuta la copia de respaldo diferencial y se crea un archivo que contiene los cambios del lunes. Si lo modificas el martes en la mañana, por la noche se ejecuta la copia de respaldo diferencial y se crea otro archivo con los cambios del lunes y del martes, si lo modificas el miércoles, se crea otro archivo con las modificaciones del lunes, el martes y el miércoles. Así sucesivamente. Ver

<http://www.palentino.es/blog/pormenores-de-las-copias-de-seguridad-analizando-el-backup-pyme/> al 2016-11-08.

o. Copia de respaldo incremental: realiza una copia creando un archivo por cada cambio que se realice desde la última copia de respaldo completo o incremental, es decir, si ejecutas la copia de respaldo completo el domingo en la noche, y modificas el archivo el lunes en la mañana, entonces en la noche del lunes se ejecuta la copia de respaldo incremental y crea un archivo sólo con las modificaciones del lunes. Si modificas el archivo el martes, en la noche se ejecuta la copia de respaldo incremental y se crea otro archivo sólo con las modificaciones del martes, si lo modificas el miércoles de mañana, en la noche se crea otro archivo solo con los cambios del miércoles y así sucesivamente. Ver



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

<http://www.palentino.es/blog/pormenores-de-las-copias-de-seguridad-analizando-el-backup-pyme/> al 2016-11-08.

p. Cuenta de usuario: cadena de caracteres que se utiliza para identificar a un usuario en la entrada a un sistema (login), como un servicio online, un sistema operativo, una red, etc. Ver <http://www.alegsa.com.ar/Dic/nombre%20de%20usuario.php> al 2016-08-26.

q. Custodio del recurso tecnológico: Es una parte designada de la Unidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. Ver http://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf al 2016-11-15.

r. Dato personal: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Dependiendo de su grado de utilización y acercamiento con la intimidad de las personas podrá ser pública, semiprivada o privada. Ver Ley Estatutaria N° 1581 de 2016-11-15 publicado en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981> al 2016-15-11.

s. Denegación de servicio: en seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de ordenadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. Ver:

<http://www.websecurity.es/que-es-un-ataque-denegaci-n-servicio> al 2016-11-23.

t. Derechos de autor: denominación que recibe la protección legal sobre toda creación del talento o del ingenio humano, dentro del ámbito científico, literario, artístico, industrial o comercial. La legislación sobre Derecho de autor protege exclusivamente la forma o medio en el cual las ideas del autor son descritas, explicadas o ilustradas, pero no protege las ideas, contenidos conceptuales, ideológicos o técnicos.

El Derecho de Autor comprende los Derechos Morales y los Derechos Patrimoniales. En el caso del software, la legislación colombiana lo asimila a la escritura de una obra literaria, permitiendo que el código fuente de un programa esté cubierto por la ley de Derechos de Autor (Ley 23 de 1982). Ver



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

http://www.iered.org/miembros/ulises/representacion-ideas/Derechos-Autor/propiedad_intelectual_en_la_legislacion_colombiana.html al 2016-12-07.

u. Derechos morales: consisten en el reconocimiento de la paternidad del autor sobre la obra realizada y el respeto a la integridad de la misma. Este derecho otorga al autor facultades para:

- 1) Exigir que su nombre y el título de la obra sean mencionados cada vez que ésta se utilice, publique o divulgue
- 2) Oponerse a las transformaciones o adaptaciones de la misma si esto afecta su buen nombre o reputación
- 3) Dejar la obra inédita o publicarla en forma anónima o bajo un seudónimo
- 4) Modificar la obra en cualquier tiempo y retirarla de la circulación, previo el pago de las indemnizaciones a que haya lugar
- 5) Estos derechos aparecen en el momento mismo de la creación de la obra, sin necesidad de registro y son del autor de manera personal e irrenunciable, por lo que no pueden enajenarse, ni embargarse, no prescriben y son de duración ilimitada Ver http://www.iered.org/miembros/ulises/representacion-ideas/Derechos-Autor/derechos_morales_y_patrimoniales_en_el_derecho_de_autor.html al 2016-12-07

v. Derechos patrimoniales: consisten en la facultad de aprovecharse y de disponer económicamente de la obra por cualquier medio, por tanto, se puede renunciar a ellos o embargarse, son prescriptibles y expropiables. Las distintas formas de utilización de una obra son independientes entre sí, tales como la: copia, reproducción, presentación pública, traducción, adaptación, etc. Sobre estas formas de utilización, el autor o titular de los derechos patrimoniales puede ceder (entregar los derechos a otra persona) o autorizar su uso (dar un permiso, pero sin ceder los derechos) para cada una de ellas y considerando límites de tiempo, cobertura y retribución económica. Para ceder los derechos se requiere la firma de un documento (público o privado) entre las partes y del registro de la obra ante la Dirección Nacional de Derechos de Autor. Para autorizar unos determinados usos, sólo se requiere explicitar las condiciones en una licencia o texto con la voluntad del autor o titular de los derechos patrimoniales. Ver http://www.iered.org/miembros/ulises/representacion-ideas/Derechos-Autor/derechos_morales_y_patrimoniales_en_el_derecho_de_autor.html al 2016-12-07.



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

w. Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de las personas, entidades o procesos autorizados cuando lo requieran. Por ejemplo, una persona autorizada para el ingreso de un aplicativo en la Unidad pueda acceder en su horario laboral. Ver http://www.iso27000.es/download/doc_sgsi_all.pdf al 2016-08-26. Es la habilidad de un servicio de TI o recurso tecnológico para realizar la función acordada cuando sea requerido. Por ejemplo, ingresar a un aplicativo de la Unidad en horario laboral.

Ver [https://www.axelos.com/Corporate/media/Files/Glossaries/ITIL_2011_Glossary_ES-\(Latin-America\)-v1-0.pdf](https://www.axelos.com/Corporate/media/Files/Glossaries/ITIL_2011_Glossary_ES-(Latin-America)-v1-0.pdf) al 2016-08-26.

x. Dispositivo Móvil: Conocido como computadora de bolsillo o computadora de mano (palmtop o handheld), es un tipo de computadora de tamaño pequeño, con capacidades de procesamiento, con conexión a Internet, con memoria, diseñado específicamente para una función, pero que pueden llevar a cabo otras funciones más generales. Algunos tipos de dispositivos móviles son:

- 1) Teléfonos inteligentes y Tabletas.
- 2) Relojes inteligentes
- 3) Agendas digitales
- 4) Calculadoras
- 5) Videoconsolas portátiles
- 6) Reproductores digitales
- 7) Cámaras fotográficas digitales
- 8) Cámaras de video digitales
- 9) Robots
- 10) Tarjetas inteligentes

Ver https://es.wikipedia.org/wiki/Dispositivo_m%C3%B3vil al 2017-10-05.

Entre los usos de los dispositivos móviles esta:

- 1) La navegación web.
- 2) El uso de canales electrónicos.
- 3) El acceso al correo electrónico.
- 4) El acceso a las redes sociales.



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

y. Enajenar: traspasar el derecho de propiedad sobre una cosa, que puede ser a cambio de un precio, como ocurre en el contrato de compra venta (enajenación onerosa) o de manera gratuita como sucede en la donación. Ver

<http://deconceptos.com/ciencias-sociales/enajenado> al 2016-12-12.

z. Encargado del tratamiento: 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. Ver Ley Estatutaria N° 1581 de 2016-11-15 publicado en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981> al 2016-11-15.

aa. Estándar: es una regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la Unidad antes de crear nuevas políticas. Ver http://www.mintic.gov.co/gestioni/615/articles-5482_G2_Politica_General.pdf al 2016-10-31.

bb. Etiqueta: es un tipo de información que describe o define algún aspecto de un recurso tecnológico (como un documento, una imagen, una página web, etc). Las etiquetas son un tipo de metadato que capturan conocimiento en forma de descripciones, categorizaciones, clasificaciones, semánticas, comentarios, notas, hiperenlaces o referencias. Ver http://www.alegsa.com.ar/Dic/etiqueta_metadato.php al 2016-11-28.

cc. Guía: una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares, buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar un proceso. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo. Ver http://www.mintic.gov.co/gestioni/615/articles-5482_G2_Politica_General.pdf al 2016-10-31.

dd. Gusano informático: es un malware o software de tipo malicioso que se caracteriza principalmente por expandirse fácil y rápidamente en los archivos y programas de una estación de trabajo generando a su paso diferentes niveles de daño. Con la masificación de internet, estos gusanos informáticos encuentran más vías de desplazamiento, teniendo mayores posibilidades de entrar a otras estaciones de trabajo y generar daños mil veces mayores. Ver <http://www.definicionabc.com/tecnologia/gusano-informatico.php> al 2016-11-23.



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

ee. Hacking ético: acto de una persona para usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño. Ver <http://www.internetglosario.com/1131/Hacking%C3%A9tico.html> al 2016-11-28.

Uso de técnicas de ataque para encontrar fallas de seguridad en los recursos tecnológicos, con el permiso de la Unidad con el objetivo de mejorar la seguridad de la misma. Ver <https://www.seguridadx.com/que-es-ethical-hacking/> al 2016-11-28.

ff. Hardware: se refiere a las partes físicas tangibles de un recurso tecnológico; sus componentes eléctricos, electrónicos, electromecánicos, mecánicos, cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado componen el hardware; contrariamente, el soporte lógico e intangible es el llamado software. Por ejemplo, disco duro, memoria RAM, procesador, tarjeta madre, monitor, teclado, mouse, impresora. Ver <https://es.wikipedia.org/wiki/Hardware> al 2016-09-06.

gg. Impacto: consecuencias que puede ocasionar a la Unidad, la materialización del riesgo. Ver <http://sgc.dadep.gov.co/1/4/127-GUIDE-05.pdf> al 2016-11-15. Efecto, aceptable o no, que un evento tiene en la Unidad. Los tipos de impactos al negocio son normalmente descritos como financieros y no financieros, y posteriormente se dividen en tipos específicos. https://drii.org/assets/glossary_doc/Glossary_Spanish.pdf al 2016-11-15.

hh. IMEI: El IMEI (del inglés International Mobile Station Equipment Identity, identidad internacional de equipo móvil) es un código USSD pregrabado en los teléfonos móviles GSM. Este código identifica al aparato de forma exclusiva a nivel mundial, y es transmitido por el aparato a la red al conectarse a esta. Ver <https://es.wikipedia.org/wiki/IMEI> al 2017-11-15.

ii. Incidente de seguridad de la información: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones de la Unidad y amenazar la seguridad de la información. Por ejemplo, el acceso no autorizado a información confidencial, robo o pérdida de información. Ver <http://www.iso27000.es/glosario.html> al 2016-08-26.

jj. Información: se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. Ver <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882> al 2016-11-15.



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

kk. Información pública: es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. Ver <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882> al 2016-11-15.

ll. 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. Ver <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882> al 2016-11-15.

mm. 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. Ver <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882> al 2016-11-15.

nn. Integridad: Propiedad que garantiza que los datos no se han modificado, destruido o perdido debido a acciones no autorizadas o accidentales. Ver https://drii.org/assets/glossary_doc/Glossary_Spanish.pdf al 2016-11-15

oo. MAC (Por sus siglas en inglés Media Access Control): Es un identificador de 48 bits (6 bloques de dos caracteres hexadecimales (4 bits)) que corresponde de forma única a una tarjeta o dispositivo de red. Ver https://es.wikipedia.org/wiki/Direcci%C3%B3n_MAC al 2017-11-14.

pp. Malware: abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: virus, troyanos (Trojans), gusanos, keyloggers, botnets, backdoors, ransomwares, spyware, adware, keyloggers, rogues, etc. En la actualidad y dado que los antiguos llamados virus informáticos ahora comparten funciones con sus otras familias, se denomina directamente a cualquier código malicioso (parásito/infección), directamente como un "Malware".

1) Virus: son programas maliciosos (malwares) que "infectan" a otros archivos del sistema con la intención de modificarlo o dañarlo. Dicha infección consiste en incrustar su código malicioso en el interior del archivo "víctima" (normalmente un ejecutable) de forma que a partir de ese momento dicho ejecutable pasa a ser portador del virus y por tanto, una nueva fuente de infección. Su nombre lo adoptan de la similitud que tienen con los virus biológicos



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

que afectan a los humanos, donde los antibióticos en este caso serían los programas Antivirus.

2) Adware: software que despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes, o a través de una barra que aparece en la pantalla simulando ofrecer distintos servicios útiles para el usuario. Generalmente, agregan ícono gráficos en las barras de herramientas de los navegadores de Internet o en los clientes de correo, la cuales tienen palabras claves predefinidas para que el usuario llegue a sitios con publicidad, sea lo que sea que esté buscando.

3) Backdoors: programas diseñados para abrir una "puerta trasera" en nuestro sistema de modo tal de permitir al creador de esta aplicación tener acceso al sistema y hacer lo que desee con él. El objetivo es lograr una gran cantidad de computadoras infectadas para disponer de ellos libremente hasta el punto de formas redes como se describen a continuación.

4) Botnet: es una red de equipos infectados por códigos maliciosos, que son controlados por un atacante, disponiendo de sus recursos para que trabajen de forma conjunta y distribuida. Cuando un equipo tecnológico a ha sido afectado por un malware de este tipo, se dice que es un equipo es un robot o zombi.

5) Gusanos: subconjunto de malware. Su principal diferencia con los virus radica en que no necesitan de un archivo anfitrión para seguir vivos. Los gusanos pueden reproducirse utilizando diferentes medios de comunicación como las redes locales, el correo electrónico, los programas de mensajería instantánea, redes P2P, dispositivos USBs y las redes sociales.

6) Keylogger: aplicaciones encargadas de almacenar en un archivo todo lo que el usuario ingrese por el teclado (capturadores de teclado). Son ingresados por muchos troyanos para robar contraseñas e información de los equipos en los que están instalados.

7) PUP: Potentially Unwanted Programs (Programa potencialmente no deseado) que se instala sin el consentimiento del usuario y realiza acciones o tiene características que pueden menoscabar el control del usuario sobre su privacidad, confidencialidad, uso de recursos del ordenador, etc.

8) Rogue: programa falso que dice ser o hacer algo que no es. Con la proliferación del spyware estos comenzaron a surgir como un importante negocio para los ciberdelincuentes en formato de "Falso Antispyware". Con el tiempo fueron evolucionando creando desde "falsos optimizadores" de windows, y en los más extendidos "falsos antivirus".



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

9) Al ejecutarlos 'siempre' van a mostrar alguna falsa infección o falso problema en el sistema que si queremos arreglar vamos tener que comprar su versión de pago, la cual obviamente en realidad no va a reparar ni desinfectar nada, pero nos va a mostrar que sí.

10) Spam: se denomina spam al correo electrónico no solicitado enviado masivamente por parte de un tercero. En español, también es identificado como correo no deseado o correo basura.

11) Troyano: en la teoría, un troyano no es virus, ya que no cumple con todas las características de los mismos, pero debido a que estas amenazas pueden propagarse de igual manera, suele incluirse dentro del mismo grupo. Un troyano es un pequeño programa generalmente alojado dentro de otra aplicación (un archivo) normal. Su objetivo es pasar inadvertido al usuario e instalarse en el sistema cuando este ejecuta el archivo "huésped". Luego de instalarse, pueden realizar las más diversas tareas, ocultas al usuario. Actualmente se los utiliza para la instalación de otros malware como backdoors y permitir el acceso al sistema al creador de la amenaza. Algunos troyanos, los menos, simulan realizar una función útil al usuario a la vez que también realizan la acción dañina. La similitud con el "caballo de Troya" de los griegos es evidente y debido a esa característica recibieron su nombre.

12) Spyware: aplicación que recopila información sobre una persona u organización sin su conocimiento ni consentimiento. El objetivo más común es distribuirlo a empresas publicitarias u otras organizaciones interesadas. Normalmente, este software envía información a sus servidores, en función a los hábitos de navegación del usuario. También, recogen datos acerca de las webs que se navegan y la información que se solicita en esos sitios, así como direcciones IP y URLs que se visitan. Esta información es explotada para propósitos de mercadotecnia, y muchas veces es el origen de otra plaga como el SPAM, ya que pueden encarar publicidad personalizada hacia el usuario afectado. Con esta información, además es posible crear perfiles estadísticos de los hábitos de los internautas. Ambos tipos de software generalmente suelen "disfrazarse" de aplicaciones útiles y que cumplen una función al usuario, además de auto ofrecer su descarga en muchos sitios reconocidos.

13) Ransomware o secuestradores: código malicioso que cifra la información del ordenador e ingresa en él una serie de instrucciones para que el usuario pueda recuperar sus archivos. La víctima, para obtener la contraseña que libera la información, debe pagar al atacante una suma de dinero, según las instrucciones que este disponga. Su popularización llevo a través de la extendida variante del "virus de la policía" la cual se ha extendido por todo el mundo secuestrando los equipos bloqueando la pantalla con una imagen perteneciente de



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

la policía de su país. Ver <https://www.infospware.com/articulos/que-son-los-malwares/> al 2016-12-07

qq. Mejor Práctica: una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad. Ver http://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf al 2016-10-31.

rr. Licencia de software: es la autorización que el autor o autores, que son quienes ostentan el derecho intelectual exclusivo de su obra, conceden a otros para utilizar sus obras, en este caso los programas. Los autores, pueden otorgar distinto tipo de licencia, pueden sólo autorizar su uso, pueden autorizar su modificación o distribución, etc. Los tipos de licencia de software más comunes que podemos encontrar:

1) Freeware: son programas gratuitos, sin límites ni en el tiempo ni en la funcionalidad del programa. En ocasiones podremos encontrarnos programas que son freeware para uso personal, pero no podremos utilizar en el ámbito comercial.

2) Shareware y Trial: el autor crea un software y lo distribuye a través de diferentes medios, para que el usuario pueda evaluar de forma gratuita el producto, normalmente por un tiempo especificado, aunque a veces el programa limita las opciones. Una vez el periodo de prueba termina, bien se abona el programa o bien se desinstala. Estos programas los podemos utilizar de forma gratuita, normalmente por un tiempo limitado. Una vez el periodo de prueba termina, tendremos que comprar el programa o bien lo desinstalamos, porque el programa dejará de funcionar. Algunos troyanos, los menos, simulan realizar una función útil al usuario a la

3) Evaluación y Demo: casi igual que el Shareware, pero en la mayoría de los casos el periodo de prueba y las funcionalidades, suelen ser más limitadas.

4) Adware: suelen ser programas shareware que de forma automática nos muestra o nos descarga publicidad a nuestro PC, a veces sólo cuando lo ejecutamos, otras simplemente cuando lo instalamos. Cuando compramos la versión registrada o la licencia, normalmente se eliminan los anuncios. Hay que estar atentos a la hora de instalarlos, pues a veces dan opción para evitar la instalación de publicidad.



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

5) Software libre: aquí el autor deja libertad a los usuarios, por tanto, el programa puede ser usado, copiado, estudiado, modificado y redistribuido libremente. Pero eso no quiere decir que tenga que ser obligatoriamente gratis, podemos encontrar programas bajo esta licencia que son de pago, aunque suelen ser muy económicos. Ver <https://basicoyfacil.wordpress.com/2008/12/13/que-es-una-licencia-de-software/> al 2016-12-18.

ss. Pentesting: un test de penetración consiste en pruebas ofensivas contra los mecanismos de defensa existentes en el entorno que se está analizando. Estas pruebas comprenden desde el análisis de dispositivos físicos y digitales, hasta el análisis del factor humano utilizando ingeniería social. El objetivo de estas pruebas es verificar bajo situaciones extremas cuál es el comportamiento de los mecanismos de defensa, específicamente, se busca detectar vulnerabilidades en los mismos. Además, se identifican aquellas faltas de controles y las brechas que pueden existir entre la información crítica y los controles existentes. Ver <http://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/> al 2016-12-07.

tt. Política: declaración de alto nivel que describe la posición de la Unidad sobre un tema específico. Ver http://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf al 2016-10-14.

uu. Privilegios o permisos: son los derechos otorgados a un usuario o rol - por ejemplo, el privilegio de modificar unos datos en particular, o para autorizar un cambio. [https://www.axelos.com/Corporate/media/Files/Glossaries/ITIL_2011_Glossary_ES-\(Latin-America\)-v1-0.pdf](https://www.axelos.com/Corporate/media/Files/Glossaries/ITIL_2011_Glossary_ES-(Latin-America)-v1-0.pdf) al 2016-09-06.

vv. Procedimiento: los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la Unidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican. Ver http://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf al 2016-10-14.



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

ww. Propietario de la información: es una parte designada de la Unidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. Ver http://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf al 2016-11-15. Es una parte designada de la Unidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de definir quienes tienen acceso y que pueden hacer con la información y de determinar cuáles son los requisitos para que la misma se salvable ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada, y al mismo tiempo de definir que se hace con la información una vez ya no sea requerida. Ver http://www.academia.edu/18756118/MANUAL_DE_BD_Ver_2012_REV al 2016-11-15.

xx. Protocolo de Transferencia de Archivos - FTP (Por sus siglas en inglés File Transfer Protocol): protocolo para intercambiar archivos en Internet. Utiliza los protocolos de Internet TCP/IP para permitir la transferencia de datos, de la misma manera que el HTTP en la transferencia de páginas web desde un servidor al navegador de un funcionario, contratista, personal que labora en las instalaciones vinculado con un proveedor de la UAECED o personal externo (empresa o entidad externa) y el SMTP para transferir correo electrónico a través de Internet. Se utiliza principalmente para descargar un archivo de un servidor o para subir un archivo a un servidor a través de Internet. Ver: <http://www.masadelante.com/faqs/ftp> al 2016-12-08. Es un protocolo de red utilizado para la transferencia de archivos entre un equipo de cómputo y otro a través del Internet. Los funcionarios, contratistas, personal que labora en las instalaciones vinculado con un proveedor de la UAECED o personal externo (empresa o entidad externa) de FTP son autenticados a través de una cuenta de usuario y su contraseña. Ver <http://soporte-libreria.iberlibro.com/2012/11/que-es-protocolo-seguro-de-transferencia-de-archivo-ftps.html> al 2016-12-12.

yy. Protocolo Seguro de Transferencia de Archivos - SFTP (Por sus siglas en inglés Secure File Transfer Protocol): es un protocolo usado para abarcar un número de formas en las cuales el Protocolo de Transferencia de Archivos – FTP puede realizar transferencias de ficheros en formas seguras. Cada forma conlleva el uso de una capa debajo del protocolo estándar FTP para cifrar los datos. Ver <http://soporte-libreria.iberlibro.com/2012/11/que-es-protocolo-seguro-de-transferencia-de-archivo-ftps.html> al 2016-12-12.



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

zz. Proveedor: Es un tercero, responsable de suministrar de bienes o servicios que se requieren para proporcionar servicios de TI. Ejemplos de proveedores incluyen a los vendedores de productos básicos de hardware y software, proveedores de redes y telecomunicaciones, y las organizaciones de outsourcing. Ver

[https://www.axelos.com/Corporate/media/Files/Glossaries/ITIL_2011_Glossary_ES-\(Latin-America\)-v1-0.pdf](https://www.axelos.com/Corporate/media/Files/Glossaries/ITIL_2011_Glossary_ES-(Latin-America)-v1-0.pdf) al 2016-08-26.

aaa. Recurso tecnológico: medio que se vale de la tecnología para cumplir con su propósito. Los recursos tecnológicos pueden ser tangibles (como una computadora, una impresora u otra máquina) o intangibles (un sistema, una aplicación virtual, un software) Ver: <http://definicion.de/recursos-tecnologicos/> al 2016-08-26.

bbb. Responsable del tratamiento: 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. Ver Ley Estatutaria N° 1581 de 2016-11-15 publicado en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981> al 2016-11-15.

ccc. 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. Ver <http://www.iso27000.es/glosario.html#section10r> al 2016-11-07.

ddd. Salvaguarda: Práctica, procedimiento o mecanismo para tratar los riesgos. Ver http://www.barrancabermeja-santander.gov.co/alcaldia/index.php?option=com_content&view=article&id=402 al 2016-11-28.

eee. Spam: son mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva. La vía más utilizada es la basada en el correo electrónico, pero puede presentarse por programas de mensajería instantánea o por dispositivos móviles. Ver <http://www.segu-info.com.ar/malware/spam.htm> al 2016-11-23.

fff. Software: conjunto de programas, instrucciones y datos que circulan en un recurso tecnológico con una función determinada, y que le permiten al usuario llevar adelante distintas tareas. A grandes rasgos, el software puede ser definido como la parte intangible del recurso tecnológico y es justamente lo opuesto del hardware. Por ejemplo, Aplicaciones ofimática, ArGIS, Oracle, antivirus, Visual Studio, Sistema Integrado de Información Catastral – SIIC. Ver: <http://www.tipos.co/tipos-de-software/#ixzz4JUYKDsFk> al 2016-09-06.



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

El software se suele clasificar en tres grandes grupos:

- 1) Software de sistema o base
- 2) Software de programación
- 3) Software de aplicación Ver <http://www.tipos.co/tipos-de-software/#ixzz4JUYKDsFk> al 2016-09-06.

ggg. Software de sistema o base: es aquel que permite a los usuarios interactuar con el sistema operativo, así como también controlarlo. Este sistema está compuesto por una serie de programas que tienen como objetivo administrar los recursos del hardware y, al mismo tiempo, le otorgan al usuario una interfaz. Ver: <http://www.tiposde.org/informatica/12-tipos-de-software/> al 2016-09-06.

El software de sistema se clasifica de la siguiente forma:

1) Sistema operativo: incluye una serie de programas abocados a la administración de los recursos tecnológicos. Además de esto, el sistema operativo controla el funcionamiento de la misma. Este software tiene cinco funciones elementales: ofrecer servicio de soporte, administrar tareas, recursos y archivos y, por último, suministrarle una interfaz al usuario. Por ejemplo, Windows, MAC OS, Ubuntu, Linux. Ver:

<http://www.tipos.co/tipos-de-software/#ixzz4JUYKDsFk> al 2016-09-06.

2) Programas utilitarios: aquellos que tienen como finalidad la resolución de inconvenientes puntuales. Sumado a esto, cumplen funciones que ayudan a mantener el recurso tecnológico, entre otras tareas. Por ejemplo, antivirus, quemadores, compresores de archivos. Ver: <http://www.tipos.co/tipos-de-software/#ixzz4JUYKDsFk> al 2016-09-06.

3) Controladores de dispositivos: sirven como puentes con otros programas de mayor complejidad para que de esta forma logren la interacción con alguno de los dispositivos del hardware. Por ejemplo, drivers para impresora, disco duro, memoria USB. Ver: <http://www.tipos.co/tipos-de-software/#ixzz4JUYKDsFk> al 2016-09-06.

4) Software de diagnóstico: por medio de software como estos, las funciones, la temperatura, la transferencia de datos, así como también el rendimiento del hardware son controlados y monitoreados. Por ejemplo, limpiadores de registro, optimizadores de velocidad y conexiones, monitoreo de herramientas del sistema, desfragmentadores, particionadores. Ver:

<http://www.tipos.co/tipos-de-software/#ixzz4JUYKDsFk> al 2016-09-06.



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

5) Servidores: estos son los programas que realizan tareas para los clientes, que son una serie de aplicaciones. Generalmente, estas tareas están vinculadas con ofrecer servicio de archivos y de aplicaciones. Por ejemplo, ArGIS, Oracle. Ver:

<http://www.tipos.co/tipos-de-software/#ixzz4JUYKDsFk> al 2016-09-06.

hhh. Software de programación: son aquellas herramientas que un programador utiliza para poder desarrollar programas informáticos. Para esto, el programador se vale de distintos lenguajes de programación. Ver: <http://www.tiposde.org/informatica/12-tipos-de-software/> al 2016-09-06. El software de programación se clasifica de la siguiente forma:

1) Compiladores: este tipo de software es el que se encarga de traducir un programa que se encuentre escrito en un determinado lenguaje de programación a otro. De esta forma, se crea un programa similar que la computadora logrará interpretar. Por ejemplo, C, C++, Visual Basic, Fortran, Cobol. Ver:

<http://www.tipos.co/tipos-de-software/#ixzz4JUYKDsFk> al 2016-09-06.

2) Depurador: este software son los que se utilizan cuando se necesita depurar o probar otros programas. También, estos programas pueden ser usados para que le incorporen protección a la memoria, para evitar de esta forma cualquier intromisión en la información. Por ejemplo, GNU Debugger (gdb), SoftICE. Ver:

<http://www.tipos.co/tipos-de-software/#ixzz4JUYKDsFk> al 2016-09-06.

3) Editores de texto: programa informático que permite crear y modificar archivos digitales compuestos únicamente por textos sin formato, conocidos comúnmente como archivos de texto o “texto plano”. Por ejemplo, Pascal, Edit de MS-DOS. Ver: https://es.wikipedia.org/wiki/Editor_de_texto al 2016-09-06.

4) Intérpretes: programa informático capaz de analizar y ejecutar otros programas. Los intérpretes se diferencian de los compiladores o de los ensambladores en que mientras estos traducen un programa desde su descripción en un lenguaje de programación al código de máquina del sistema, los intérpretes sólo realizan la traducción a medida que sea necesaria, típicamente, instrucción por instrucción, y normalmente no guardan el resultado de [https://es.wikipedia.org/wiki/Int%C3%A9rprete_\(inform%C3%A1tica\)](https://es.wikipedia.org/wiki/Int%C3%A9rprete_(inform%C3%A1tica)) al 2016-09-06.

5) Enlazadores: programa que toma los objetos generados en los primeros pasos del proceso de compilación, la información de todos los recursos necesarios (biblioteca), quita aquellos recursos que no necesita, y enlaza el código objeto con su(s) biblioteca(s) con lo



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

que finalmente produce un fichero ejecutable o una biblioteca. En el caso de los programas enlazados dinámicamente, el enlace entre el programa ejecutable y las bibliotecas se realiza en tiempo de carga o ejecución del programa. Por ejemplo, Oracle, Circle. Ver: <https://es.wikipedia.org/wiki/Enlazador> al 2016-09-06.

6) Entornos de Desarrollo Integrados (IDE): aplicación informática que proporciona servicios integrales para facilitarle al desarrollador o programador el desarrollo de software. Normalmente, un IDE consiste de un editor de código fuente, herramientas de construcción automáticas y un depurador. Por ejemplo, Microsoft® Visual Studio, Visual C++, Eclipse, Netbeans, IntelliJ IDEA, JBuilder de Borland, JDeveloper de Oracle, KDevelop, Anjuta, Clarion. Ver: https://es.wikipedia.org/wiki/Entorno_de_desarrollo_integrado al 2016-09-06.

iii. Software de aplicación: aquí se incluyen todos aquellos programas que permiten al usuario realizar una o varias tareas específicas. Aquí se encuentran aquellos programas que las personas usan de manera cotidiana como: procesadores de texto, hojas de cálculo, editores, telecomunicaciones, software de cálculo numérico y simbólico, videojuegos, entre otros. Ver: <http://www.tiposde.org/informatica/12-tipos-de-software/> al 2016-09-06.

El software de aplicación se clasifica de la siguiente forma:

1) Programas de CAD: software como estos son sumamente utilizados por profesionales como diseñadores, arquitectos o ingenieros a la hora de realizar un plano. Por ejemplo, Blender y AutoCAD.

<http://www.tipos.co/tipos-de-software/#ixzz4JUYKDsFk> al 2016-09-06.

2) Aplicaciones ofimáticas: Recopilación de aplicaciones informáticas utilizadas en oficinas, para realizar diferentes funciones sobre archivos y documentos, como crear, modificar, organizar, escanear, imprimir, entre otros. Por ejemplo, Word, Excel, Power Point, Visio. Ver https://es.wikipedia.org/wiki/Paquete_de_oficina al 2016-09-02.

3) Diseño gráfico: permiten realizar tareas de retoque, composición e incluso manipulación de cualquier imagen. Por ejemplo, Adobe InDesign, Adobe Illustrator, CorelDraw, Adobe PhotoShop. <http://www.tipos.co/tipos-de-software/#ixzz4JUYKDsFk> al 2016-09-06.

4) Bases de datos: este tipo de software permite guardar información para luego poder hacer un monitoreo de la misma. Entre otras cosas, se almacenan registros de productos, materiales, clientes, proveedores, etcétera. Por ejemplo, Office Base o Microsoft Access,



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

BBase, FoxPro, FileMaker, Kexi. <http://www.tipos.co/tipos-de-software/#ixzz4JUYKDsFk> al 2016-09-06.

5) Programas médicos: herramientas son muy útiles para que los médicos puedan llevar un control ordenado de sus pacientes. El software médico permite, entre otras cosas, medir e interpretar la presión arterial, la respiración o la frecuencia cardíaca. Además, hay programas diseñados para almacenar y organizar datos e información vinculada con farmacias, turnos, medicamentos, seguros médicos, entre muchas otras cosas. Por ejemplo, Cardiactrex X/70. <http://www.tipos.co/tipos-de-software/#ixzz4JUYKDsFk> al 2016-09-06.

6) Juegos de video: son diseñados con el objetivo de entretener a los usuarios. De todas formas, existen algunas opciones que permiten darles otros usos, vinculados con la salud, la educación o bien para practicar disciplinas o deportes. Existen distintas variedades de videojuegos, de acuerdo a su contenido, entre otros, se pueden nombrar los siguientes: de aventura, de carreras, de simulación, deportivos, los que requieren agilidad mental, de luchas, de disparos, de estrategia, musicales. <http://www.tipos.co/tipos-de-software/#ixzz4JUYKDsFk> al 2016-09-06.

7) Software de gestión empresarial: son diseñados a partir de las necesidades y requisitos de la Unidad, con el objetivo de facilitar o automatizar ciertas tareas esenciales en la labor diaria. Por medio de estos programas, se obtiene una mejor productividad y organización. Por ejemplo: Sistema Integrado de Información Catastral – SIIC, SI – Capital. <http://www.tipos.co/tipos-de-software/#ixzz4JUYKDsFk> al 2016-09-06.

8) Editores de texto: esta clase de software le permite al usuario la modificación, así como también la creación de archivos de textos que no posean formato alguno. Entre otras cosas, estos programas permiten formatear, importar, seleccionar texto, cortar, copiar, pegar, buscar, reemplazar y filtrar, entre otras cosas. Por ejemplo, Bloc de notas, Kate, Gedit, Vi y Emacs. <http://www.tipos.co/tipos-de-software/#ixzz4JUYKDsFk> al 2016-09-06.

9) Software educativo: es una herramienta pedagógica o de enseñanza que, por sus características, es aquello vinculado a la educación (la instrucción, formación o enseñanza que se imparte) y el aprendizaje autónomo y que, además, permite la adquisición de conocimientos y el desarrollo de ciertas habilidades cognitivas. Por ejemplo, Clic, GCompris, PLATO. Ver https://es.wikipedia.org/wiki/Software_educativo al 2016-09-06.

jjj. Software libre: software que, por elección manifiesta de su autor, puede ser copiado, estudiado, modificado, utilizado libremente con cualquier fin y redistribuido con o sin cambios o mejoras. Ver: https://es.wikipedia.org/wiki/Software_libre al 2016-09-06.



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

kkk. Titular: persona natural cuyos datos personales sean objeto de tratamiento. Ver Ley Estatutaria N° 1581 de 2016-11-15 publicado en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981> al 2016-11-15.

III. Tratamiento: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. Ver Ley Estatutaria N° 1581 de 2016-11-15 publicado en <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981> al 2016-11-15.

mmm. 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. Ver http://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf al 2016-11-10 y <http://www.iso27000.es/glosario.html#section10a> al 2016-11-10.

nnn. Usuario: cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información. Ver http://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf al 2016-11-15.

ooo. Virus informático: es un malware o software desarrollado con fines maliciosos; su objetivo es afectar el funcionamiento de la estación de trabajo sin que el funcionario, contratista, personal que labora en las instalaciones vinculado con un proveedor de la UAECD o personal externo (empresa o entidad externa) lo advierta o lo autorice. Por eso estos programas se "camuflan" detrás de una apariencia inofensiva: pueden ofrecerse como juegos, películas o música, por ejemplo, pero en realidad se trata de virus. Ver <http://definicion.de/virus-informatico/> al 2016-11-23.

ppp. VPN (Virtual Protocol Network): Red Privada Virtual es una tecnología que permite la extensión de una red pública como Internet a un espacio de red local. Brinda la posibilidad de conectarse a una red pública generando una extensión a nivel de área local. Si bien se utiliza una red pública como es la de conexión a Internet, los datos son transmitidos por un canal privado, de forma que no peligran la seguridad ni la integridad de la información interna. Los datos son cifrados y descifrados alternativamente, ahorrando dinero y problemas a empresas de distinta escala. Ver <http://www.definicionabc.com/tecnologia/vpn.php> al 2016-11-15 Es una extensión



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

segura de una LAN (Local Area Network o Red de Área Local) sobre Internet u otro tipo de red pública. Gracias a la VPN, una computadora puede recibir y enviar datos sobre redes públicas o que están compartidas con las mismas garantías de seguridad y funcionalidad de una red privada. Ver <http://definicion.de/vpn/> al 2016-11-15.

qqq. Vulnerabilidad: debilidad en un activo o control que puede ser explotada por una o más amenazas. Ver <http://www.iso27000.es/glosario.html#section10v> al 2016-11-07. Grado de exposición de una persona, activo, proceso, información, infraestructura y otros recursos a las acciones o efectos de un riesgo, suceso u otro acontecimiento. Ver https://drii.org/assets/glossary_doc/Glossary_Spanish.pdf al 2016-11-15.

3 DOCUMENTOS DE REFERENCIA

- a. Norma técnica colombiana NTC-ISO-IEC COLOMBIANA 27001 versión 2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos.
- b. Norma técnica colombiana NTC-ISO-IEC COLOMBIANA 27000 versión 2007. Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información.
- c. Guía técnica GTC-ISO/IEC COLOMBIANA 27003 Tecnología de la información. Técnicas de seguridad. Guía de implementación de un sistema de gestión de seguridad de la información.
- d. Ley N° 1712 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones" del 2014-03-06.
- e. Ley N° 1581 "Por la cual se dictan disposiciones generales para la protección de datos personales" del 2012-10-17.
- f. Decreto N° 1377 "Por el cual se reglamenta parcialmente la Ley 1581 de 2012" del 2013-06-27.
- g. Circular 094 de 2013 de la Secretaría General de la Alcaldía Mayor de Bogotá D.C., asunto: "Actualización de políticas - marco general sobre la protección de datos personales. Implementación y cumplimiento del Decreto 1377 de 2013 'por el cual se reglamenta parcialmente la Ley 1581 de 2012'".



ALCALDÍA MAYOR
DE BOGOTÁ D.C.
HACIENDA
Unidad Administrativa Especial
Catastro Distrital

POLITICAS DETALLADAS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

- h. Norma técnica colombiana NTC-5722 versión 2012. Continuidad de negocio. -Sistemas de gestión de continuidad de negocio. Requisitos.
- i. Norma internacional ISO22301:2012 versión 2012. Seguridad de la sociedad - Sistemas de gestión de la continuidad del negocio.