INDICE

A B C D E F G H I J K L LL

M N O P R S T U V W X Z

-A

ACTIVO INFORMATICO
Cualquier cosa que tiene valor para la organización en el campo informático. En este concepto se incluyen la información, todo el Hardware y Software, e infraestructura de redes y comunicaciones, tales como equipos de cómputo o para procesamiento de información, sistemas operativos, bases de datos, sistemas de almacenamiento masivo de información, aplicaciones, programas, sistemas de información, dispositivos de comunicaciones alámbrica e inalámbricas y dispositivos y accesorios relacionados con todos los anteriores así como los dispositivos para control de acceso físico y lógico y para seguridad informática.

ACUERDO DE USO
Acuerdo que contiene las condiciones para el buen uso de los recursos y servicios informáticos y de la(s) cuenta(s) de usuario asignadas para el acceso y utilización de la información de la Empresa de Acueducto y Alcantarillado de Bogotá, E.S.P.

ADMINISTRADOR
Persona que se encarga de todas las tareas de mantenimiento de un sistema informático. Tiene acceso total y sin restricciones al mismo

AMENAZA
Eventos que pueden desencadenar un incidente informático en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos. La amenaza se puede materializar y transformarse en agresiones. Puede afectar confidencialidad, integridad y disponibilidad de los sistemas de información. Existen amenazas relacionadas con falla humanas, con ataques malintencionados o con catástrofes naturales.

ANÁLISIS DE RIESGO
El análisis de riesgo, es el estudio de las causas de las posibles amenazas, y los daños y consecuencias que éstas puedan producir. Este tipo de análisis es ampliamente utilizado como herramienta de gestión en estudios financieros y de seguridad para identificar riesgos (métodos cualitativos) y otras para evaluar riesgos (generalmente de naturaleza cuantitativa).

ANÁLISIS DE VULNERABILIDADES
Análisis del estado de la seguridad de un sistema o sus componentes mediante el envío de pruebas y recogida de resultados en intervalos.

ANTI-VIRUS
Aplicación cuya finalidad es la detección y eliminación de virus, troyanos y gusanos informáticos

ANTISPAM
Equipo dedicado o software que mediante una serie de reglas y filtros, busca identificar correos publicitarios no deseados (spam) para evitar llenar el buzón y evitar pérdida de tiempo en la revisión de éstos. Los equipos antispam se valen de diferentes tipos de filtros, como las listas negras, los bayesianos, entre otros

ANTISPYWARE
Equipo dedicado o software que detecta y elimina el spyware detectado, así como previene la instalación de nuevo spyware. Los equipos antispyware al reconocer un equipo infectado, evitan las acciones que realiza el spyware, así como el envío de información privada, que el spyware se extienda en otros equipos, etc.

ARCHIVO
Conjunto de bytes relacionados y tratados como una unidad. Un archivo puede contener programas, datos o ambas cosas.

ATAQUE
Intento de comprometer alguna de las capacidades de un sistema de información. Dependiendo del objetivo del ataque, pueden afectar a la confidencialidad, integridad o disponibilidad del sistema. El ataque puede ser un evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

ATACANTE
Son las personas que buscan tener acceso ilegal a los activos informáticos de una organización. En este rol se pueden distinguir tres tipos hacker, cracker y lammer:

ATAQUES A PASSWORDS - Password Attacks
Es un intento de obtener o descifrar una password legítima de usuario. Las medidas de seguridad contra estos ataques es muy limitada consistiendo en una política de passwords, que incluye una longitud mínima, palabras no reconocibles y cambios frecuentes.

ATAQUE DE DICCIONARIO -Dictionary Attack
Método empleado para romper la seguridad de los sistemas basados en passwords (contraseñas) en la que el atacante intenta dar con la clave adecuada probando todas (o casi

todas) las palabras posibles o recogidas en un diccionario idiomático. Generalmente no se introducen manualmente las posibles contraseñas sino que se emplean programas especiales que se encargan de ello.

ATAQUE DE FUERZA BRUTA - Brute Force Attack
Método empleado para romper la seguridad vía contraseña probando todas las combinaciones posibles de palabras (distinto del ataque de diccionario que prueba palabras aisladas). Un ataque de fuerza bruta teóricamente no puede ser resistido por ningún sistema, siempre y cuando se disponga del tiempo suficiente y del equipo adecuado. Así, las claves lo suficientemente largas (y mejor aún si combinan caracteres alfanuméricos) ponen una limitación física, pero no lógica, al éxito de este tipo de ataque.

AUDITABILIDAD
Cuando la información relacionada con las acciones y actividades de los usuarios (personas o procesos) se encuentra debidamente registrada y monitoreada. P.e.: Logs de las transacciones que un usuario ha realizado en un sistema determinado

AUDITOR
Son generalmente personas externas a la organización que realizan revisiones a la seguridad implantada y realizan recomendaciones para su mejoramiento. Son personas de apoyo para el administrador de seguridad porque le pueden dar consejos de implantaciones de seguridad, hacerlo caer en la cuenta de falencias de seguridad y apoyarlo en nuevos diseños e implantaciones al respecto

AUDITORÍA
Análisis de las condiciones de una instalación informática por un auditor externo e independiente que realiza un dictamen sobre diferentes aspectos. Conjunto de procedimientos y técnicas para evaluar y controlar, total o parcialmente, un sistema informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente.

AUTORIZACIÓN
Proceso por el que se acredita a un sujeto o entidad, para realizar una acción determinada. Se dice que hay autorización cuando la información es accedida solo por los usuarios que tienen los privilegios necesarios y suficientes para hacerlo. Ejemplo: perfiles de usuario en las aplicaciones.

AUTENTICIDAD
Propiedad fundamental de la información de ser confrontada en cualquier momento de su ciclo de vida contra su origen real (Verdadero/falso). Especialmente importante en sistemas económicos (banca, comercio electrónico, bolsa de valores, apuestas, etc.)

-B

BACKDOOR

Es un software que permite el acceso al sistema de la computadora ignorando los procedimientos normales de autenticación. De acuerdo en como trabajan e infectan a otros equipos, existen dos tipos de puertas traseras

BACKUP
Es una réplica de datos que nos permite recuperar la información en caso de ser necesario. Hacer un backup, consiste en guardar en un medio extraíble (para poder guardarlo en lugar seguro) la información sensible referida a un sistema. Esta se puede realizar tanto en ordenadores personales como en servidores. Este medio puede ser un disco duro externo, un CD-ROM grabable, cintas de datos (DAT), discos ZIP o JAZ o magneto-ópticos ó cualquier otro dispositivo de almacenamiento.

BASE DE DATOS
Es un conjunto de datos estructurados que pertenecen al mismo contexto almacenados sistemáticamente para su posterior uso.

BIOMETRÍA
Ciencia que estudia las características biológicas del ser humano (el iris, la huella dactilar, la voz, etc...) para su aplicación a la seguridad informática como medio de identificación del usuario.

BIOMÉTRICOS
Son elementos electrónicos que mediante la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, pueden “verificar” identidades o “identificar” individuos

BIT
El bit es la unidad mínima de información empleada en informática, en cualquier dispositivo digital, o en la teoría de la información. Con él, podemos representar dos valores cualesquiera, como verdadero o falso, abierto o cerrado. Basta con asignar uno de esos valores al estado de "apagado" (0), y el otro al estado de "encendido" (1).

BOMBA DE E-MAIL -MAILBOMB
Son mensajes de correo electrónico excesivamente largos enviados a la cuenta de correo de un usuario con el propósito de provocar la caída del sistema o evitar que los mensajes verdaderos sean recibidos.

BOMBA DE TIEMPO - TIME BOMB
Programa que se activa en una determinada fecha.

BOMBA LÓGICA - LOGIC BOMB
Programa que se ejecuta cuando existen condiciones especificas para su activación. Este tipo de programas los suelen utilizar muchos virus como mecanismo de activación.

BRIDGE - PUENTE

Elemento que posibilita la conexión entre redes físicas, cableadas o inalámbricas, de igual o distinto estándar

BUFFER OVERFLOW
Error generado cuando un programa (generalmente un servidor o "demonio") recibe una entrada mayor a la que espera, sobrescribiendo áreas críticas de memoria.

BUG
Un error en un programa o en un equipo. Se habla de bug si es un error de diseño, no cuando la falla es provocada por otro motivo.

BYTE
Combinación de Bits. En la representación más común 8 bits forman un byte. **–**

-C

CABALLO DE TROYA
Programa aparentemente útil el cual contiene código adicional escondido, desarrollado para obtener algún tipo de información o causar algún daño. Véase también Troyano

CABLEADO ELÉCTRICO
Circuito eléctrico o electrónico que exige el montaje de distintos módulos unidos (cableados) entre sí, para realizar un determinado proceso o secuencia lógica, que por lo general servirá para controlar un sistema de potencia

CADENA DE CUSTODIA
Seguimiento que se debe dar a la evidencia con el objeto que no sea alterada, cambiada o perdida. La cadena de custodia debe mantenerse en un lugar seguro donde sólo tenga acceso personal autorizado.

CERTIFICADO DIGITAL
Es la certificación electrónica que emiten las Autoridades Certificadoras donde constan unos datos de verificación de firma a un signatario y confirma su identidad. Entre los datos figuran la fecha de emisión y la fecha de caducidad, la clave pública y la firma digital del emisor. Los Certificados Digitales siguen las estipulaciones del estándar X.509. Este documento sirve para vincular una clave pública a una entidad o persona

CLIENTE
Es toda persona natural o jurídica con la cual la entidad establece y mantiene una relación contractual o legal para el suministro de cualquier producto o servicio propio de su actividad.

CLAVE
Palabra o frase que permite acceder a un sistema, encriptar un dato, determinar privilegios de usuarios, etc. *Véase Contraseña - Password.*

CÓDIGO FUENTE
Un programa escrito en un formato entendible por el hombre pero no por la computadora. Necesita ser "traducido" (Compilar) a código máquina para ser interpretado por esta última.

CÓDIGO MALICIOSO / VIRUS
Se define como todo programa o fragmento del mismo que genera algún tipo de problema en el sistema en el cual se ejecuta, interfiriendo de esta forma con el normal funcionamiento del mismo. Existen diferentes tipos de código malicioso; a continuación mencionamos algunos de ellos bombas lógicas, troyanos, gusanos, Keyloggers, Cookies, Spyware

COMPILADOR
Programa que toma el Código Fuente de un programa y lo convierte a un ejecutable.

COMPUTACIÓN MÓVIL
Se puede definir la Computación Móvil como la serie de artefactos y equipos portátiles, hardware, que hacen uso de la computación para lograr su funcionamiento, así, se tiene a las computadoras portátiles, los teléfonos celulares, los cuadernos de notas computarizados, las calculadoras de bolsillo, etc.

CONFIDENCIAL
Tipo de clasificación de la información que por su contenido solo interesa a quienes va dirigida y cuya divulgación no autorizada puede ocasionar perjuicios a determinada entidad, agrupación o persona.

CONFIDENCIALIDAD
Requisito de seguridad que indica que el acceso a los recursos de sistema debe estar limitado exclusivamente a los usuarios con acceso autorizado.

CONTINGENCIA
Es la posibilidad de algo suceda. Lo que puede o no suceder. Las contingencias de orden natural o humano, deben ser previstas mediante un plan que describa la aplicación de medidas técnicas, humanas y organizativas que garanticen la continuidad del Acueducto.

CONTRASEÑA - PASSWORD
Conjunto de caracteres alfanuméricos y símbolos que forman una serie secreta de que permite a un usuario tener acceso a un archivo, a un ordenador, o a un programa. En sistemas multiusos, cada usuario debe incorporar su contraseña antes de que el ordenador responda a los comandos. Las contraseñas ayudan a asegurar que los usuarios desautorizados no tengan acceso al ordenador. Además, los ficheros de datos y los programas pueden también requerir contraseñas.

CONTROL DE ACCESOS - ACCESS CONTROL
Se utiliza para restringir el acceso a determinadas áreas del PC, de la red, mainframes, Internet, ftp, web, etc... El permiso o la denegación de acceso puede realizarse en función de la dirección IP, el nombre de dominio, nombre de usuario y password, certificados

CONTROL REMOTO DE EQUIPOS
Un atacante puede tomar el control de un equipo en forma remota y no autorizada, mediante la utilización de programas desarrollados para tal fin, e instalados por el atacante mediante, por ejemplo la utilización de troyanos

COOKIE
Fragmento de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página. Esta información puede ser luego recuperada por el servidor en posteriores visitas

COPIAS DE BACKUP
Copia de respaldo de información

CORREO ELECTRÓNICO (E-MAIL)
Aplicación que permite enviar mensajes a otros usuarios de la red sobre la que esté instalado. También denominado E-Mail.

CORTAFUEGOS - *Véase Firewall.*

CRACKER
El término cracker (del inglés crack, romper) tiene varias acepciones. Un cracker es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo.

CRIPTOGRAFÍA
Ciencia que consiste en transformar un mensaje inteligible en otro que no lo es, mediante la utilización de claves, que solo el emisor y receptor conocen.

CRITERIOS DE SEGURIDAD DE LA INFORMACIÓN

- **Confidencialidad**: Hace referencia a la protección de información cuya divulgación no está autorizada.
- **Integridad:** La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.
- **Disponibilidad:** La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

CSIRT
Un Equipo de Respuesta a Incidentes de Seguridad (CSIRT) es una organización que es responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad. Sus servicios son generalmente prestados para un área de cobertura definida que podría ser una entidad relacionada u organización de la cual dependen, una corporación, una organización de gobierno o educativa; una región o país, una red de investigación; o un servicio pago para un cliente. Un CSIRT puede ser un equipo formalizado o un equipo ad hoc. Un equipo formalizado realiza un trabajo de respuesta a incidentes como su función

principal. A un equipo ad hoc se convoca durante un incidente de seguridad que esté ocurriendo en ese momento o para responder a un incidente cuando surge la necesidad.

CUSTODIO DE LA INFORMACIÓN
Funcionarios de Acueducto que mantienen o administran los recursos de información en nombre de los dueños de la información.

-D

DEFACE
Modificación de un portal o Web sin autorización del administrador

DELITO INFORMÁTICO
El delito informático implica cualquier actividad ilegal que encuadra en figuras tradicionales ya conocidas como hurto, fraude, falsificación, perjuicio, estafa y sabotaje, suplantación, pero siempre que involucre la informática de por medio para cometer la ilegalidad. En Colombia existe la ley 1273 del 2009.

NEGACIÓN DE SERVICIO (DoS) – Denial of Service
Ataque a la disponibilidad cuyo objetivo es degradar considerablemente o detener el funcionamiento de un servicio ofrecido por un sistema o dispositivo de red. Existen diferentes técnicas para la explotación de este tipo de ataques.

DES
Algoritmo que codifica los textos haciendo bloques de datos de 64 bits y utilizando una clave de 56 bits. Existe otra modalidad más avanzada denominada 3DES que utiliza el algoritmo DES tres veces. Hay varios tipos de algoritmo 3DES en función del número de claves que utilicen y de la longitud de éstas.

DETECCIÓN DE INTRUSOS (IDS)
Sistema que agrupa un conjunto de técnicas cuyo propósito es detectar las intrusiones en una computadora o un sistema.

DETECCIÓN DE INTRUSIONES
Proceso de monitorizar los eventos de un sistema o red en busca de signos que indiquen problemas de seguridad.

DETECCIÓN DE USOS INDEBIDOS
Detección basada en la actividad de sistema que coincide con la definida como mala.

***DHCP* - Dynamic Host Configuration Protocol)**
Es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a

los clientes conforme estas van estando libres, sabiendo en todo momento quien ha estado en posesión de esa IP, cuánto tiempo la ha tenido, a quien se la ha asignado después

DISCLAIMERS
Declaración que propende por conservar la confidencialidad y la privacidad de la información.

DISPOSITIVO
Mecanismo, máquina o aparato dispuesto para producir una función determinada.

DISPOSITIVOS DE ALMACENAMIENTO REMOVIBLES
Medios para almacenamiento de información dentro de los cuales se encuentran: memoria flash (USB, SD, MiniSD), cámaras digitales, reproductores de MP3/MP4, discos duros removibles, agendas digitales personales (PDA), teléfonos celulares, disquetes, discos ópticos (ZIP- DRIVE, CD y DVD), cintas para realizar respaldo, entre otros.

DISPONIBILIDAD
Requisito de seguridad que implica que la información y los servicios del sistema continúen en funcionamiento y que los usuarios autorizados puedan acceder a los recursos cuando lo necesiten, dónde lo necesiten, y en la forma en que lo necesiten.

DISPOSITIVO MÓVIL (DM) - MOBILE DEVICE
Dispositivo electrónico cuya función es la de recibir/enviar información desde la estación en que esté instalado (portátiles, PDAs, móviles, cámaras, impresoras,.). Este dispositivo puede ser una tarjeta PCMCIA, USB, PCI -Slot de un PC de sobremesa-, ó Centrino, que sustituyen a las tarjetas de red.

DUEÑO DE LA INFORMACIÓN
Funcionarios del Acueducto responsable de definir la clasificación, determinar los niveles de acceso, autorizar la asignación de permisos de acceso y aplicar los controles necesarios para el almacenamiento, procesamiento, distribución y uso de la información.

- E

ENCRIPCIÓN ASIMÉTRICA
Método criptográfico que usa **un par** de claves para el envío de mensajes

ENCRIPCIÓN SIMÉTRICA
Método criptográfico que usa **una** misma clave para cifrar y para descifrar mensajes

ESTÁNDAR
Conjunto de requisitos de obligatorio cumplimiento, que especifican tecnologías y métodos, para implementar las políticas de seguridad de la información expuestas por la alta gerencia,

establecen un marco de acción coordinado que busca alinear los esfuerzos de la organización para procurar los fundamentos de la seguridad informática.

ETHERNET
Arquitectura de red de área local desarrollada en 1976 por Xerox Corp. en cooperación con DEC e Intel. Emplea una topología lineal (bus) o de estrella, o lo que es lo mismo, los datos pasan en todo momento por todos los puntos de conexión (a 10 Mbps) utilizando el método de acceso por detección de portadora con detección de colisiones (CSMA/CD). Una nueva versión denominada 100Base-T (o Fast Ethernet) soporta velocidades de 100 Mbps. Y la más reciente, Gigabit Ethernet soporta 1 Gb por segundo.

EVALUACIÓN DE RIESGOS INFORMATICOS
Análisis y valoración de las amenazas y vulnerabilidades que son relativos a la información y a las instalaciones de procesamiento de la misma, frente a la probabilidad de ocurrencia y el impacto que puedan causar.

EVENTO ADVERSO
Es la consecuencia negativa que compromete la confidencialidad, integridad o disponibilidad de los activos.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN
Una situación que indica un posible incumplimiento de la política de seguridad de la información, una falla en los controles, o una situación previamente desconocida que puede ser pertinente para la seguridad de la información.

- F

FALLO - BUG
O error en un programa. Cuando uno de ellos tiene errores, se dice que tiene Bugs. Como los virus son programas, también pueden contener bugs. Esto implicaría que, si el virus debe realizar determinadas acciones, podría no realizarlas, o no hacerlo bajo las condiciones que su programador ha establecido inicialmente.

FALSO NEGATIVO-FALSE NEGATIVE
Evento que se da como inexistente cuando realmente si existe, por ejemplo, decir que un sistema está limpio de virus cuando realmente está infectado.

FALSO POSITIVO - FALSE POSITIVE
Evento que se da como existente cuando realmente no existe, por ejemplo, decir que un sistema está infectado de virus cuando realmente está limpio.

FIREWALL
Barrera de protección. Es un procedimiento de seguridad que coloca un sistema de computación programado especialmente entre una red segura y una red insegura. Un sistema o combinación de sistemas que fija los límites entre dos o más redes y restringe la entrada y salida de la información.

FORENSE
Personas experta que se encargan de realizar análisis de siniestros de seguridad ocurridos dentro de la organización para determinar lo que paso y quién lo hizo, y si es el caso, aportar en procesos penales contra los atacantes

FRAUDE INFORMÁTICO
Se trata del perjuicio económico efectuado a una persona mediante la utilización de un sistema informático, ya sea, modificando datos, introduciendo datos falsos o verdaderos o cualquier elemento extraño que sortee la seguridad del sistema.

- G

GATEWAY
Dispositivo de enrutamiento. En la actualidad, se utiliza el término Router para describir los nodos que realizan esta función, mientras que Gateway se refiere a un dispositivo para fines especiales que convierte información de la capa de aplicación de un stack de protocolo a otro

GESTIÓN DE SEGURIDAD
Proceso de establecer y mantener la seguridad en un sistema o red de sistemas informáticos. Las etapas de este proceso incluyen la prevención de problemas de seguridad, detección de intrusiones, investigación de intrusiones, y resolución. 2. En gestión de redes, controlar (permitir, limitar, restringir, o denegar) acceso a la red y recursos, buscar intrusiones, identificar puntos de entrada de intrusiones, y reparar o cerrar estas posibles vías de acceso.

GESTIÓN DEL RIESGO
Proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los sistemas de información**.**

GUSANO
Es un virus o programa auto replicante que no altera los archivos sino que reside en la memoria y se duplica a sí mismo

- H

HACKING
Técnicas y procedimientos utilizados por un hacker para cumplir un determinado objetivo, generalmente estos procedimientos son ilegales o malignos y están orientados a obtener información confidencial y sensible de los sistemas de información de las entidades.

HACKER
Son personas expertas en sistemas que saben de seguridad y buscan tener acceso a recursos informáticos generalmente con el fin de demostrarse a si mismo y a otros que lo pudieron hacer y conseguir prestigio como expertos en seguridad

HARDWARE
Se denomina hardware o soporte físico al conjunto de elementos materiales que componen un computador. Hardware también son los componentes físicos de una computadora tales como el disco duro, CD-Rom, disquetera (floppy), etc.. En dicho conjunto se incluyen los dispositivos electrónicos y electromecánicos, circuitos, cables, tarjetas, armarios o cajas, periféricos de todo tipo y otros elementos físicos.

HOSTING Servicio por el cual un proveedor proporciona el/los servidores para alojar y publicar un sitio Web. En este caso todo el equipamiento pertenece al proveedor.

HONEYPOT
(tarros de miel en castellano). Un servidor diseñado para ser atacado y que actúa como señuelo para hackers los cuales piensan que se conectan a un verdadero sistema informático y actúan sobre él, permitiendo así a su propietario monitorizar la actividad del "pirata" con distintos fines: estudiar su comportamiento, fijar los puntos débiles de su red, etc.

HOST
Sistema Central. Computadora que permite a los usuarios comunicarse con otros sistemas de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el Correo Electrónico, Telnet y FTP.

HTML - Hypertext Markup Language -
lenguaje de marcas hipertextuales. Lenguaje de marcación diseñado para estructurar textos y presentarlos en forma de hipertexto, que es el formato estándar de las páginas web, formato especial de archivos sobre el que está basada la estructura de la aplicación WWW (World Wide Web).

HTTP - Hypertext Transfer Protocol
El protocolo de transferencia de hipertexto es el protocolo usado en cada transacción de la Web (WWW). El hipertexto es el contenido de las páginas web, y el protocolo de transferencia es el sistema mediante el cual se envían las peticiones de acceder a una página web, y la respuesta de esa web, remitiendo la información que se verá en pantalla. También sirve el protocolo para enviar información adicional en ambos sentidos, como formularios con mensajes y otros similares.

- I

ID
Conjunto de caracteres alfanuméricos que sirven para Identificar a un usuario para su acceso a la red o un sistema de información. Ej: rfgarcia.

IDS

Intrusión Detection System, es un programa usado para detectar accesos desautorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

INCIDENTE INFORMÁTICO
Cualquier acción, evento adverso o intento de ocurrencia de estos en un sistema o red informática que ponga en riesgo la confidencialidad, integridad y disponibilidad de la información

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN
Evento o serie de eventos adversos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

INFECCIÓN
Acción que realiza un virus al introducirse en un sistema, empleando cualquier método, para poder ejecutar sus acciones dañinas y su carga destructiva, o bien simplemente al haber conseguido acceder al mismo

INGENIERÍA SOCIAL
Habilidad que tiene una persona para engañar a otra con el fin de obtener información confidencial, mediante la conversación o llamada telefónica; se enfoca en el eslabón más débil de la cadena… El Recurso Humano. Se diferencia del resto de las amenazas básicamente porque no se aprovecha de debilidades y vulnerabilidades propias de un componente informático para la obtención de información.

INSTRUCTIVOS
Define un conjunto de pasos operacionales específicos sugeridos para efectuar una labor particular, que se puede modificar en respuesta a los cambios en la dinámica del negocio y la tecnología

INTEGRIDAD
Requisito de seguridad que indica que la información deberá ser protegida ante alteraciones no autorizadas.

INTRUSIÓN
Violación intencionada de las políticas de seguridad de un sistema.

INTEGRIDAD DE ARCHIVOS
Técnicas utilizadas para conseguir archivos de backup correctos de modo que se pueda recurrir a ellos en caso de tener que recuperar datos críticos después de que los datos originales se contaminen debido a una acción accidental o provocada (por ejemplo, un virus).

INTERNET

Sistema de redes de computación ligadas entre si, con alcance mundial, que facilita servicios de comunicación de datos como registro remoto, transferencia de archivos, correo electrónico y grupos de noticias.

INTRANET
Red de ordenadores de una red de área local (LAN) privada empresarial o educativa que proporciona herramientas de Internet, las cuales tienen como función principal proveer lógica de negocios para aplicaciones de captura, reportes, consultas, etc

INTRUSO
Aquella persona que con una variedad de acciones intenta comprometer un recurso de hardware o software.

IP – Internet Protocol
Protocolo de internet. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de internet. El IP es la dirección numérica de una computadora en internet, de forma que cada dirección electrónica se asigna a una computadora conectada a internet y por lo tanto es única. La dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI.y está compuesta de cuatro octetos, como por ejemplo : 132.248.53.10 .

ISO
Organización Internacional para la Estandarización

ISO 17999/27001
Estándar para la gestión de la seguridad de la información

ISP (Internet Service Provider)
Compañía o individuo dedicado a vender acceso (servicio) a Internet.

- J

JAVA
Lenguaje de programación desarrollado por SUN microsystems para la elaboración de pequeñas aplicaciones exportables a la red (Applets) y capaces de operar sobre cualquier plataforma a través, normalmente, de navegadores.

- K

KEYLOGGERS
Es una aplicación destinada a registrar todas las teclas que un usuario tipea en su computador; algunos de ellos además registran otro tipo de información útil para un atacante, como ser, imágenes de pantalla

-L

LDAP - Protocolo de Acceso Ligero a Directorio
Protocolo para el acceso a a directorios jerárquicos de información. Basado en el estándar X.500, pero significativamente más simple por lo que también se le denomina x.500-lite, se diferencia de éste porque soporta TCP/IP, necesario para cualquier tipo de acceso a Internet. Aunque no está ampliamente extendido, debería poderse implementar en la práctica mayoría de aplicaciones que se ejecutan virtualmente sobre plataformas informáticas para obtener información de directorios tales como direcciones de correo y llaves públicas. Ya que es un protocolo abierto, no afecta el tipo de servidor en el que se aloje el directorio.

LAMMER
Principiante ó aprendiz de hacker. Esta es una nueva categoría, se trata de personas que no saben mucho de los sistemas de seguridad y se dedican a utilizar herramientas o aplicaciones desarrolladas por otros (*hackers* o *crackers*) para hacer daño a las organizaciones. Los *lamers* no saben de la técnica que hay detrás de un ataque o un mecanismo de violación de un sistema, solo siguen instrucciones respecto al uso de algunas herramientas y realizan fechorías con esto. Este tipo de atacantes puede hacerlo por el simple placer de hacerlo o con ánimo de obtener alguna retribución por sus acciones.

LAN (Local Area Network)
Red de área local. Red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LANs conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un único edificio u otra área geográficamente limitada. Véase también MAN y WAN.

LOG
Conjunto de archivos que contienen registros detallando todos los eventos relacionados con la seguridad de los recursos informáticos

LOGIN
Nombre de acceso de un usuario a una red o sistema multiusuario. Este término se le puede aplicar tanto al nombre de su cuenta como al hecho de ingresar a un sistema de este tipo. El usuario debe usar el nombre, así como su contraseña (password), para tener acceso al sistema.

- LL

LLAVES PÚBLICAS
Parte pública para criptografía que se entrega a quién se desea hacer un intercambio de información seguro

LLAVES PRIVADAS
Parte privada para criptografía que se **no se** entrega para hacer intercambio de información seguro y se utiliza para desencriptar la información encriptada con la llave publica

- M

MALWARE
Este programa o archivo, que es dañino para el ordenador, está diseñado para insertar virus, gusanos, troyanos, spyware o incluso los bots, intentando conseguir algún objetivo, como podría ser el de recoger información sobre el usuario o sobre el ordenador en sí.

MAN(Metropolitan Area Network)
Red de área metropolitana. En general, una MAN abarca un área geográfica más vasta que una LAN, pero cubre un área geográfica más pequeña que una WAN

MAN-IN-THE-MIDDLE
Modalidad de ataque en que el atacante se interpone entre el origen y el destino en una comunicación pudiendo conocer y/o modificar el contenido de los paquetes de información, sin esto ser advertido por las víctimas. Esto puede ocurrir en diversos ambientes, como por ejemplo, en comunicaciones por e-mail, navegación en Internet, dentro de una red LAN, etc.

MAPA DE RIESGO
Metodología para determinar el nivel de riesgo al que está expuesto el Acueducto y sus Unidades de Negocio. Sirve como soporte a la elaboración de un plan de acción de orden preventivo, activo y correctivo, que permite la reducción del riesgo.

MEDIO MAGNÉTICO
Dispositivo para almacenamiento de información dentro de los cuales se encuentran: memoria flash (USB, SD, MiniSD), discos duros, disquetes, discos ópticos (ZIP- DRIVE, CD y DVD), cintas de backup y otros dispositivos.

MBPS (MEGABITS POR SEGUNDO)
Unidad de medida de la capacidad de transmisión por una línea de telecomunicación. Cada megabit está formado por 1.048.576 bits

MP3
Es un formato de audio digital comprimido con pérdida desarrollado por el Moving Picture Experts Group (MPEG) para formar parte de la versión 1 (y posteriormente ampliado en la versión 2) del formato de video MPEG. Su nombre es el acrónimo de MPEG-1 Audio Layer 3. MPEG-1 Audio Layer 3, más conocido como MP3, conocido también por su grafía emepetrés,

MULTICAST (Multidifusión)
Modo de difusión de información, que permite que ésta pueda ser recibida por múltiples nodos de la red y por lo tanto por múltiples usuarios.

- N

NEGACIÓN DE SERVICIO - Ver DoS.

NO REPUDIO
Característica de los sistemas de autenticación fuertes. Se da cuando la información involucrada en un evento corresponde a quien participa, quien no podrá evadir su intervención en éste. Ejemplo: Un emisor de un mensaje no puede negar que lo generó y viceversa, un receptor de un mensaje no puede negar que lo recibió.

NODO
Cualquier computadora o periférico conectado directamente a una red

NORMA
Es una declaración organizacional que limita las responsabilidades entre diferentes áreas, estableciendo pautas de acción según lo que le correspondan en ámbito de sus funciones

- O

OSGSI
Oficial del Sistema de Gestión de Seguridad Informática

ONLINE
En general, se dice que algo está en línea, on-line u online si está conectado a una red o sistema mayor (que es, implícitamente, la línea).

***OSI (*Open System Interconection)**
Lanzado en 1984 fue el modelo de red descriptivo creado por ISO. Proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial.

OSI -Oficial de Seguridad de la Información
Persona que tiene la función de brindar los servicios de seguridad en la organización, a través de la planeación, coordinación y administración de los procesos de seguridad informática, así como difundir la cultura de seguridad informática entre todos los miembros de la organización.

- P

PASSWORD - *Véase Contraseña.*

PATCH (Parche)
Modificación de un programa ejecutable para solucionar un problema, corregir un Bug o para cambiar su comportamiento.

PAZ Y SALVO DE DATOS
Para la devolución de la custodia de la información y recursos informáticos a cargo de un usuario de la información será necesaria la suscripción del Acta de Paz y Salvo de Datos y el Acta de Paz y Salvo de Recursos Informáticos, establecidas a partir de la asignación de un activo de información o recurso informático.

PERFIL DE USUARIO
Información a la que el usuario necesita acceder para el desarrollo de sus tareas, criticidad de la información, funciones del puesto, etc.

PETI
La Planeación Estratégica de Tecnología de Información (PETI), establece las políticas requeridas para controlar la adquisición, uso y la administración de los recursos TI. Integra la perspectiva de negocios/organizacional con el enfoque de TI, estableciendo un desarrollo informático que responde a las necesidades de la organización y contribuye al éxito de la empresa.

PLAN DE CONTINGENCIA
Definición de acciones a realizar, recursos a utilizar y personal a emplear en caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos de una organización.

PHISHING
Ataque a la seguridad que consiste en el envío masivo de mensajes electrónicos que fingen ser notificaciones oficiales de entidades/empresas legítimas con el fin de obtener datos personales y bancarios de los usuarios.

PIN
Personal Identification Number. Número de Identificación Personal

PORTAL
Sitio web cuyo objetivo es ofrecer al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios, entre los que suelen encontrarse buscadores, foros, compra electrónica, etc.

POLÍTICAS DE SEGURIDAD INFORMÁTICA
Son directrices de nivel del Acueducto en la cual se expresan valores y objetivos de la Institución para proporcionar dirección y soporte a los temas relacionados con seguridad de la información, la política de seguridad en el acueducto fue aprobado por la resolución 1127 de Diciembre 23 de 2009.

PROCEDIMIENTO Ó INSTRUCTIVO
Define un conjunto de pasos operacionales específicos sugeridos para efectuar una labor particular, que se puede modificar en respuesta a los cambios en la dinámica del negocio y la tecnología. P.e Procedimiento para toma de respaldos.

PROTOCOLO
Conjunto de normas (lenguaje de reglas y símbolos) que rige cada tipo de comunicación entre dos computadoras (intercambio de información).

PROXY
Software que permite a varios ordenadores acceder a Internet a través de una única conexión física y puede permitir acceder a páginas WEB, FTP, correo electrónico, etc; y también servidor de comunicaciones responsable de canalizar el tráfico entre una red privada e Internet, que contiene un cortafuegos.

PUERTO
Punto de acceso a un ordenador ó medio a través del cual tienen lugar las transferencia de información – entradas / salidas - Todas las conexiones y diálogos TCP/IP se llevan a cabo sobre estos, y cada protocolo para su uso tiene definido un puerto estándar. En Internet, el término *puerto* se refiere a un número que se muestra en una URL, después de una coma justo después del Nombre de Dominio. Cada servicio en un servidor de Internet *escucha* en un número de puerto particular. La mayoría de estos servicios tienen números de puerto estándares. Los servidores web *escuchan* normalmente en el puerto 80.

PKI
Infraestructura de Clave Pública. Procedimiento criptográfico que utiliza dos claves, una pública y otra privada; la primera para cifrar y la segunda para descifrar. Se utiliza en Internet, que es una red pública no segura, para proteger aquellas comunicaciones cuya confidencialidad se desea garantizar (ejemplo transacciones comerciales o bancarias).

- R

RED
Conjunto de computadoras, impresoras, Routers, Switches, y otros dispositivos, que pueden comunicarse entre sí por algún medio de transmisión.

REDIRECCIONAR
Acceder a una determinada dirección mediante otra. Cambiar el destino de algo. Por ejemplo, redirigir una llamada es hacer que suene en un teléfono distinto del que se intentaba llamar.

REDUNDANCIA
Consiste en intensificar y repetir la información o el servicio con el fin de tener una fuente alternativa en caso de daño del sistema principal.

REGISTROS (LOGS)
Registro oficial de eventos durante un periodo de tiempo en particular

RIESGO

Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio (pérdida continuidad, imagen, incumplimiento, pérdida de ingresos, entre otros.).

ROOTKIT
Herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios de administrador del equipo. Esta disponible para una amplia gama de sistemas operativos. Estos programas son insertados en una computadora después de que algún atacante ha ganado el control de un sistema

ROUTER
Dispositivo que transmite paquetes de datos a lo largo de una red. Un router está conectado al menos a dos redes, generalmente dos LANs o WANs o una LAN y la red de un ISP. Los routers emplean cabeceras y tablas de comparación para determinar el mejor camino para enviar los paquetes a su destino, y emplean protocolos como el ICMP para comunicarse con otros y configurar la mejor ruta entre varios host

-S

SAP
Servicio informático del Acueducto destinado a apoyar los procesos de negocio de la Empresa

SEGURIDAD DE LA INFORMACION
Adoptar mejores prácticas que permitan reducir los riesgos a los que se expone nuestra información.
El propósito de la seguridad de la información es proteger la información de una amplia gama de amenazas para garantizar la continuidad del negocio, minimizar las pérdidas por daños y maximizar las oportunidades de negocios. Principalmente se ocupa de garantizar la confidencialidad, integridad y disponibilidad de la información frente a las amenazas y riesgos que afectan los sistemas de información.

SEGURIDAD INFORMÁTICA
Área de la Informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

SEGURIDAD PERIMETRAL
Medidas de control enfocadas a proteger el acceso físicos o lógicos a los activos y su objetivo es detectar y reportar cualquier intrusión o violación.

SERVER (Servidor)

Máquina que ofrece servicios a otras dentro de una red. También llamado Host.

SIE
El Sistema de Información Empresarial, hace parte de la Gerencia de Tecnología, y se creó con el fin de sistematizar la información de la empresa y facilitar los procesos dentro de la misma.

SIMI
Formulario de informática que permite la creación, modificación y eliminación de usuarios. Este formulario ofrece el registro de solicitudes de autorización, control de acceso a los servicios informáticos y el procesamiento de solicitudes a los sistemas de información de Acueducto.

SISTEMA DE GESTIÓN DE LA INFORMACIÓN - SGSI
Sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información.

SISTEMA OPERATIVO
Operating System (OS) en inglés. Programa especial el cual se carga en una computadora al prenderla, y cuya función es gestionar los demás programas, o aplicaciones, que se ejecutarán, como por ejemplo, un procesador de palabras o una hoja de cálculo, un juego o una conexión a Internet. Windows, Linux, Unix, MacOS son todos sistemas operativos.

SOFTWARE
Se denomina software (también programática, equipamiento lógico o soporte lógico) a todos los componentes intangibles de un ordenador o computadora, es decir, al conjunto de programas y procedimientos necesarios para hacer posible la realización de una tarea específica, en contraposición a los componentes físicos del sistema (hardware).

SPAM
Son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas.

SPYWARE
Aplicaciones que recogen y envían información sobre las páginas web que más frecuentemente visita un usuario, tiempo de conexión, datos relativos al equipo en el que se encuentran instalados (sistema operativo, tipo de procesador, memoria, etc.) e, incluso, hay algunos diseñados para informar de si el software que utiliza el equipo es original o no.

-T

TCP/IP
Es un conjunto de protocolos de red que implementa la pila de protocolos en la que se basa Internet y que permiten la transmisión de datos entre redes de computadoras

TELNET
Es el nombre de un protocolo (y del programa informático que implementa el cliente) que sirve para acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella

TERCERO
Persona natural o jurídica que le presta un servicio a el Acueducto, tales como contratista, proveedor, entre otros.

TRABAJO REMOTO (Teletrabajo)
Toda forma de trabajo que no requiera la presencia de la persona en la oficina o planta de la empresa. Para su realización deben actuar elementos telemáticos, ya sea computadoras, teléfonos o cualquier otra tecnología de la información y la Comunicación

TROYANO
Es una pieza de software dañino disfrazado de software legítimo. Los caballos de troya no son capaces de replicarse por sí mismos y pueden ser adjuntados con cualquier tipo de software por un programador o puede contaminar a los equipos por medio del engaño.

-U

***URL* - Uniform Resource Locator-**
El URL es un localizador uniforme de recurso. Es la cadena de caracteres con la cual se asigna dirección única a cada uno de los recursos de información disponibles en Internet. Existe un URL único para cada página de cada uno de los documentos de la World Wide Web.
El URL de un recurso de información es su dirección en Internet, la que permite que el navegador la encuentre y la muestre de forma adecuada. Por ello el URL combina el nombre del ordenador que proporciona la información, el directorio donde se encuentra, el nombre del fichero y el protocolo a usar para recuperar los datos. Y reemplaza la dirección numérica o IP de los servidores. Haciendo de esta manera más fácil la navegación, si no de otra forma se tendría que hacer bajo direcciones del tipo http://148.210.01.7 en vez de http://www.pagina.com

USERNAME (nombre de usuario):
Nombre único que identifica a un usuario, y es utilizado como medio de identificación ante un Sistema

USUARIO
Aquella persona natural o jurídica a la que, sin ser cliente, la entidad le presta un servicio**.**

-V

VIRUS
Es un programa que se copia automáticamente y que tiene por objeto alterar el funcionamiento de la computadora, sin el permiso o el conocimiento del usuario

VULNERABILIDAD
Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos de una entidad.

-W

WAN *-Wide Area Network-*
Red de area extensa. Red de comunicación de datos que sirve a usuarios ubicados a través de una amplia zona geográfica y a menudo utiliza dispositivos de transmisión suministrados por portadoras comunes. Véase también LAN y MAN.

WAP
Wireless Application Protocol o WAP (protocolo de aplicaciones inalámbricas) es un estándar abierto internacional para aplicaciones que utilizan las comunicaciones inalámbricas, p.ej. acceso a servicios de Internet desde un teléfono móvil.

WEP - Wired Equivalent Privacy
Protocolo para la transmisión de datos "segura". La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de encriptación. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits!, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red.

Wi-Fi - Tecnología utilizada en Redes Inalámbricas
Abreviatura de Wireless Fidelity. Es el nombre “comercial” con que se conoce a todos los dispositivos que funcionan sobre la base del estándar 802.11 de transmisión inalámbrica. En lenguaje popular: Redes wifi.

WIMAX
Técnica de modulación FDM (empleada por el 802.11a y el 802.11g) para transmitir grandes cantidades de datos digitales a través de ondas de radio. OFDM divide la señal de radio en múltiples subseñales más pequeñas que luego serán transmitidas de manera simultánea en diferentes frecuencias al receptor. OFDM reduce la cantidad de ruido (crosstalk) en las transmisiones de señal

-X

XML
Es un metalenguaje extensible de etiquetas desarrollado por el World Wide Web Consortium (W3C). Es una simplificación y adaptación del SGML y permite definir la gramática de

lenguajes específicos (de la misma manera que HTML es a su vez un lenguaje definido por SGML).

-Z

ZONA DESMILITARIZADA, RED PERIMÉTRICA (DMZ):
Máquina o pequeña subred situada entre una red interna de confianza (como una red local privada) y una red externa no confiable (como Internet). Normalmente en esta zona se sitúan los dispositivos accesibles desde Internet, como servidores Web, FTP, SMTP o DNS, evitando la necesidad de acceso desde el exterior a la red privada. Este término es de origen militar, y se utiliza para definir un área situada entre dos enemigos.

ZOMBIE
Ordenador o servidor Web no seguro utilizado de forma ilegítima para enviar spam o lanzar un ataque de denegación de servicio. Los equipos zombie son primero infectados o atacado por un hacker y después usados a voluntad del hacker. Los usuarios de éste equipo usualmente no se percatan que su computadora es usada para fines ilegales.