# GLOSARIO DE TÉRMINOS

**Amenaza**.- Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

**BASH**.- (*Bourne Again Shell*) Intérprete de órdenes de la mayoría de los sistemas operativos GNU/LINUX, desarrollado a partir de Bourne Shell. También proporciona los mecanismos que le permiten considerarse un lenguaje de programación.

**Captcha** (*Completely Automated Public Turing test to tell Computers and Humans Apart*) Prueba de desafío-respuesta utilizada en computación para determinar cuándo el usuario es o no humano.

**CC/CERT.-**Coordinación de equipos de respuesta a incidentes de seguridad en cómputo. Fue el primer CERT y fue fundado en la Universidad Carnegie Mellon.

**CERT**.- (*Computer Emergency Response Team*) Equipo de respuesta a incidentes de seguridad en cómputo.

**Confidencialidad**.- Según [ISO/IEC 13335-1:2004]: característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

**Dependencia**.- Cualquier organización que usa direcciones IP que pertenecen al espacio de direccionamiento de RED-UNAM.

**Disponibilidad**.- Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera

**DGSCA.-** *(Dirección General de Servicios de Cómputo Académico)*. Fue el nombre de la DGTIC hasta 2010.

**DGTIC.-** (*Dirección General de Tecnologías de Cómputo y de Tecnologías de Información y Comunicación*). Organización líder en tecnologías en cómputo en la UNAM, primera Institución en México en operar supercomputadoras Cray Y-MP en 1990. También ha sido la institución promotora de importantes proyectos como Internet 2, visualización científica, seguridad en cómputo, supercómputo así como una importante fuente de recursos humanos en diferentes áreas de cómputo.

**Evento**.- Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior desconocida que podría ser relevante para la seguridad.

**FIRST**.- (*Forum of Incident Responders and Security Teams*) Foro de equipos de respuesta a incidentes y equipos de seguridad en cómputo. Organización formada por CC/CERT con el propósito de permitir responder más efectivamente a los incidentes de seguridad en cómputo, así como desarrollar medidas proactivas.

**Hash**.- Una función de hash H es una transformación que toma un valor m como entrada y devuelve una cadena de longitud constante, la cual es llamada el valor de hash o simplemente hash con valor h. Por ende h =H(m).

La función de hash tiene tres requisitos, puede recibir una cadena m de cualquier valor, la salida es de una longitud constante, H(x) es fácil de calcular, es una función unidireccional y está libre de colisiones

**IANA.-** (*Internet Assigned Numbers Authority*) Autoridad de asignación de números de Internet. Es la organización responsable de asignar direcciones de internet, números de sistemas autónomos por medio de sus organismos regionales. También administra los servidores DNS raíz y los sistemas de numeración de protocolos de Internet.

**IETF**.- (*Internet Engineering Task Force*) Fuerza de Trabajo de Ingeniería de Internet es una comunidad abierta e internacional de proveedores, operadores, diseñadores e investigadores de redes de datos involucrados en la arquitectura y operación de Internet. Su misión es producir documentos técnicos y de alta calidad que influyan la manera de diseñar, usar y administrar el Internet.

**Incidente**.- Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

**INETD**.- Actúa como un servidor de gestión de otros servicios. Cuando inetd recibe una conexión se determina qué servicio debería responderla, se lanza un proceso que ejecuta dicho servicio y se le entrega el "socket". La ejecución de una única instancia de inetd reduce la carga del sistema en comparación con lo que significaría ejecutar cada uno de los servicios que gestiona de forma individual.

**Integridad**.- Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO/IEC 13335-1:2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos

**ISO**.- (*International Organization for Standardization*) Organización Internacional para la Estandarización. Ha publicado la mayor cantidad de estándares internacionales y se conforma por miembros de 161 países, uno por país y tiene como sede central Génova, Suiza, desde donde se coordina la organización.

**ISO/IEC 27000**.- Conjunto de estándares desarrollados o en fase de desarrollo por ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*),

que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

**LACNIC.-** Organismo regional de IANA para la región de Latinoamérica y el Caribe.

**NIST**.- (*National Institute for Standards And Technology*) Instituto Nacional de Estados Unidos para Estándares y Tecnología. Fue fundada por el Departamento de Comercio de Estados Unidos en 1901, trabaja en una amplia gama de actividades entre las cuales se encuentran el desarrollo de metodologías, estándares y herramientas de seguridad de la información por medio de la División de seguridad en cómputo (CSD).

**PERL**.- (*Practical Extraction and Report Language*) Lenguaje de programación interpretado desarrollado por en Larry Wall en 1987. Proporciona una gran capacidad de procesamiento de texto.

**Proyecto HONEYNET**.- (*Honeynet Project)* Organización internacional de seguridad dedicada a la investigación de las últimas amenazas de seguridad y desarrollo de herramientas de código abierto para mejorar la seguridad de internet. Está integrada por varios capítulos en todo el mundo que están formados por voluntarios

**RFC**.- *(Request for Comments)* Conjunto de documentos sobre internet desarrollados por la IETF. Cada documento es una propuesta oficial y detallada para un nuevo protocolo de Internet que permiten a los implementadores desarrollarlos sin ambigüedades.

**RSS feed**.- *(Rich Site Summary)* Formato para proveer información en forma resumida de sitios web que cambian constantemente.

**SAI**.- *(Sistema de Atención a Incidentes)* Sistema que gestiona los incidentes atendidos por UNAM-CERT y permite la administración de la información de contacto de los administradores de RED-UNAM.

**Seguridad de la información**.- Según [ISO/IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

**SSI/UNAM**.-Subdirección de Seguridad de la Información de la DGTIC.

**US-CERT.-** Equipo de respuesta a incidentes del Gobierno de Estados Unidos. Fue uno de los primeros CERTs en ser acreditados y ha tenido influencia en otros CERTs alrededor del mundo.