Capítulo 1. Conceptos básicos de la seguridad informática

"Las ideas fundamentales la ciencia son esencialmente sencillas y, por regla general pueden ser expresadas en un lenguaje comprensible para todos."

Albert Einstein.

En este Capítulo se presentan los conceptos básicos de la seguridad informática, la situación actual de la UDLA y el objetivo que se pretende alcanzar con este trabajo.

1.1 Gestión de seguridad y gestión de red

La gestión se define como el conjunto de actividades que controlan o vigilan el uso de los recursos[AMS88][STA94]. Debe proporcionar la posibilidad de supervisar el estado, medir el rendimiento, reconocer actividades anormales y recuperar el servicio. Las funciones de red se suelen agrupar en dos categorías[STA94]:

Supervisión de red. Se considera una función de "lectura" y se encarga de observar y analizar el estado y el comportamiento de la configuración y componentes de la red.

Control de red. Se le considera como una función de "escritura" y se encarga de alterar los parámetros de los distintos componentes de la configuración de la red y hacer que lleven a cabo las acciones que se determinen.

1.1.1 Supervisión de red

Normalmente la supervisión de red se divide en tres áreas de diseño[STA94]:

A. **Acceso a información supervisada.** Trata de cómo definir la información supervisada y como trasladarla desde un recurso a un gestor.
B. **Diseño de los mecanismos de supervisión.** Trata de determinar la mejor forma de obtener la información de un recurso.
C. **Aplicaciones con la información supervisada.** Cómo se usa la información en las distintas áreas funcionales de gestión.

La supervisión de red se dirige hacia tres áreas funcionales:

A. **Supervisión del rendimiento.** Es imposible una gestión de red sin medir el rendimiento de la misma. Las medidas que se llevan a cabo son: disponibilidad, tiempo de respuesta, eficiencia, rendimiento (Throughput) y utilización. Las tres primeras están orientadas a los servicios y las segundas a la eficiencia de la red.
B. **Supervisión de fallos.** Pretende descubrir los fallos del sistema, identificar lo antes posible su causa y llevar a cabo las acciones para poder remediarlos.
C. **Supervisión de cuentas** . Lleva a cabo el control del uso de los distintos recursos de la red por parte de los usuarios. Algunos recursos sujetos a supervisión, pueden ser: facilidades de comunicación, como LANs, WANs, líneas alquiladas, hardware, como estaciones de trabajo y servidores.

1.1.2 Control de red

Esta parte de la supervisión de red se encarga de la modificación de parámetros, y hacer que se lleven a cabo las acciones por parte del sistema final, del sistema intermedio y las subredes que constituyen la configuración que debe ser gestionada. El control de red se divide en áreas funcionales:

A. **Configuración.** Trata de la inicialización, mantenimiento, y apagado de los componentes individuales y subsistemas lógicos del sistema. Algunas de las funciones que se deben llevar a cabo en la gestión de la configuración son las siguientes: elaboración de la información de la configuración, establecer y modificar los valores de configuración, definir y cambiar las relaciones, iniciar y finalizar operaciones de red, distribución de software e informar del estado de la configuración.
B. **Control de seguridad** . Se encarga de que se cumplan los siguientes requisitos:
   Privacidad. A la información sólo debe acceder áquel que esté autorizado.
   Integridad. Las características del sistema sólo deben poder modificarse por personas autorizadas.
C. **Disponibilidad** . Los recursos deben ser efectivos para uso de aquellos a los que se les permita.

1.2 Objetivos de la seguridad

La labor principal en seguridad informática es el aislamiento de los actos no deseables, y la prevención de aquellos que no se hayan considerado, de forma que si se producen hagan el menor daño posible. Entre las distintas actividades que se deben llevar a cabo se destacan las siguientes [AMO94] :

- **Identificación de los usuarios.** Existen varias técnicas entre las que se encuentran las contraseñas (passwords), o sistemas más sofisticados como reconocimiento del habla o a partir de huella dactilar o la retina del ojo.
- **Detección de intrusos en la red** . Se debe detectar y actuar sobre cualquier acceso no autorizado a un sistema. El objetivo es la detección de intrusos en tiempo real, antes de que el sistema haya sido dañado seriamente.
- **Análisis de riesgo.** Intenta cuantificar los beneficios obtenidos con la protección contra amenazas de seguridad. El riesgo es función de la frecuencia con la que se producen dichas amenazas, vulnerabilidad de la protección contra las mismas y las pérdidas potenciales que se produjesen en el caso de que se diese una.
- **Clasificación apropiada de los datos.** En la gestión de seguridad llegan gran cantidad de datos provenientes de los distintos programas de control generados a partir de las actuaciones que llevan a cabo los usuarios en el sistema. Es importante, para una buena supervisión de la seguridad, el clasificar los datos convenientemente, de tal forma que se ahorre tiempo en su análisis.
- **Control de las nuevas aplicaciones** . Cuando se instala una nueva aplicación se debe comprobar que no introduzca nuevas brechas de seguridad especialmente si se ejecuta con permisos de root.
- **Análisis de los accesos de los usuarios.** Es necesario tener un control para poder detectar intentos de acceso no autorizado.

1.3 Compromisos específicos de seguridad

Antes de comenzar a analizar los diferentes aspectos sobre seguridad es importante tener claras una serie de ideas sobre lo que significa. Existen varias formas de abordar la seguridad de un sistema[NAT94]. Un punto de vista es entenderla como una forma de prevenir futuras pérdidas, una manera de gestionar los riesgos relacionados con la tecnología. Otros consideran que es algo necesario para evitar que usuarios maliciosos entren en el sistema. Aparte de las diferencias que puedan existir entre ambas concepciones, se presenta una definición para este concepto dentro de los sistemas de computadoras [NAT94]:

La seguridad en sistemas de computadoras es la protección de la integridad, disponibilidad, y si es necesario la confidencialidad de la información y recursos que se usan, para la entrada, almacenamiento, proceso y comunicación de los mismos.

Existen una serie de compromisos básicos sobre la seguridad de sistemas de computadoras [NAT94]:

A. **No dificultar las labores de los usuarios** . El propósito de la seguridad es la protección de recursos considerados importantes dentro de la organización donde el sistema de seguridad está activo. En ocasiones lleva consigo ciertas imposiciones a

los usuarios de los recursos. Deben ser siempre aceptables y no ser una carga excesivamente grande.

B. **La seguridad es responsabilidad de la gestión de riesgos.** Una de las responsabilidades en la gestión de un sistema de computadoras en una determinada organización es el control del riesgo. De igual forma que a una determinada organización controla el dinero y los empleados, es necesario un control de la información. Tan crítico como los demás, puesto que se depende de ella para alcanzar los objetivos marcados. Se debe conseguir que la información esté disponible, sea correcta y esté completa. En algunos casos se debe restringir también el acceso a determinados datos.
C. **Se deben especificar claramente las responsabilidades en seguridad.** Para asegurarse que los objetivos de la gestión de seguridad se lleven a cabo, es necesario que se asignen responsabilidades de forma precisa. Los grupos a los que se le asignan estas tareas suelen ser los gestores de seguridad, operadores del sistema, gestores de las aplicaciones, el encargado de la seguridad física, la oficina de recuperación de desastres, los usuarios, y los encargados de los informes de supervisión.
D. **La seguridad requiere una estructuración clara.** La eficiencia de la seguridad precisa que distintos grupos y áreas dentro y fuera de la organización colaboren. La arquitectura o programa de seguridad se suele dividir en bloques que se denominan controles, agrupados en controles técnicos, de operación y de servicio. Para que la gestión de seguridad sea la óptima hay que conocer esta estructuración y la interacción entre cada uno de ellos.
E. **La protección del sistema debe tener un costo soportable.** Los costos y los beneficios de la seguridad del sistema deben ser examinados cuidadosamente, para que el primero no sobrepase al segundo. Hay que tener en cuenta que una inversión en seguridad puede suponer disminuir el número de pérdidas debido a fallos del sistema o por manipulación fraudulenta de los recursos. Los beneficios de la seguridad no son sólo monetarios, evita hackers así como otros elementos hostiles a nuestro sistema, ayudando a ofrecer una buena imagen hacia el público.

1.4 Servicios de seguridad

Para hacer frente a las amenazas a la seguridad del sistema se definen una serie de servicios para proteger los sistemas de proceso de datos y de transferencia de información de una organización. Estos servicios hacen uso de uno o varios mecanismos de seguridad. Una clasificación útil de los servicios de seguridad es la siguiente[AMO94]:

- **Confidencialidad:** Requiere que la información sea accesible únicamente por las entidades autorizadas. La confidencialidad de datos se aplica a todos los datos intercambiados por las entidades autorizadas o tal vez a sólo porciones o segmentos seleccionados de los datos, por ejemplo mediante cifrado. La confidencialidad de flujo de tráfico protege la identidad del origen y destino(s) del mensaje, por ejemplo enviando los datos confidenciales a muchos destinos además del verdadero, así como el volumen y el momento de tráfico intercambiado, por ejemplo produciendo una cantidad de tráfico constante al añadir tráfico espurio al significativo, de forma que sean indistinguibles para un intruso. La desventaja de estos métodos es que incrementan drásticamente el volumen de tráfico intercambiado, repercutiendo negativamente en la disponibilidad del ancho de banda bajo demanda.

- **Autenticación:** Requiere una identificación correcta del origen del mensaje, asegurando que la entidad no es falsa. Se distinguen dos tipos: de entidad, que asegura la identidad de las entidades participantes en la comunicación, mediante biométrica (huellas dactilares, identificación de iris, etc.), tarjetas de banda magnética, contraseñas, o procedimientos similares; y de origen de información, que asegura que una unidad de información proviene de cierta entidad, siendo la firma digital el mecanismo más extendido.
- **Integridad:** Requiere que la información sólo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de los mensajes transmitidos. La integridad de datos asegura que los datos recibidos no han sido modificados de ninguna manera, por ejemplo mediante un hash criptográfico con firma, mientras que la integridad de secuencia de datos asegura que la secuencia de los bloques o unidades de datos recibidas no ha sido alterada y que no hay unidades repetidas o perdidas, por ejemplo mediante time−stamps.
- **No repudio:** Ofrece protección a un usuario frente a que otro usuario niegue posteriormente que en realidad se realizó cierta comunicación. Esta protección se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje. Las firmas digitales constituyen el mecanismo más empleado para este fin.
- **Control de acceso:** Requiere que el acceso a los recursos (información, capacidad de cálculo, nodos de comunicaciones, entidades físicas, etc.) sea controlado y limitado por el sistema destino, mediante el uso de contraseñas o llaves hardware, por ejemplo, protegiéndolos frente a usos no autorizados o manipulación.
- **Disponibilidad:** Requiere que los recursos del sistema informático estén disponibles a las entidades autorizadas cuando los necesiten.

1.5 Amenazas deliberadas a la seguridad de la información

Se entiende por amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo). La política de seguridad y el análisis de riesgos habrán identificado las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios[NAT94].

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente, como por ejemplo un archivo o una región de la memoria principal, a un destino, como por ejemplo otro archivo o un usuario. Un ataque no es más que la realización de una amenaza [AMO94] [SAN94].

Las cuatro categorías generales de amenazas o ataques son las siguientes (v. Figura 1.1):

- **Interrupción:** un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos.

- **Intercepción:** una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o una computadora. Ejemplos de este ataque son tomar una línea con datos que circulen por la red y la copia ilícita de archivos o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

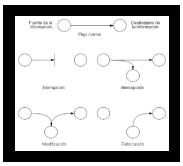

Figura 1.1 Categorías generales de amenazas

- **Modificación** : una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.
- **Fabricación:** una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad. Ejemplos de este ataque son la inserción de mensajes esporádicos en una red o añadir registros a un archivo.

Estos ataques se pueden así mismo clasificar de forma útil en términos de ataques pasivos y ataques activos.

1.5.1 Ataques pasivos

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitorea, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

- Obtención del origen y destinatario de la comunicación, leyendo las cabeceras de los paquetes monitoreados.
- Control del volumen de tráfico intercambiado entre las entidades monitoreadas, obteniendo así información acerca de actividad o inactividad inusuales.
- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

1.5.2 Ataques activos

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

- **Suplantación de identidad:** el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.
- **Reactuación:** uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.
- **Modificación de mensajes:** una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesos en la cuenta A" podría ser modificado para decir "Ingresa un millón de pesos en la cuenta B".
- **Degradación fraudulenta del servicio:** impide o inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones. Por ejemplo, el intruso podría suprimir todos los mensajes dirigidos a una determinada entidad o se podría interrumpir el servicio de una red inundándola con mensajes esporádicos. Entre estos ataques se encuentran los de denegación de servicio, consistentes en paralizar temporalmente el servicio de un servidor de correo, Web, FTP, etc.

1.6 Mecanismos de seguridad

No existe un único mecanismo capaz de proveer todos los servicios anteriormente citados, pero la mayoría de ellos hacen uso de técnicas criptográficas basadas en el cifrado de la información. Los más importantes son los siguientes [AMO94] [NAT94].:

a. **Intercambio de autenticación:** Corrobora que una entidad, ya sea origen o destino de la información, es la deseada, por ejemplo, A envía un número aleatorio cifrado con la clave pública de B, B lo descifra con su clave privada y se lo reenvía a A, demostrando así que es quien pretende ser. Por supuesto, hay que ser cuidadoso a la hora de diseñar estos protocolos, ya que existen ataques para desbaratarlos.
b. **Cifrado:** Garantiza que la información no es legible para individuos, entidades o procesos no autorizados (confidencialidad). Consiste en transformar un texto claro mediante un proceso de cifrado en un texto cifrado, gracias a una información secreta o clave de cifrado. Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico. Estos sistemas son mucho más rápidos que los de clave pública, resultando apropiados para funciones de cifrado de grandes volúmenes de datos. Se pueden dividir en dos categorías: cifradores de bloque, que cifran los datos en bloques de tamaño fijo (típicamente bloques de 64 bits), y cifradores en flujo, que trabajan sobre flujos continuos de bits. Cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es asimétrico o de clave pública. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública, puede ser conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas, para descifrar. El sistema tiene la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada. Los criptosistemas de clave

pública, aunque más lentos que los simétricos, resultan adecuados para las funciones de autenticación, distribución de claves y firmas digitales.

c. **Integridad de datos:** Este mecanismo implica el cifrado de una cadena comprimida de datos a transmitir, llamada generalmente valor de comprobación de integridad (Integrity Check Value o ICV). Este mensaje se envía al receptor junto con los datos ordinarios. El receptor repite la compresión y el cifrado posterior de los datos y compara el resultado obtenido con el que le llega, para verificar que los datos no han sido modificados.
d. Firma digital: Este mecanismo implica el cifrado, por medio de la clave secreta del emisor, de una cadena comprimida de datos que se va a transferir. La firma digital se envía junto con los datos ordinarios. Este mensaje se procesa en el receptor, para verificar su integridad. Juega un papel esencial en el servicio de no repudio.
e. **Control de acceso:** Esfuerzo para que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red, como por ejemplo mediante las contraseñas de acceso.
f. **Tráfico de relleno:** Consiste en enviar tráfico espurio junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.
g. **Control de encaminamiento** : Permite enviar determinada información por determinadas zonas consideradas clasificadas. Así mismo posibilita solicitar otras rutas, en caso que se detecten persistentes violaciones de integridad en una ruta determinada.
h. **Unicidad:** Consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos. De esta forma se evitan amenazas como la reactuación o resecuenciación de mensajes.

Los mecanismos básicos pueden agruparse de varias formas para proporcionar los servicios previamente mencionados. Conviene resaltar que los mecanismos poseen tres componentes principales:

- Una información secreta, como claves y contraseñas, conocidas por las entidades autorizadas.
- Un conjunto de algoritmos, para llevar a cabo el cifrado, descifrado, hash y generación de números aleatorios.
- Un conjunto de procedimientos, que definen cómo se usarán los algoritmos, quién envía qué a quién y cuándo.

Así mismo es importante notar que los sistemas de seguridad requieren una gestión de seguridad. La gestión comprende dos campos bien amplios:

- Seguridad en la generación, localización y distribución de la información secreta, de modo que sólo pueda ser accesada por aquellas entidades autorizadas.
- La política de los servicios y mecanismos de seguridad para detectar infracciones de seguridad y emprender acciones correctivas.

1.7 Situación Actual UDLA

En la actualidad se han implantado diversas herramientas para solucionar problemas específicos de seguridad como es el caso de ***Kerberos*** (autenticación de usuarios). Desgraciadamente, la mayoría de estas soluciones solicitan adecuar las máquinas (hardware)

al sistema (software), cuando lo idóneo es hacerlo al revés. Por otro lado su elevado costo las hace inaccesibles.

Actualmente el aceso remoto desde un nodo externo hacia el interior del campus se encuentra cerrado. Los únicos servicios disponibles mundialmente son consulta ***Web*** , acceso a correo electrónico a través de ***IMAP o POP*** y experimentalmente conexión ***telnet*** a través de un ambiente restringido. El acceso desde el exterior hacia la UDLA está cerrado por no contar con un esquema que integre servicios eficientes de seguridad.

Por otro lado, la intranet UDLA no se monitorea en el total de sus actividades para detectar casos sospechosos debido a los pocos recursos económicos y de personal capacitado. Mucho menos se cuenta con procesos automáticos que hagan dicha labor. Este seguimiento se hace bajo demanda de algún usuario que ha sido perjudicado en el uso incorrecto de su cuenta. Debido a que el acceso remoto desde fuera del campus hacia el interior está cerrado, el sospechoso suele ser alguien cercano al afectado que de alguna forma consiguió su password. El esquema actual se resume en la siguiente figura:(Figura 1.1)

1.8 Propuesta: ASIS, un esquema integral

Si se contara con un esquema integral de seguridad informática en la UDLA entonces se tendrían procedimientos consistentes de acción y prevención ante un ataque, actividad sospechosa o cumplimiento de políticas definidas por el administrador de la red de la Universidad.

El objetivo general de este proyecto consiste en diseñar y aplicar un esquema integral de seguridad informática basado en un estudio de metodologías de seguridad para satisfacer los requerimientos usuario−infraestructura−administrador de la red de la UDLA.

Figura 1.2 Esquema Actual de Seguridad Informática en la UDLA

Alcances y limitaciones

El alcance principal será renovar el esquema de seguridad existente en la UDLA (Internet−Intranet) mejorándolo en su documentación, ofrecer servicios típicamente internos al exterior sin comprometer la seguridad y renovar las herramientas que ya tienen algunos años funcionando a sus versiones modernas.

Las tecnologías de seguridad más importantes no pueden exportarse de EEUU a ningún otro país, lo cual limitará el nivel seguridad de este proyecto.