***Universidad Tecnológica de Panamá***

***FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES***

***Tópicos Especiales II - Seguridad Informática***

***Vocabulario #1***

***Nombre***: *César Nuñez 2-733-2271; Batista Johel 8-914-587 ;*

*Luis Villarreal 8-876-1699*

**1 - Ciberseguridad:** Por otro lado, la ciberseguridad es el conjunto de tecnologías, procesos y prácticas diseñados para proteger redes, computadoras, programas y datos de ataques, daños o accesos no autorizados. En un contexto informático, incluye seguridad cibernética y física.

Una definición contextual, basada en una que sea relevante, se ajusta a los ejemplos como el de la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés) que subraya que es la recopilación de herramientas, políticas, conceptos de seguridad, medidas de seguridad, directrices, enfoques de gestión de riesgos, acciones, capacitación, mejores prácticas, aseguramiento y tecnologías que pueden utilizarse para proteger el entorno cibernético y la organización y los activos del usuario.



**2 - Seguridad en la Información:** Se refiere a un conjunto de métodos, procesos o técnicas para la protección de los sistemas informáticos, desde redes, infraestructura, equipos de comunicación hasta la información en formato digital que estos almacenen.

Kaspersky Lab dicta que la seguridad informática es la práctica de defender computadoras, servidores, dispositivos móviles, sistemas electrónicos, redes y datos de ataques maliciosos. Un término amplio y que se aplica a todo, desde la seguridad informática hasta la recuperación ante desastres y la educación del usuario final.

**3 - Seguridad en las Aplicaciones:** La identificación de las necesidades de seguridad es vital a la hora de crear protocolos efectivos. Es en esta etapa donde se deben tomar en cuenta y evaluar aquellos factores más propensos a causar un impacto en la seguridad de aplicaciones web.

Por ejemplo: Nivel de sensibilidad de los datos manejados en la aplicación, accesibilidad; rastreabilidad, tipo de usuarios que tendrán acceso, etc. Después del proceso de identificación lo más recomendable es priorizar los factores de mayor impacto para así proceder a establecer las estrategias efectivas.

**4 - Seguridad en la Nube:** La seguridad en la nube son todas aquellas medidas de seguridad basadas en software que se toman para proteger la información que fluye a través de los recursos de la nube.

La nube surge como una opción eficiente y sencilla a la hora de guardar información ya que evita que el usuario tenga que preocuparse de mantener servidores físicos y dispositivos de memoria. Esto supone un ahorro del 41% en recursos y un aumento del 46% en la disponibilidad de los datos.

**5 - Criptografía:** Es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Su utilización es tan antigua como la escritura. Los romanos usaban códigos para ocultar sus proyectos de guerra de aquellos que no debían conocerlos, con el fin de que sólo las personas que conocían el significado de estos códigos descifren el mensaje oculto.

A partir de la evolución de las computadoras, la criptografía fue ampliamente divulgada, empleada y modificada, y se constituyó luego con algoritmos matemáticos. Además de mantener la seguridad del usuario, la criptografía preserva la integridad de la web, la autenticación del usuario así como también la del remitente, el destinatario y de la actualidad del mensaje o del acceso.

****

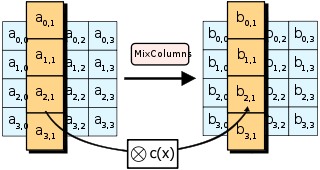
**6 - Cifrado Simétrico:** Un sistema de cifrado simétrico es un tipo de cifrado que usa una misma clave para cifrar y para descifrar. Las dos partes que se comunican mediante el cifrado simétrico deben estar de acuerdo en la clave a usar de antemano. Una vez de acuerdo, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra usando la misma clave.

Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando. Sólo si el atacante obtuviera la clave, le serviría conocer el algoritmo. Los algoritmos de cifrado usados en GnuPG tienen estas propiedades.

Dado que toda la seguridad está en la clave, es importante que sea muy difícil adivinar el tipo de clave. Esto quiere decir que el abanico de claves posibles, o sea, el espacio de posibilidades de claves, debe ser amplio. Richard Feynman fue famoso en Los Álamos por su habilidad para abrir cajas de seguridad. Para alimentar la leyenda que había en torno a él, llevaba encima un juego de herramientas que incluían un estetoscopio. En realidad, utilizaba una gran variedad de trucos para reducir a un pequeño número la cantidad de combinaciones que debía probar, y a partir de ahí simplemente probaba hasta que adivinaba la combinación correcta. En otras palabras, reducía el tamaño de posibilidades de claves.

**7 - AES:** Es uno de los algoritmos más seguros que existen hoy en día. Está clasificado por la National Security Agency (NSA) de EE.UU. para la más alta seguridad de la información secreta. Se basa en varias sustituciones, permutaciones y transformaciones lineales, ejecutadas en bloque de datos de 16 bytes, que se repiten varias veces.

Hasta el momento no existe posibilidad de ataque contra AES, por lo que este algoritmo sigue siendo el estándar de cifrado preferido por gobiernos, bancos y sistemas de alta seguridad de todo el mundo.



**8. Cifrado Asimétrico:** También conocido como “Criptografía de Llave Pública”, emplea dos llaves en vez de una para ejercer las funciones de cifrado y descifrado de la información. En el cifrado asimétrico cada usuario que interviene en la comunicación cuenta con dos llaves: una llave pública y una llave privada. La llave pública es utiliza para cifrar la información y llave privada para descifrar la información.

Los sistemas de cifrado asimétrico se inventaron con el fin de evitar por completo el problema del intercambio de claves. Un sistema de cifrado asimétrico usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona.

La otra clave es privada y el propietario debe guardarla para que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje.



**9. RSA:** Es un algoritmo de cifrado de clave pública que le permite al usuario conservar la confidencialidad de la información cuando es transmitida o compartida con otros usuarios. Conocer en qué consiste es la mejor opción para utilizarlo de forma adecuada y salvaguardar la información más sensible.

La fortaleza del algoritmo RSA se basa en la complejidad de cálculo que tiene encontrar los dos factores primos de un número compuesto muy grande. La operación inversa de este problema, es decir multiplicar dos números primos grandes, es una operación poco costosa computacionalmente y que se puede realizar rápidamente, pero en sentido contrario, es decir encontrar los factores primos de un número es una operación que a medida que se incrementa el tamaño del número aumenta los requerimientos de hardware para su cálculo además de aumentar el tiempo requerido para su cálculo.

El uso de este algoritmo se ha extendido hasta tal punto que se publicó el RSA Cryptography Standard, que contiene las recomendaciones para la implementación de métodos criptográficos de clave pública basados en el algoritmo RSA. Esta documentación contiene algunas nociones básicas sobre cifrado y descifrado y sobre firma y verificación de mensajes.

**10. Seguridad de Infraestructura:** Se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

Se encarga de asegurar la parte software de un sistema informático, que se compone de todo lo que no es físico, como programas y datos. También se encarga de controlar el acceso al sistema informático, desde el punto de vista software, se realice correctamente y por usuarios autorizados, ya sea desde dentro del sistema informático o desde fuera, es decir, desde una red externa, usando una VPN, la WEB, transmisión de archivos, conexión remota, etc.

**11. Respuestas a Incidentes:** Estos equipos controlan y minimizan el número de riesgos y amenazas, evalúan constantemente las vulnerabilidades en los sistemas, protegen datos e información, promueven la difusión hacia la seguridad de la información, brindan soporte de forma rápida y efectiva, analizan y gestionan incidentes de seguridad.

Actualmente, los equipos de respuesta de seguridad informática evolucionan con el objetivo de satisfacer de una mejor manera las necesidades requeridas por la comunidad, orientando un modelo integral de gestión hacia la seguridad de la información a través de una estructura proactiva y reactiva, mediante la integración de un conjunto de habilidades que se centran en la continuidad de la práctica, la respuesta, la prevención y el seguimiento hacia los incidentes de seguridad de la información. Los servicios del CSIRT\* se pueden dividir en tres categorías:

* **Servicios reactivos**: Hacen referencia a los servicios centrados a responder y tratar los incidentes y reducir los riesgos que puedan presentarse.
* **Servicios proactivos**: Estos servicios están enfocados hacia la prevención de incidentes mediante la sensibilización, la asesoría y la formación para brindar seguridad a los sistemas de comunicación, redes e información.
* **Servicios de gestión de calidad de la seguridad**: Son servicios establecidos para medidas educativas por medio de la experiencia adquirida en la prestación de los servicios reactivos y proactivos.

**12. Vulnerabilidad:** Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos.

Estas vulnerabilidades son producto de fallos producidos por el mal diseño de un software, sin embargo, una vulnerabilidad también puede ser producto de las limitaciones propias de la tecnología para la que fue diseñado.

**13. Amenaza:** Todo elemento o acción capaz de atentar contra la seguridad de la información. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

Diversas situaciones, tales como el incremento y el perfeccionamiento de las técnicas de ingeniería social, la falta de capacitación y concientización a los usuarios en el uso de la tecnología, y sobre todo la creciente rentabilidad de los ataques, han provocado en los últimos años el aumento de amenazas intencionales. Las amenazas pueden clasificarse en dos tipos:

* **Intencionales**, en caso de que deliberadamente se intente producir un daño (por ejemplo, el robo de información aplicando la técnica de trashing, la propagación de código malicioso y las técnicas de ingeniería social).
* **No intencionales**, en donde se producen acciones u omisiones de acciones que, si bien no buscan explotar una vulnerabilidad, ponen en riesgo los activos de información y pueden producir un daño (por ejemplo, las amenazas relacionadas con fenómenos naturales).

**14. Riesgo:** La posibilidad que suceda una eventualidad que imposibilita el cumplimiento de un objetivo, en lo relacionado con la informática generalmente el riesgo se plantea como amenaza determinando el grado de posibilidad a una pérdida, por ejemplo, el riesgo de perder información o datos, virus informáticos, etc. Se pueden identificar varios elementos los cuales son: probabilidad, amenazas, vulnerabilidades, activos e impactos.

Es importante recordar que el riesgo es el impacto negativo en el ejercicio de la vulnerabilidad, considerando la probabilidad y la importancia de ocurrencia. Por lo que podemos decir a grandes rasgos que la administración de riesgos es el proceso de identificación, evaluación y toma de decisiones para reducir el riesgo a un nivel aceptable.

Para poder establecer la posición real a los riesgos se incurre a una herramienta llamada, análisis de riesgo el cual tiene como objetivo, identificar el riesgo mediante la identificación de sus elementos y lograr establecer el riesgo total, realizar el análisis del riesgo es muy importante para lograr administrar adecuadamente los mismos, el proceso de administración del riesgo es continuo dado que es necesario evaluar periódicamente si los riesgos identificados y la exposición a los mismos calculado anteriormente se mantiene vigente.

**15**. **Gestión de Vulnerabilidades**: Es el proceso de identificar brechas de seguridad en el software y, después, repararlas para evitar el acceso no deseado a sistemas y datos confidenciales. La gestión de vulnerabilidades de TI es un ciclo continuo que abarca la supervisión, el triaje y la reparación de las debilidades del sistema. El ciclo incluye el desarrollo de políticas de seguridad, detección e inventario de activos, supervisión de perímetros, y evaluación y priorización de amenazas.

Los escáneres y los asignadores de red, puertos e IP, junto con los sistemas de alertas, se pueden emplear con esta finalidad. Las redes que son seguras en este aspecto se definen a menudo como "redes" reforzadas. Dado que los atacantes están constantemente al acecho de debilidades de la red, la gestión de vulnerabilidades es un componente esencial de un programa de seguridad de red completo.

Junto con soluciones de perímetro como firewalls, antivirus y sistemas de detección de intrusión, las soluciones de gestión de vulnerabilidades pueden ayudar a evitar el acceso no deseado a sistemas y datos confidenciales. Un buen sistema de gestión de vulnerabilidades te ayudará a eliminar las debilidades internas al priorizar la protección de tus activos más importantes.

**16**. **Respaldo (Desde el punto de vista de la información)**: también llamado “Backup” o “Copia de seguridad”, es el procedimiento que se implementa cuando queremos tener resguardados nuestros datos o documentos en caso de que suceda algún imprevisto con nuestros sistemas informáticos, más precisamente con los discos duros, ya que estos son bastante delicados y son uno de los componentes informáticos con más alta probabilidad de presentar fallos.

Un respaldo de información bien organizado y estructurado nos permitiría volver a acceder a nuestros documentos para continuar trabajando con la mayor velocidad y eficiencia posibles, además de evitar que información importante se pierda. El respaldo de nuestros datos debería ser realizado en múltiples dispositivos de almacenamiento, y también, para mayor seguridad en la nube, en cualquiera de los servicios que existen para ello en la actualidad.

**17**. **Violación de Datos (Data Breach)**: Incidente donde información es robada o tomada por un sistema sin conocimiento o autorización del dueño del sistema. La información robada puede ser sensitive o confidencial como tarjetas de crédito, información de clientes, secretos, u otros asuntos de seguridad.

Los daños de la violación de datos pueden ser en monetarios por parte de la empresa y los usuarios o no monetarios, por ejemplo, la pérdida de credibilidad de la organización.

**18**. **Sistema de Gestión de Seguridad de la Información** (ISMS, information security management system): Un ISMS, es un grupo de políticas y procedimientos para manejar sistemáticamente la información sensitiva de una organización. El objetivo de un ISMS es minimizar los riesgos y asegurar la continuidad de un negocio al limitar activamente el impacto que puede tener una violación de datos.

Usualmente, un ISMS es dirigido al comportamiento del empleado y a los procesos que tengan que ver con tecnología e información. Puede ser dirigido a un tipo específico de violación de datos o puede ser implementado de una manera que forme parte de la cultura de la sociedad.

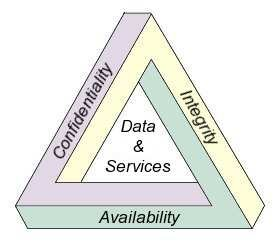
**19**. **Reglamento General de Protección de Datos** (GDPR, General Data Protection Regulation): es la nueva normativa que regula la protección de los datos de los ciudadanos que vivan en la Unión Europea. Este reglamento recoge y reconoce, por tanto, derechos, como al olvido y el derecho a la portabilidad.

El primero establece que los ciudadanos podemos solicitar y lograr que nuestros datos personales sean eliminados cuando, entre otros casos, estos ya no sean necesarios para la finalidad con la que fueron recogidos, cuando se haya retirado el consentimiento o cuando estos se hayan recogido de forma ilícita.

Mientras, el derecho a la portabilidad te permite que, si tus datos se están tratando de modo automatizado, puedas recuperarlos en un formato para cederlos a otro responsable. Estos datos deben estar "en un formato estructurado, de uso común y lectura mecánica para que pueda transmitirlos fácilmente a otro responsable y facilitar así un cambio de proveedor

**20**.**Tríada CIA**: Es un modelo para la creación de políticas usadas al identificar problemas y soluciones en el área de la seguridad de información. Fue creado para ayudar a las personas a pensar sobre diferentes partes de la seguridad. Sus siglas vienen de Confidencialidad, integridad y disponibilidad (availability).

La triada dice que proteger la confidencialidad depende de poder definir y enforzar diferentes accesos de nivel para la información separándose y organizándose en áreas dependiendo quién puede acceder o no. La integridad quiere decir que la información debe ser protegido de ser borrada o modificada por un externo no autorizado. Y la información debe tener disponibilidad en cualquier momento que sea necesitada.



**21**. **Gobierno (de la seguridad de información):** Conjunto de responsabilidades y prácticas ejercidas por la junta directiva y la dirección ejecutiva, con la finalidad de brindar una dirección estratégica, garantizar que se logren los objetivos, determinar que los riesgos se administren en forma apropiada y verificar que los recursos de la empresa se utilicen con responsabilidad.

También es definida como estructura a través de la cual se establecen los objetivos de la empresa, y se determinan los medios para alcanzar dichos objetivos y monitorear el desempeño.

**22**. **ISO/IEC 27001**: norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

Puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. La norma se ha convertido en la principal norma a nivel mundial para la seguridad de la información.

**23**. **ISO/IEC 27002**: norma que establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Esto también incluye la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa.

La versión más reciente es la ISO/IEC 27002:2013. La ISO 27002 no distingue entre los controles que son aplicables a una organización determinada y los que no lo son. Por otro lado, la ISO 27001 exige la realización de una evaluación de riesgos sobre cada control para identificar si es necesario disminuir los riesgos y, en caso de que sea necesario, hasta qué punto deben aplicarse.

**24**.**NIST (National Institute of Standards and Technology)**: llamada entre 1901 y 1988 Oficina Nacional de Normas (NBS por sus siglas del inglés *National Bureau of Standards*) es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.

