TEMA

Tema 1. Conceptos básicos de Seguridad Informática

Administración de sistemas informáticos en Red

Seguridad y alta disponibilidad

Autor/a: Joaquín Erencia

Linkia FP

Tema 1: Conceptos básicos de Seguridad Informática

¿Qué aprenderás?

- Cuando se considera un sistema informático seguro.
- Qué es el ESN.
- Qué capas del sistema informático se deben proteger.
- Qué significa el concepto de Alta Disponibilidad.

¿Sabías que…?

- Los problemas informáticos de las empresas tienen su origen, en un porcentaje muy elevado, en el interior de estas.

1.1. Introducción

1.1.1. ¿Por qué es necesario este módulo?

Si eres estudiante de Sistemas y has llegado a este módulo de segundo curso, esta pregunta que te hago no es necesaria que la respondas. La respuesta la tienes clara. Estoy convencido que no has parado de recibir inputs sobre este tema durante estos años: Seguridad, Hacking, Piratas informático, cortafuegos, proxy, Cloud…

Seguro que ya has asumido que estamos en un mundo interconectado, donde **TU INFORMACIÓN** es importante, y, por lo tanto, debes protegerla. Tienes una contraseña fuerte, usas la huella digital para los programas importantes de tu móvil, no entras en páginas web inseguras, no te conectas a la web de tu banco desde la wifi de un centro comercial, no tienes la contraseña apuntada en un papelito en el monitor de tu ordenador, la cámara de portátil está tapada, no das tus datos a ningún correo electrónico que te llegue, te preocupas por saber qué información comparte tu nevera o microondas o termostato o tu coche, y … ¿Seguro?

También te puedes plantear tener toda tu información personal en la nube, en el famoso **Cloud**, y te interesa saber si la empresa que "gratuitamente" te brinda una serie de gigas tan desinteresadamente cumple los criterios que tú mantienes en tu día a día. Pero también tienes claro que necesitas que esa información que has subido a ese servicio, para no almacenarla tú en tu disco duro, por el motivo que sea, esté disponible cuando la necesites. Y no solo tu información, imagina que eres el responsable del departamento informático de una empresa y decides externalizar parte o toda la información de tu empresa y traspasarla a la nube: ¿está **protegida**? ¿cumple con las **normativas legales de protección de datos**? ¿puedes utilizarla cuando quieras? Imagina cuantos problemas puedes tener si alguno de estas preguntas no tiene una respuesta afirmativa.

Pues de estos dos párrafos últimos trata este módulo de Seguridad y Alta Disponibilidad, pero seamos realistas. Todo lo que vas a aprender durante este módulo te servirá para poder entrar y ver lo amplio que es este mundo. No vamos a profundizar en ninguno de los campos de los que se

compone, no es el objetivo, lo que sí que te va a dar la visión necesaria para elegir uno (o varios si tienes mucho tiempo) y dedicarte con pasión en ellos. No te voy a formar como experto de seguridad, ni como responsable de protección de datos de una empresa, ni como hacker ético, ni serás un pirata bueno (hacker) o un pirata malo (cracker), pero si al acabar el módulo tienes claro qué campo és el que más te atrae y he despertado en ti las ganas de dedicar mucho de tu tiempo en él, me quedo satisfecho.

1.1.2. Por si todavía no te he despertado tu interés

A continuación, tienes algunas noticas importantes que pueden indicarte que lo que vamos a aprender está dentro de tu vida diaria.

1. NOTICIA 1:

Con 9.000 vulnerabilidades reportadas en la primera mitad del año, se prevé que el total final para 2020 podría superar el doble

Fuente: Los expertos predicen un récord de vulnerabilidades para 2020 | Security and Risk Management | Discover The New (ituser.es)

2. NOTICIA 2:

Prácticamente 9 de cada 10 empresas, un 87% de las organizaciones, no dispone del presupuesto necesario para poner en marcha sistemas efectivos de ciberseguridad que permita frenar los ciberataques a las que se ven sometidas.

Entre las principales vulnerabilidades que destacan los directivos que deben afrontar, destacan la falta de cuidado por parte de los ***empleados*** *(34%), los controles de seguridad desfasados (26%), y los accesos externos desautorizados (13%). Junto a éstos, también destacan los riesgos asociados al uso de la nube para almacenar la información (10%).*

Fuente:https://www.muycanal.com/2019/02/25/ey-presupuesto-ciberseguridad

3. NOTICIA 3:

Los cuatro ataques más importantes de la historia:

- *PlayStation Network (2011)* en el que 77 millones de cuentas se quedaron sin conexión durante 23 días
- *Sony Pictures Entertainment (2014*) tuvieron acceso a información sobre empleados de Sony Pictures Entertainment, e-mails confidenciales, direcciones e información financiera. ¡Incluso los informes médicos de varias estrellas de Hollywood!
- *Epsilon (2011).* Epsilon, el mayor proveedor de servicios de marketing a nivel mundial recibió una serie de ataques que costaron en torno a los tres mil millones de dólares.
- *Heartbleed (2012-2014)* Heartbleed no fue un virus, sino un Bug que por error fue escrito en OpenSSL. Esta brecha de seguridad fue descubierta por un rápido grupo de hackers que aprovechó para conseguir información.

Estos y algunos más en el siguiente artículo.

Fuente: https://www.computing.es/seguridad/noticias/1116703002501/10-ciberataques-mas-grandes-de-decada.1.html

4. NOTICIA 4

2021, el año de la ciberseguridad también para los automóviles.

Fuente: https://www.niusdiario.es/economia/motor/2021-ano-ciberseguridad-hackers-tambien-automovil_18_3070995079.html

1.2. Conceptos básicos para empezar

1.2.1. Seguridad informática

Tengamos una cosa clara, la seguridad no existe. No hay un sistema que esté libre de daño, peligro o riesgo. Lo que tenemos que hacer es integrar de una manera ordenadas todos los elementos necesarios que como responsable y/o usuario de un sistema nos proporciones la sensación de seguridad, dificultando lo máximo posible la aparición de puntos débiles.

Por lo tanto, podemos definir **Seguridad de un Sistema Informático** como los mecanismos de prevención, detección, restauración y análisis que se llevan a cabo para garantizar la seguridad del sistema. En la siguiente imagen puedes ver todos los puntos de que se componen y que, lógicamente, no se aplican a todas las situaciones.

Imagen: Medidas de Seguridad del ENS (Esquema Nacional de Seguridad)

También te invito a leer, tranquilamente, la reglamentación que desarrolla esta imagen en el siguiente enlace: https://www.ccn.cni.es/index.php/es/esquema-nacional-de-seguridad-ens

1.2.2. Sistema seguro

Visto lo anterior vamos a definir que podemos hablar de un Sistema Seguro cuando cumple los siguientes criterios:

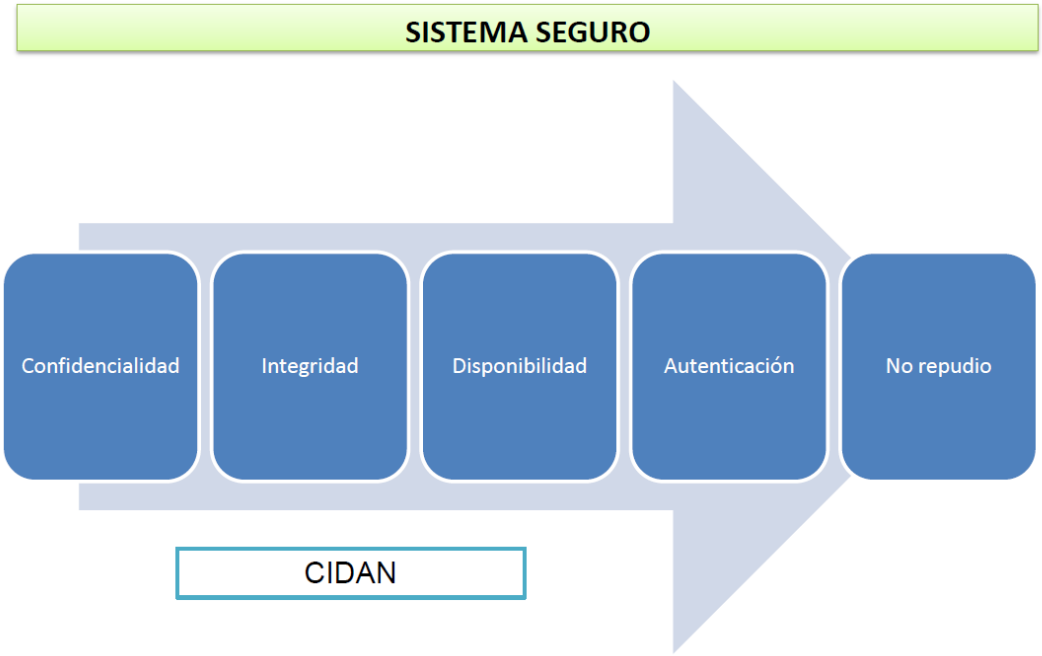


Imagen: CIDAN Fuente: Propia

Definamos a continuación los puntos que lo componen:

1. **Confidencialidad**: La información almacenada en el sistema informático solamente va a estar disponible para aquellas personas autorizadas. O sea, si nos roban el portátil no podrán acceder a la información que hay dentro.
2. **Integridad**: La información que se ha almacenado y/o transmitido no ha sido modificada sin autorización. Por ejemplo, los datos bancarios no pueden ser capturados y modificados en el tránsito desde el servidor del banco a nuestro navegador.
3. **Disponibilidad**: Tanto el sistema informático como la información que contiene van a estar disponibles al usuario en cada momento. Supongamos que realizamos un curso a distancia y queremos poder subir el documento de la práctica a la hora que queramos.
4. **Autenticación**: Para introducirse a un sistema informático se verificará la identidad digital del usuario y solo tendrá acceso a la información y con los permisos que tenga determinados.
5. **No repudio**: No se puede negar que en las dos partes de una comunicación (emisor-receptor) uno no es quien dice ser. Esto es muy importante en las transacciones comerciales en Internet.

1.2.3. Capas del sistema a proteger

Basándonos en el ENS, vamos a estudiar las siguientes capas de nuestro sistema informático a leer y el elemento que la protege, los cuales van a coincidir con los temas de este Módulo de Seguridad y Alta Disponibilidad.

Imagen: Medidas de protección Fuente: Propia

1.2.4. Amenaza informática

Definiremos **Amenaza** como todo elemento o acción capaz de atentar contra la seguridad de la información.

Si tenemos constancia de una amenaza (por ejemplo, recibimos correos electrónicos indeseados, ralentización del sistema, publicidad no deseada…) es una advertencia de que puede ser inminente el daño a algún activo de la información o que se está produciendo.

Clasificaremos estas amenazas en:

- Internas: Las que provienen del interior del sistema informático
- Externas: Las que provienen de agentes externos a nuestro sistema

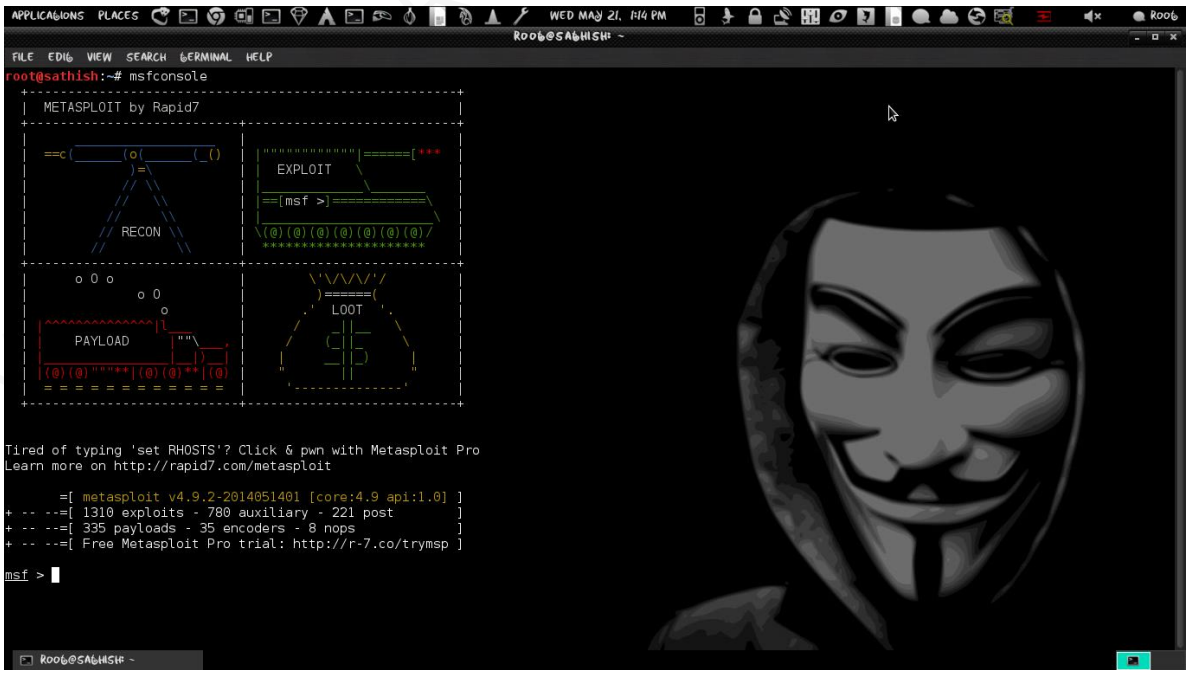
1.2.5. Vulnerabilidad

Una **vulnerabilidad** en un sistema es la puerta abierta que tenemos para posibles ataques y que en cualquier momento pueden ser aprovechadas.

Todos los sistemas informáticos sufren vulnerabilidades pues cada día aparecen fallos informáticos en los programas que tenemos instalados o hay gente que los encuentra. Es nuestra responsabilidad mantener los sistemas siempre actualizados para poder reducir su número. Cada vez que visito una empresa y veo que el sistema operativo está desactualizado, páginas webs con versiones de gestor antiguas, redes inalámbricas abiertas, no ocultas y con una contraseña "por defecto" … pienso "cuanto que hay por hacer".

También hay una "vulnerabilidad humana", el usuario. Para ello dedicaremos un tema especial pues campos como Cortafuegos, Proxy y la "Ingeniería Social", son necesarios para ahorrarnos muchos problemas de esos que luego nos dicen "pero si yo no he hecho nada".

A las vulnerabilidades que permiten a un intruso acceder a un sistema y disponer de permisos de administrador, se les denomina **Exploit**. Más concretamente, el Exploit es la herramienta creada para aprovechar una vulnerabilidad concreta.



Estos Exploit se pueden clasificar en dos tipos:

- Conocido. Son de los que tenemos constancia y podemos tomar medidas para evitarlos.
- Desconocidos (**0-day**). Son vulnerabilidades que aún no han sido reportadas al público y que un sistema actualizado (0-day) no puede detectar.

1.2.6. Alta disponibilidad

Disponemos de un sistema de **Alta Disponibilidad** cuando buscamos que el mismo esté accesible por el usuario durante 24 horas, 7 días a la semana, 365 días al año.

Figura: Alta Disponibilidad

Fuente: Propia

Para ello debemos tener en cuenta las paradas previstas de alguna parte del sistema, las imprevistas, cuánto tiempo vamos a tener detenida esa parte del sistema, qué medidas tenemos previstas para recuperar el sistema e informar al usuario de qué Grado de Disponibilidad tiene nuestro sistema. Todos los puntos de la imagen, los desarrollaremos detalladamente en el tema correspondiente.

Recursos y enlaces

Cosas Básicas de funcionamiento VirtualBox:

Objetivo: Repasar los conceptos básicos para poder crear una máquina Virtual en Oracle VirtualBox.

- https://youtu.be/Pj0nIAZ94Nk

Cosas básicas de VMWare Workstation 14:

Objetivo: Repasar los conceptos básicos para crear una máquina virtual en el programa VMWare Workstation.

- https://youtu.be/VFekWwZ3OLQ

Conectarnos a la Máquina Virtual:

Objetivo: El objetivo de este vídeo es repasar las formas de conectar tu ordenador con la máquina virtual para poder compartir información, tanto en Oracle Virtual Box como en VMWare Workstation.

- VMWare Workstation: https://youtu.be/6A88J7ccWLk
- Oracle VirtualBox: https://youtu.be/CeNQkWadHUs

Instalación de Kali Linux 2020

Objetivo: El objetivo de este video es preparar correctamente la máquina virtual de Kali Linux, la cual usarás durante buena parte del curso.

- https://youtu.be/uOvwZexYkcI

Instalación de Webmin

Objetivo: El objetivo de este video es instalar para cualquier distribución Linux el programa Webmin. Este programa es un gestor web del sistema operativo Linux, que nos permitirá aumentar nuestra productividad en este entorno ya que nos permite una gestión gráfica del mismo.

- https://youtu.be/dygXDlpwq0c

- Centro Criptológico Nacional https://www.ccn-cert.cni.es/

- Listado de Exploit https://www.exploit-db.com/

- Ingeniería Social: https://es.wikipedia.org/wiki/Ingeniería_social_(seguridad_informática)

Test de autoevaluación

1. El criterio de seguridad que me permite asegurarme de que mis fotos que voy a enviar a mi hermano no van a ser modificadas es:
   a) Confidencialidad
   b) Integridad
   c) Disponibilidad
   d) Autenticación

2. El criterio de seguridad que me permite asegurarme de que solamente yo puedo entrar en mi correo de Gmail es:
   a) Confidencialidad
   b) Integridad
   c) Disponibilidad
   d) Autenticación

3. El criterio de seguridad que me permite asegurarme de que puedo acceder a los apuntes del Módulo 11, a través de la web de Linkia, a las 22:00 h de un sábado es:
   a) Confidencialidad
   b) Integridad
   c) Disponibilidad
   d) Autenticación

4. Acabo de actualizar mi sistema operativo y he actualizado mis soluciones de seguridad, ¿estoy a salvo de vulnerabilidades?:
   a) Si, si no entras en páginas maliciosas
   b) Si, para eso tienes instalado un antivirus
   c) Si, durante 24 horas
   d) No, puedes tener una vulnerabilidad 0-day

Solucionarios

Test de autoevaluación

1. El criterio de seguridad que me permite asegurarme de que mis fotos que voy a enviar a mi hermano no van a ser modificadas es:
   a) Confidencialidad
   b) Integridad
   c) Disponibilidad
   d) Autenticación

2. El criterio de seguridad que me permite asegurarme de que solamente yo puedo entrar en mi correo de Gmail es:
   a) **Confidencialidad**
   b) Integridad
   c) Disponibilidad
   d) Autenticación

3. El criterio de seguridad que me permite asegurarme de que puedo acceder a los apuntes del Módulo 11, a través de la web de Linkia, a las 22:00 h de un sábado es:
   a) Confidencialidad
   b) Integridad
   c) **Disponibilidad**
   d) Autenticación

4. Acabo de actualizar mi sistema operativo y he actualizado mis soluciones de seguridad, ¿estoy a salvo de vulnerabilidades?:
   a) Si, si no entras en páginas maliciosas
   b) Si, para eso tienes instalado un antivirus
   c) Si, durante 24 horas
   d) No, puedes tener una vulnerabilidad 0-day