UNIVERSIDAD TECNOLOGICA DEL PERU

FITT Facultad de Ingeniería de Telecomunicaciones y Telemática

CONCEPTOS Y DEFINICIONES CLAVE EN CIBERSEGURIDAD Y CIBERDEFENSA

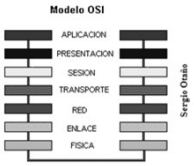
SEGURIDAD INFORMÁTICA

¿QUÉ ES?

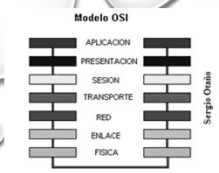
- ES EL ÁREA QUE SE ENCARGA DE LA PROTECCIÓN DE LAS INFRAESTRUCTURAS COMPUTACIONALES Y TODO LO RELACIONADO CON ÉSTAS, ASÍ COMO DE LA INFORMACIÓN CONTENIDA O CIRCULANTE.

¿PARA ELLO EXISTEN?

- ESTÁNDARES
- PROTOCOLOS
- MÉTODOS
- REGLAS
- HERRAMIENTAS
- LEYES



TODO ESTO CON LA FINALIDAD DE **REDUCIR LOS RIESGOS** A LAS INFRAESTRUCTURAS Y A LA INFORMACIÓN



Seg Info comprende el software, que incluye los programas y los datos, Y el hardware, que incluye todas las maquinas y redes

- **NO CONFUNDIR EL CONCEPTO DE SEG INFO CON EL DE SEG INFORMATICA, EL 1RO SE ENCARGA PROTECCION DE LA INFORMACION, ESTE O NO CONTENIDA EN LOS MEDIOS INFORMATICOS Y EL 2DO SOLO DE LA PROTECCION EN LOS MEDIOS INFORMATICOS**

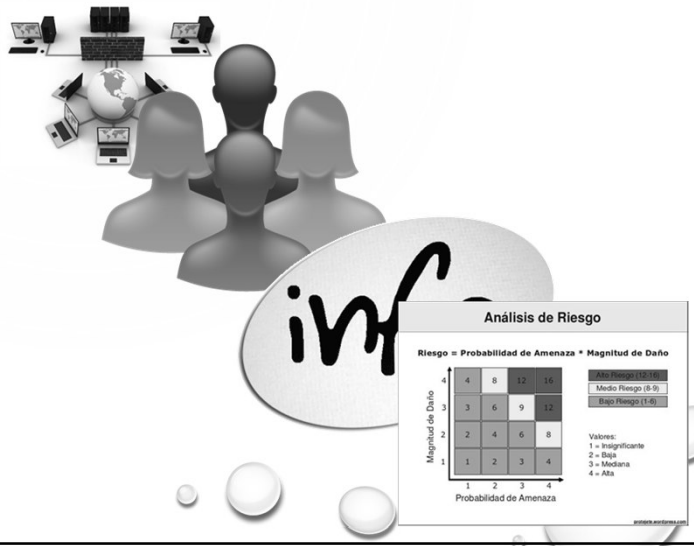
SEGURIDAD INFORMÁTICA VS. SEGURIDAD DE LA INFORMACIÓN

SEGURIDAD INFORMÁTICA

- Diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.
- Debe establecer **normas que minimicen los riesgos** a la información o infraestructuras informáticas
- Procurar un equilibrio entre la seguridad y la capacidad de trabajo u operatividad

¿QUÉ DEBE PROTEGER?

- La infraestructura computacional
  Asegurar Equipos Ok,Capac Anticip,respuesta a Incidencias
- Los usuarios
  Aseg Prot Info,el uso de ella,dependiendo del usuario
- La información
- Activo Princi org, debe Ana Riesgos que proteger
- Análisis de riesgos informáticos
  Proceso Identif :Activo Infot, vulnerab y amenazas-Fin detrminar control – disminuir,trasferir o evitar riesgos



SEGURIDAD DE LA INFORMACIÓN

- Tiene como objetivo preservar:
  - **Confidencialidad**: control de accesos autorizados a la información.
  - **Integridad**: Modificación no autorizada de la información.
  - **Disponibilidad**: Garantización del acceso autorizado.

Magister Miguel A. Del Pozo Matta

ESTRATEGIA DE SEGURIDAD

Gestión de la Seg busca establecer
Y mantener programas, controles y políticas, que tengan
Como finalidad conservar CIA, si falla una de estas el sistema No es seguro.

- Tienen como objeto el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo y que ayuden a proteger y salvaguardar la información y los sistemas
- La información es uno de los recursos principales de las organizaciones y su seguridad incide en la propia existencia de organización.
- La seguridad de la información se encarga de protegerla de una amplia gama de amenazas, a fin de garantizar la continuidad de la actividad, minimizar los daños y maximizar el retorno a la actividad.

Magister Miguel A. Del Pozo Matta

26/04/2019

CLASIFICACIÓN DE LAS AMENAZAS QUE AFECTAN A LA SEGURIDAD INFORMÁTICA

Pueden ser:

- Amenazas físicas
- Amenazas lógicas

Pueden estar producidas por:

- Las personas
- Programas específicos
- Catástrofes naturales

Magister Miguel A. Del Pozo Matta

TAMBIÉN SE PUEDE CLASIFICAR POR

Por su Intencionalidad.

- Accidentes: averías del hardware y fallos del software, incendio, inundación, etc...
- Errores humanos: errores de utilización, de explotación, de ejecución de procedimientos, etc...
- Actos antisociales: robos, fraudes, sabotajes, espionaje, etc...

Por su Origen.

- Amenazas naturales: inundación, incendio, tormenta, fallo eléctrico, explosión, etc...
- Amenazas de agentes externos: virus informáticos, ataques de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas, etc...

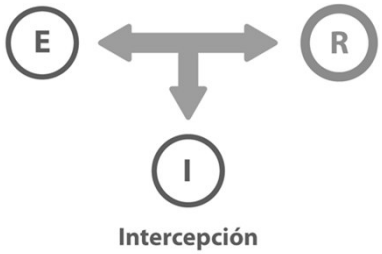
Magister Miguel A. Del Pozo Matta

26/04/2019

NATURALEZA DE LAS AMENAZAS

Interceptación: acceso a la información por parte de personas no autorizadas.

- Suele hacerse por medio de privilegios que no le corresponden al intruso y resulta muy difícil de detectar.
- Se mantienen la Integridad y la Disponibilidad, pero se pierde la Confidencialidad de la información, ya que alguien no autorizado está accediendo a ella.
- Ejemplos: las copias ilicitas de programas, la escucha en línea de datos.

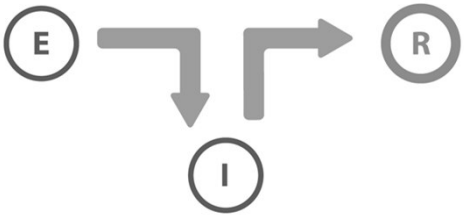


Intercepción

NATURALEZA DE LAS AMENAZAS

Modificación: es un acceso no autorizado utilizado para modificar el entorno o la información, con un objetivo ilícito.

- La detección es bastante compleja dependiendo de la forma de realización.
- Se mantiene la Disponibilidad, pero no se garantiza ni la Integridad, ni la Confidencialidad.
- Ejemplos: la modificación de bases de datos, modificación de elementos del Hardware.



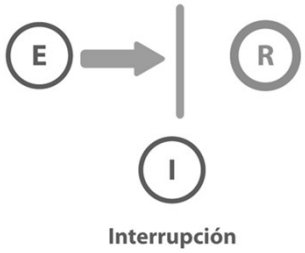
Modificación

Fabricación Falsa, en este caso se mantiene "C", xq nadie autorizado
Accede a la información, la "I" xq los datos enviados No se modifican en el camino
En el caso de trasmisiones, sin embargo la info puede ser manipulada. La "D" se mantiene.

NATURALEZA DE LAS AMENAZAS

Interrupción: puede provocar que un elemento del sistema se pierda o quede inutilizado o no disponible.

- La detección de este tipo de ataque es inmediata, ya que no se recibe lo que se esperaba.
- Se mantiene la Confidencialidad porque no hay accesos no autorizados a la información y también se mantiene la Integridad porque los datos no son modificados. Se pierde la Disponibilidad porque posiblemente la recepción no sea correcta o no exista, en el caso de las transmisiones.
- Ejemplos: la destrucción del hardware, el borrado de programas y/o datos, los fallos en el sistema operativo o inhibiciones de radio.



Interrupción

DEFINICIONES DE TIPOS DE ATAQUES Y AMENAZAS CIBERNÉTICAS

El principal objetivo de los ataques es la obtención de información, aunque existen otras motivaciones de distinta índole y resulta imprescindible la investigación y alerta continua, ya que continuamente aparecen nuevos métodos de ataque a los sistemas computacionales y hay que implementar las contramedidas lo antes posible para evitar males mayores.

TIPOS DE ATAQUES Y AMENAZAS CIBERNÉTICAS

La propagación de virus informáticos:

- Los Virus Informáticos son programas maliciosos, que infectan a otros archivos del sistema con la intención de modificarlo o dañarlo.
- Consiste en la inserción de código malicioso en el interior de un archivo víctima, que casi siempre es un programa ejecutable, de forma que este pasa a ser portador del virus y por tanto, una nueva fuente de infección.

TIPOS DE ATAQUES Y AMENAZAS CIBERNÉTICAS

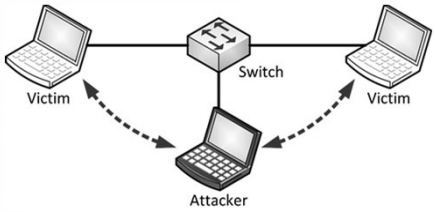
El envió masivo de correo no deseado o SPAM:

- Se llama Spam a los mensajes no solicitados, no deseados, de remitente no conocido, casi siempre con publicidad y enviados en grandes cantidades. Perjudican de alguna o varias maneras al receptor. La forma más utilizada entre el público en general es a través del correo electrónico.
- El correo basura puede tener objetivo los teléfonos móviles, atraves de SMS y/o whatsapp.
- Los spammers pueden ser individuos o empresas y utilizan diversas técnicas para conseguir largas listas de direcciones de correo de victimas.

TIPOS DE ATAQUES Y AMENAZAS CIBERNÉTICAS

La suplantación de los Remitentes de mensajes con la técnica Spoofina:

- Por spoofing se conoce a la creación de tramas TCP/IP utilizando una dirección IP falseada; la idea de este ataque es muy sencilla, aunque no es fácil llevarlo a cabo:
- Un atacante simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado.



TIPOS DE ATAQUES Y AMENAZAS CIBERNÉTICAS

El envió o instalación inconsciente de archivos espías o Kevloggers:

- Un Keylogger es un programa que registra y graba la pulsación de teclas y algunos también los clicks del ratón. La información obtenida será utilizada después por el atacante. Se puede hacer por software y por hardware.