Seguridad de la Información

Una introducción con enfoque práctico

Ing. Mariano Aliaga

Universidad Católica de Córdoba - Facultad de Ingeniería

2021

Panorama General

1. Presentación Materia
   - Objetivos
   - Contenidos
   - Aprobación
   - Material de estudio
2. Definiciones y Conceptos
   - Definiciones Seguridad de la Información
   - Conceptos y terminología
   - Dificultades de la Seguridad de la Información
   - 4 Virtudes de la Seguridad
   - 8 Reglas de la Seguridad

Objetivos

- Conocer un panorama general de la Seguridad de la Información.
- Desarrollar las habilidades prácticas para llevar a cabo tareas relacionadas con la Seguridad de la Información.
- Desarrollar una “mente segura”.
- Conocer tecnologías y herramientas Open Source para su aplicación en SI y otras áreas.

Contenidos

- **UNIDAD I:** Introducción a la Seguridad de la Información (SI)
- **UNIDAD II:** Conceptos básicos necesarios para la SI
- **UNIDAD III:** Criptografía
- **UNIDAD IV:** Seguridad en Redes
- **UNIDAD V:** Seguridad en Sistemas Operativos
- **UNIDAD VI:** Seguridad en Aplicaciones

Aprobación

- 2 Parciales
- Trabajos prácticos presentados en Moodle
- 1 Final
- Seguridad Información (Ing. Aliaga)
  AND
  Auditoría Informática (Ing. Pardo)
- Promedio entre ambas

Material de estudio

- **Campus Virtual UCC:** `http://campusvirtual.ucc.edu.ar/`
- **COLE, Eric.** *Hackers Beware.* New Riders Publishing. 2001.
- **DAY, Kevin**. *Inside the Security Mind: Making the Tough Decisions.* Prentice Hall. 2003
- **GRAVES, Kimberly.** *CEH Official Ethical Hacker Review Guide.* Wiley Publishing. 2007
- **LUCENA LÓPEZ, Manuel J.**. *Criptografía y Seguridad en Computadores*. `https://www.u-cursos.cl/ingenieria/2010/2/EL65C/1/material_docente/bajar?id_material=311979`
- **RAMIÓ AGUIRRE, Jorge.** *Libro Electrónico de Seguridad Informática y Criptografía.* Universidad Politécnica de Madrid. `http://www.criptored.upm.es/guiateoria/gt_m001a.htm`
- **SKOUDIS, Ed - LISTON, Tom.** *Counter Hack Reloaded, Second Edition: A Step-by-Step Guide to Computer Attacks and Effective Defenses.* Prentice Hall. 2005.

Definiciones de Seguridad de la Información

Diversos enfoques

1. Conjunto de medidas de protección
2. Control de accesos: mantener el control, protegerse de ataques
3. Preservación de la tríada CID: Confidencialidad, Integridad, Disponibilidad
4. Existencia de un estado: invulnerabilidad, protección

Ejemplos de Definiciones

Seguridad como conjunto de medidas

NIST Glossary: "La protección de la información y sistemas de información de acceso no autorizado, uso, difusión, disrupción, modificación o destrucción, a fines de proporcionar confidencialidad, disponibilidad e integridad."

Ejemplos de Definiciones

Seguridad como control de accesos

William R. Cheswick: "Hablando ampliamente, la seguridad es evitar que alguien haga cosas que no quieres que haga con o desde tu ordenador o alguno de sus periféricos"

Ejemplos de Definiciones
Seguridad como preservación de CID

ISO17799: "La seguridad de la información se puede caracterizar por la preservación de la confidencialidad, integridad y disponibilidad (CID)."

- **Confidencialidad:** Capacidad de proporcionar acceso a usuarios autorizados, y negarlo a no autorizados.
  - Identificación
  - Autenticación
  - Autorización
  - Auditoría
  - No repudio
- **Integridad:** Capacidad de garantizar que una información o mensaje no han sido manipulados o alterados y de que los servicios procesan correctamente la información.
- **Disponibilidad:** Capacidad de acceder a información o utilizar un servicio siempre que lo necesitemos.

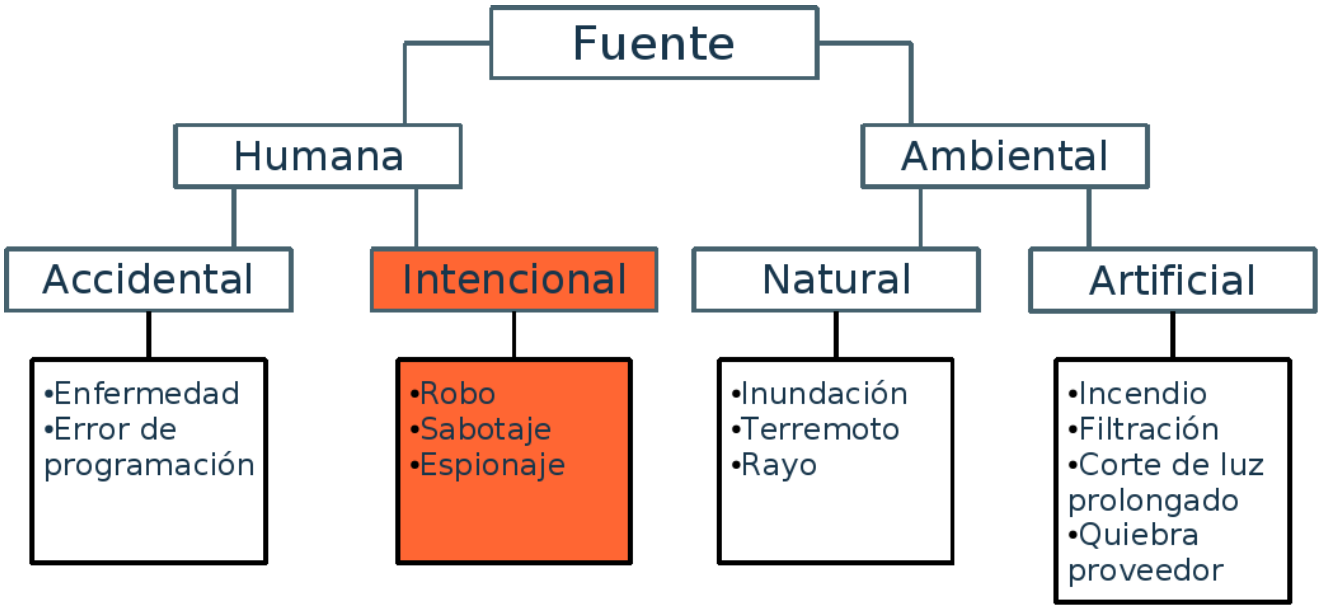
Ejemplos de Definiciones

Seguridad como existencia de un estado

Gene Spafford: "El único sistema verdaderamente seguro es aquel que se encuentra apagado, encerrado en una caja fuerte de titanio, enterrado en un bloque de hormigón, rodeado de gas nervioso y vigilado por guardias armados y muy bien pagados. Incluso entonces, yo no apostaría mi vida por ello."

Conceptos y terminología

- **Activos (qué se protege?):** recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.
- **Amenaza (de qué se protege?):** es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

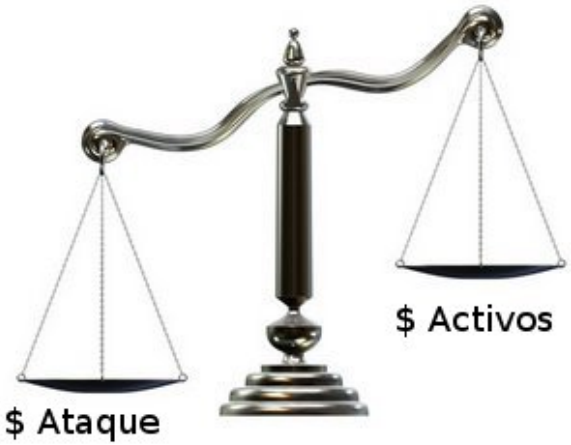


Conceptos y terminología

- **Vulnerabilidad:** es una debilidad que influye negativamente en un activo y que posibilita la materialización de una amenaza.
- **Exposición:** una exposición innecesaria de información que puede utilizarse para llevar a cabo un ataque.
- **Exploit:** es una pieza de software, un grupo de datos o una secuencia de comandos que aprovechan una falla o vulnerabilidad para causar un comportamiento no deseado o imprevisto en sistemas de software o hardware.
- **Ataque:** evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
- **Incidente (ataque exitoso):** acceso, uso, divulgación, modificación o destrucción no autorizada de información; impedimento en la operación normal de las redes, sistemas o recursos informáticos.
- **Defensa:** conjunto de productos, medidas y procesos tendientes a evitar la concreción de un incidente.
- **Riesgo:** es la probabilidad de que suceda la amenaza o evento no deseado.
- **Impacto:** medir la consecuencia al materializarse una amenaza.

Dificultades de la Seguridad de la Información

- No existe sistema 100% seguro
- Equilibrio Usabilidad Vs. Seguridad
- Eslabón más débil
- No es un problema únicamente tecnológico
- La SI debe ser un proceso



4 Virtudes de la SI

1. Consideración diaria
2. Esfuerzo comunitario
3. Foco generalizado
4. Educación para todos

4 Virtudes de la SI

Consideración diaria

Lo que NO hay que hacer:

1. Hacer algo sin pensar en la Seguridad
2. Sufrir un incidente de seguridad
3. Descubrir que lo que se hizo en el **Paso 1** introdujo una vulnerabilidad que permitió la ocurrencia del **Paso 2**.
4. Asegurar la organización contra el ataque específico del **Paso 2**.
5. Esperar
6. Tener un incidente de nuevo
7. Darse cuenta de que mientras se esperaba en el **Paso 5**, otro nuevo ataque se llevó a cabo relacionado a lo que se hizo en el **Paso 1**.

4 Virtudes de la SI

Consideración diaria

Lo que SÍ hay que hacer:

1. Pensar en la seguridad
2. Hacer algo (mientras se sigue pensando en seguridad)
3. Continuar pensando en seguridad

Podemos evitar la vasta mayoría de incidentes de seguridad haciendo de ésta una **consideración diaria**.

4 Virtudes de la SI

Consideración diaria

Prácticas Recomendadas

- Hacer de la seguridad un pensamiento continuo
- Promocionar en otros este pensamiento continuo
- Incluir formalmente la seguridad en todo nuevo proyecto
- Incluir formalmente la seguridad en toda nueva implementación

4 Virtudes de la SI

Esfuerzo comunitario

Comunidad de seguridad **INTERNA**

- La seguridad no puede ser lograda por profesionales de la seguridad solos
- Nuestro rol debe ser el de integrar a los usuarios finales en las prácticas de seguridad locales

Comunidad de seguridad **EXTERNA**

- Organizaciones con buenas prácticas de seguridad se ven afectadas por la falta de seguridad de otras.
- La mayoría de los ataques a sistemas "no importantes" se utilizan para lanzar ataques a otras organizaciones
- Nuestro rol: mantenernos seguros para que los otros estén seguros de nosotros.

Las buenas prácticas de seguridad requieren un **esfuerzo comunitario** donde todos cumplan su parte para proteger sus propios sistemas.

4 Virtudes de la SI

Esfuerzo comunitario

Prácticas Recomendadas

- Mantenerse informado
- Informar a los otros
- Mantenerse actualizado
- Informar a los usuarios finales
- Tomar decisiones en equipo

4 Virtudes de la SI

Foco generalizado

... En el mundo de la SI, hay miles de vulnerabilidades explotables por decenas de miles de ataques con virtualmente millones de permutaciones posibles ...

La seguridad es muy dinámica, y requiere **métodos elevados de pensamiento**.

4 Virtudes de la SI

Foco generalizado

Prácticas Recomendadas

- Aprender y compartir los conceptos detrás de las virtudes y reglas de la SI
- Pensar en términos de la "vista panorámica"
- Definir documentos escritos con políticas de alto nivel

4 Virtudes de la SI

Educación para todos

Si la seguridad va a ser un **trabajo diario**, un **esfuerzo comunitario**, y considerado en **todo**, entonces **todos** deben estar envueltos en algún grado en las prácticas de seguridad. Por lo tanto, todos los implicados deben tener algún nivel de **educación en seguridad**.

- Podemos transformar al usuario final de ser un riesgo de seguridad, a un colaborador en mantener la seguridad del entorno
- No existe una solución "tecnológica" que no pueda ser deshecha por un grupo de usuarios finales no entrenados, no informados o no cooperativos.

4 Virtudes de la SI

Educación para todos

Prácticas Recomendadas

- Buenas prácticas de instalación de software
- Buena práctica de reconocimiento de eventos “sospechosos”
- Buenas prácticas de navegación
- Buenas prácticas de confidencialidad
- Explicar conceptos de seguridad a empleados en forma permanente

8 Reglas de la SI

1. Regla del menor privilegio
2. Regla de los cambios
3. Regla de la confianza
4. Regla del eslabón más débil
5. Regla de la separación
6. Regla del proceso de tres etapas
7. Regla de la acción preventiva
8. Regla de la respuesta inmediata y adecuada

8 Reglas de la SI

Regla del menor privilegio

Permita sólo el acceso requerido para hacer el trabajo, y **nada más**. Es la única forma en que podemos estar seguros de que sabemos *quién* tiene *acceso* a *qué*, y *por qué*.

- **Sujeto:** la persona, lugar o cosa que obtiene el acceso. (Quién?)
- **Objeto:** la persona, lugar o cosa a la cual el sujeto obtiene acceso. (A qué?)
- **Acceso:** el nivel o grado de acceso dado al sujeto. (Cómo?)
- **Contexto:** la situación o circunstancias que rodean al acceso. (Cuándo? Por qué?)

8 Reglas de la SI

Regla del menor privilegio

Prácticas Recomendadas

- Crear todas las políticas de seguridad desde el punto de vista del mínimo privilegio.
- Siempre comenzar por negar todo.
- Evaluar si el sujeto realmente necesita acceso al objeto y bajo qué circunstancias.

8 Reglas de la SI

Regla de los cambios

Los cambios deben ser administrados, coordinados y deben considerarse las posibles implicancias de seguridad.

- Los cambios sólo deberían ocurrir después de que se ha probado que sean seguros.
- Los cambios deberían ser consistentes y no introducir demasiada diversidad.
- Sólo deberían poder realizar cambios quienes estén calificados para ello (mínimo privilegio).

8 Reglas de la SI
Regla de los cambios

Prácticas Recomendadas

- Implementar el control de cambios.
- Controlar cambios de seguridad.
- No implementar un producto hasta que haya sido correctamente probado.
- Estandarizar las tecnologías a utilizar.

8 Reglas de la SI
Regla de la confianza

Un buen practicante de la seguridad es alguien que es amigo de todos... pero que en realidad no confía en nadie.

- Aplicar el principio de mínimo privilegio: sólo confiar en aquello que es necesario.
- Aplicar distintos "niveles de confianza" según sea necesario.

8 Reglas de la SI
Regla de la confianza

Prácticas Recomendadas

- Recordar que cualquiera puede ser el enemigo, incluso uno mismo!
- No confiar en nada que esté fuera de nuestro control.
- Tener en cuenta de las derivaciones de confiar en algo o alguien.
- Crear políticas globales que vayan más allá de los niveles de confianza.

8 Reglas de la SI

Regla del eslabón más débil

Una cadena es tan fuerte como su eslabón más débil... Una práctica de seguridad es sólo tan fuerte como su control más débil.

- Instalaciones por defecto
- Malas contraseñas
- Modems activos en equipos de la red
- Falta de monitoreo y control de logs
- Servidores o equipos temporales
- Backups descuidados o no probados
- Aplicaciones no autorizadas
- Antivirus desactualizado

8 Reglas de la SI

Regla del eslabón más débil

Una cadena es tan fuerte como su eslabón más débil... Una práctica de seguridad es sólo tan fuerte como su control más débil.

- Instalaciones por defecto
- Malas contraseñas
- Modems activos en equipos de la red
- Falta de monitoreo y control de logs
- Servidores o equipos temporales
- Backups descuidados o no probados
- Aplicaciones no autorizadas
- Antivirus desactualizado

8 Reglas de la SI

Regla del eslabón más débil

Prácticas Recomendadas

- Buscar el "eslabón más débil" en forma continua.
- Documentar dónde existen debilidades de seguridad.
- Evitar la introducción de nuevos eslabones débiles.

8 Reglas de la SI
Regla de la separación

Para asegurar algo, ésto debe estar separado de los peligros y amenazas del mundo que lo rodea.

- Las fortalezas y debilidades de un objeto están normalmente relacionadas con las tareas que dicho objeto lleva a cabo.
- Cada servicio tiene su propia "sensibilidad" a la seguridad. Cuidado al combinarlos!

8 Reglas de la SI
Regla de la separación

Prácticas Recomendadas

- Aislar servicios y datos importantes.
- Aislar servicios que son más propensos a ataques.
- Aislar todos los “servicios de seguridad”.
- Sólo agrupar servicios basados en factores comunes de seguridad.

8 Reglas de la SI

Regla del proceso de tres etapas

Toda medida de seguridad debe ser pensada como un proceso de tres etapas: implementación, monitoreo y mantenimiento.

- **Implementación:** realizamos un análisis, diseñamos una solución, adquirimos las herramientas, lo construimos, lo probamos y ponemos en producción.
- **Monitoreo:** no existe la "seguridad completamente automatizada".
- **Mantenimiento:** cualquier dispositivo de seguridad sin actualizaciones por un tiempo prolongado fallará en reconocer nuevos ataques.

8 Reglas de la SI

Regla del proceso de tres etapas

Prácticas Recomendadas

- Considerar la regla del proceso de tres etapas desde un comienzo.
- Asegurarse de que existan controles de registros y monitoreo.
- Mantenerse actualizado.

8 Reglas de la SI

Regla de la acción preventiva

La seguridad sólo puede ser exitosa si se enfrenta con un enfoque proactivo.

- Es una tendencia humana el tener respuestas "reactivas" en la mayoría de las situaciones.
- Muchas veces se consideran las medidas proactivas una pérdida de tiempo o distracción.
- La proactividad "no vende".

8 Reglas de la SI

Regla de la acción preventiva

Prácticas Recomendadas

- Mantenerse informado de los temas de seguridad actuales.
- Realizar pruebas periódicas en dispositivos de seguridad.
- No quedarse sólo con los problemas más comunes.

8 Reglas de la SI

Regla de la respuesta inmediata y apropiada

Se debe contar con un plan organizado de cómo responder a un ataque, analizar los riesgos pendientes y planificar los pasos futuros.

- Los pasos que demos luego de un ataque son tan importantes como los que dimos para evitarlo.
- Se debe estar preparado con anterioridad para reaccionar correctamente.

8 Reglas de la SI

Regla de la respuesta inmediata y apropiada

Prácticas Recomendadas

- Desarrollar un buen plan de respuesta de incidentes.
- Tener una "cadena de mando" bien definida para estas circunstancias.
- Reaccionar rápidamente.
- Hacer un seguimiento del incidente.

Más información

- **IETF**. RFC 2828*: Internet Security Glossary*. `http://www.ietf.org/rfc/rfc2828.txt`
- **Wikipedia**. *Seguridad Informática*. `http://es.wikipedia.org/wiki/Seguridad_informática` `http://en.wikipedia.org/wiki/Information_security`
- **NIST.** *Glossary of Key Information Security Terms*. `https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf`
- **Schneier, Bruce**. *Computer Security: Will We Ever Learn?*. `http://www.schneier.com/crypto-gram-0005.html`
- **DAY, Kevin**. *Inside the Security Mind: Making the Tough Decisions.* Capítulos 3 y 4.