

PRIMERA UNIDAD DE APRENDIZAJE

CAPÍTULO 1: FUNDAMENTOS DE SEGURIDAD DE LA INFORMACIÓN

1.1. SEGURIDAD DE LA INFORMACIÓN

Se denominan **seguridad de la información** a la capacidad de la organización para proteger sus activos de información (servicios, datos, aplicaciones, equipos informáticos, redes de comunicación, soporte, instalaciones, etc.) de riesgos y ataques, para ello se implementa un conjunto de métodos, técnicas, procesos, etc., que trabajan de manera preventiva o reactiva.

El propósito de la seguridad en cualquier ámbito de aplicación es reducir riesgos hasta un nivel aceptable que permita mitigar amenazas latentes. En un sentido amplio, por seguridad también se entienden todas aquellas actividades destinadas a proteger de algún tipo de peligro o amenaza.

Ya que lo que se desea proteger es la información, hay que observar que ésta puede encontrarse en forma digital (archivos en medios electrónicos u ópticos), en forma física (escrita o impresa), también de manera no representada (ideas o conocimiento) por ello hay que observar que los activos de información pueden encontrarse en distintas formas.

Además, la información debe ser almacenada, procesada o transmitida de diferentes formas: formato electrónico, de forma verbal o a por mensajes impresos, entonces existe en diferentes estados.

La información requiere de medidas de protección adecuadas de acuerdo con su importancia y criticidad, y éste es precisamente el ámbito de la seguridad de la información. La seguridad en cómputo se limita a la protección de los sistemas y equipos que permiten el procesamiento de la información, mientras que la seguridad informática involucra métodos, procesos o técnicas para el tratamiento automático de la información en formato digital, teniendo un alcance mayor, ya que incluye la protección de las redes e infraestructura tecnológica.

Por ejemplo y con base en las definiciones, cuando se busca proteger el hardware, redes, software, infraestructura tecnológica o servicios, nos encontramos en el ámbito de la **seguridad informática** o ciberseguridad. Cuando se incluyen actividades de seguridad relacionadas con la información que manejan las personas, seguridad física, cumplimiento o concientización nos referimos a **seguridad de la información**.

Hay también que establecer diferencias entre ciberseguridad y seguridad de la información. La ciberseguridad se define “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados” (ISAKA). La norma ISO 27001 define activo de información como los conocimientos o datos que tienen valor para una organización, mientras que los sistemas de información comprenden a las aplicaciones, servicios, activos de tecnologías de información u otros componentes que permiten el manejo de la misma.

Por lo tanto, la ciberseguridad tiene como foco la protección de la información digital que se maneja dentro de los sistemas interconectados y está comprendida dentro de la seguridad de la información. Resulta entonces que la seguridad de la información tiene un alcance mayor que la ciberseguridad, puesto que la primera busca proteger la información de riesgos que puedan afectarla, en sus diferentes formas y estados.

Por el contrario, la ciberseguridad se enfoca principalmente en la información en formato digital y los sistemas interconectados que la procesan, almacenan o transmiten, por lo que tiene un mayor acercamiento con la seguridad informática.

La seguridad de la información se basa en metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos, que soportan la protección en las distintas facetas de la información, por lo que involucra la aplicación y gestión de medidas de seguridad apropiadas, a través de un enfoque global.

Se denominan **sistemas críticos** a aquellos en los que un fallo o mal funcionamiento ocasionaría consecuencias graves en el entorno en el que está trabajando, tanto humanas, económicas o materiales (por ejemplo: desfibriladores cardíacos, sistemas de control de aviónica, sistemas de control de las plantas de energía nuclear o de productos químicos, sistemas de frenos de los automóviles, etc.).

Los sistemas críticos deben tener aseguradas las siguientes **propiedades**:

- Confiabilidad sobre el sistema, su infraestructura y su funcionalidad
- Disponibilidad, asegurándose que el sistema esté activo y funcionando en todo momento.
- Fiabilidad, durante un periodo de tiempo mínimo y predefinido, el sistema debe funcionar correctamente tal como se espera.
 - Corrección en el nivel de detalle preciso proporcionado al usuario.
 - Precisión al proveer la información cuando esta es requerida.
- Seguridad al interactuar con los usuarios y el medio que lo rodea.
- Protección, porque debe ser capaz de soportar ataques e intrusiones premeditadas o accidentales, para ello el sistema debe:
 - Integridad sobre los datos y la información que maneja el sistema
 - Permitir acceso solo a usuarios autorizados para acceder y modificar la información.
 - Garantizar la autenticación de los usuarios para implementar acciones de auditoria.
- Mantenimiento, tanto en su forma preventiva como correctiva, se deben conocer las condiciones que lo ameritan y el tiempo que el proceso demore.

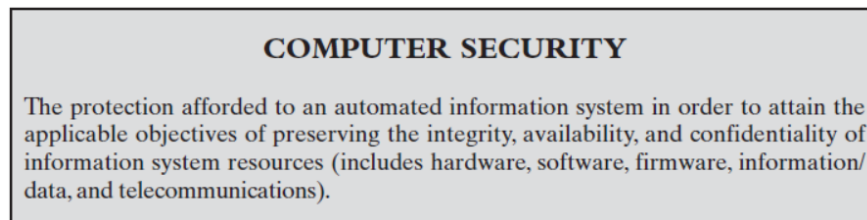
La seguridad informática, ciberseguridad o seguridad de tecnologías de la información, es la disciplina que se encarga del manejo de la seguridad en los sistemas, la que contempla tanto el hardware (infraestructura computacional) y software (la información, bases de datos, metadatos, archivos). Para ello se han desarrollado estándares, protocolos, métodos, metodologías, algoritmos y leyes cuyo objetivo es minimizar los posibles riesgos. Sin embargo, la seguridad informática no garantiza por sí sola la seguridad de la información. Las implantaciones de este tipo de herramientas se traducen en un Sistema de Gestión de Seguridad de la Información SGSI, el que debe considerar al menos los cinco tópicos propuestos en la ISO27001:2013

- a. Sistema de toma de decisiones
- b. Sistema de gestión de riesgos
- c. Sistema de monitoreo
- d. Sistema de gestión de proyectos
- e. Sistema de gestión documental

Como la mayoría de ataques y riesgos proviene del exterior de las organizaciones, la seguridad de los sistemas depende fundamentalmente de la seguridad en la red, por lo que la mayor parte del curso aborda el problema del aseguramiento en este sentido. El punto de partida en el análisis de la seguridad es la capacidad de identificar de donde pueden venir las amenazas, la mayoría de ellas proviene de:

- Usuarios
- Programas maliciosos (virus, gusanos, troyano, bomba lógica, spyware o malware)
- Errores de programación usados como exploits.
- Intrusos (crackers, defacers, hackers, script kiddie o script boy, viruxers, etc.).
- Un siniestro o catástrofe natural
- Personal técnico interno
- Fallos electrónicos

NIST *Computer Security Handbook*, define el término *computer security*, de la siguiente manera



Esta definición implica que hay tres factores claves en la seguridad computacional o informática en torno a los cuales se han desarrollado todo un conjunto de definiciones y recomendaciones (FIPS 199), que deben aplicarse en la etapa de definición de requerimientos del sistema

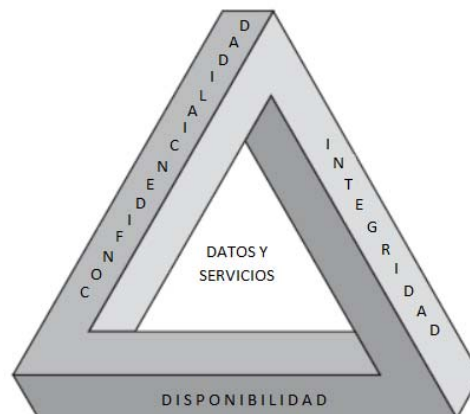


Figura 1.1. Atributos de la seguridad


- ✚ **Confidencialidad:** preservar las restricciones autorizadas sobre la información, acceso y divulgación, incluyendo medios para proteger la privacidad personal y la información de propiedad. Una pérdida de confidencialidad es la divulgación no autorizada de información.
- ✚ **Integridad:** es proteger contra la modificación o destrucción indebida de la información, incluyendo la garantía de no rechazo y autenticidad de la información. Una pérdida de integridad es la modificación no autorizada o la destrucción de información.

- ✚ **Disponibilidad:** garantizar el acceso oportuno y fiable a la información y su uso. Una pérdida de disponibilidad es la interrupción del acceso o el uso de información o un sistema de información.

Adicionalmente a ellos también es importante definir requerimientos en torno a:

- ✚ **Autenticidad:** garantizando que la información sea genuina y que esta pueda ser verificada y de confianza; así como la confianza en la validez de la transmisión de un mensaje o la fuente del mismo. Esto significa verificar que los usuarios son quienes dicen ser y que cada entrada que llega al sistema proviene de una fuente confiable.
- ✚ **Rendición de cuentas:** la meta de seguridad genera el requisito de que las acciones de una entidad se rastreen exclusivamente a esa entidad. Esto apoya el no rechazo, la disuasión, el aislamiento de fallas, la detección y prevención de intrusiones, y la recuperación después de la acción y la acción legal. Debido a que los sistemas verdaderamente seguros todavía no son un objetivo alcanzable, debemos ser capaces de rastrear una violación de seguridad a una parte responsable. Los sistemas deben mantener registros de sus actividades para permitir análisis forenses posteriores para rastrear infracciones de seguridad o para ayudar en disputas de transacción.

Existen tres **tipos** fundamentales de sistemas críticos

- Sistemas de seguridad críticos:** son sistemas cuyo mal funcionamiento puede provocar pérdidas de vida o generar un grave daño al medio ambiente en el tiempo, por ejemplo: el sistema de control de fabricación de algún producto químico
- Sistemas de misión críticos:** son sistemas cuyo mal funcionamiento puede provocar errores en algunas actividades dirigidas por objetivos, por ejemplo: el sistema de navegación de una nave espacial
-  **Sistemas de negocios críticos:** son sistemas cuyo mal funcionamiento puede provocar costes elevados para el negocio que lo utiliza, por ejemplo: un sistema de cuentas bancarias

Según FIPS PUP 199, los costos de los ataques pueden ser de tres niveles:

- **Bajo:** si la pérdida tiene un efecto adverso limitado sobre la organización, sus operaciones, activos organizacionales o individuos, lo que significa que la pérdida de confidencialidad, integridad o disponibilidad podría (i) provocar una degradación en la capacidad de la misión en una medida y duración tal que la organización sigue desempeñando funciones primarias, pero otras funciones se reducen notablemente; (ii) dar lugar a daños menores en los activos organizacionales; (iii) dar lugar a pérdidas financieras menores; o (iv) resulte en menor daño a las personas.
- **Moderado:** la pérdida podría tener un efecto grave en las operaciones de la organización, los activos de la organización o los individuos. La pérdida podría (i) provocar una degradación significativa de la capacidad de la misión en la medida y en la duración que la organización pueda desempeñar sus funciones primarias, pero la eficacia de las funciones se reduce considerablemente; (ii) resultar en un daño significativo a los activos de la organización; (iii) dar lugar a pérdidas financieras significativas; o (iv) resultar en un daño significativo a las personas, pero sin pérdida de vidas o lesiones serias y mortales.
- **Alto:** la pérdida tiene un efecto adverso severo en las operaciones de la organización, los activos de la organización o los individuos. La pérdida podría (i) provocar una grave pérdida de la capacidad de la misión en una extensión y duración que la

organización no pueda llevar a cabo una o más de sus funciones primarias; (ii) resultar en un daño importante a los activos de la organización; (iii) dar lugar a pérdidas financieras importantes; o (iv) resultar en daño severo a personas que implican pérdida de vidas o lesiones serias y potencialmente mortales.



Trabajo de investigación formativa 1.

En grupos de tres alumnos presentar una revisión de la siguiente normativa sobre seguridad:

NTP-ISO/IEC 17799, ISO 27000, ISO 27001, ISO 27002, ISO 27003, ISO 27004, ISO 27005, ISO 27006, ISO 27799

1.2. ATRIBUTOS DE LA SEGURIDAD: CONFIABILIDAD, INTEGRIDAD Y DISPONIBILIDAD

1.2.1 Confiabilidad

La IEEE define confiabilidad como la “habilidad de un sistema o componente de realizar las funciones requeridas bajo condiciones específicas en periodos de tiempo determinados”

El término “**confiabilidad**” fue propuesto por Laprie (1995) y depende de los atributos relacionados con sistemas de **disponibilidad, fiabilidad**, protección o mantenimiento y seguridad. Dichas propiedades están vinculadas, así que tiene sentido disponer de un solo término para tratarlas a todas.

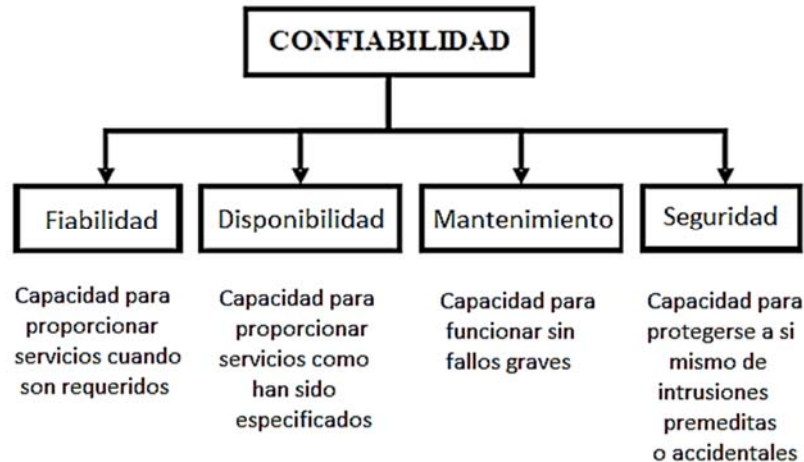


Figura 1.2. Atributos de la confiabilidad (Sommerville)

1. **Fiabilidad**: es la probabilidad, durante un tiempo determinado, de que el sistema brindará correctamente servicios como espera el usuario. La que considera los campos de:
 - **Disponibilidad**: condición de trabajo que el sistema debe tener al ser encendido luego de una parada de mantenimiento.
 - **Mantenibilidad**: relacionado con que al ser apagado para **mantenimiento el sistema** volverá a su condición de trabajo dentro de un periodo específico.
 - **Reparabilidad**: probabilidad de fallo del sistema y que **pueda ser reparado bajo condiciones y periodos específicos de tiempo**.

2. **Disponibilidad:** es la probabilidad de que en un momento dado éste funcionará, ejecutará y ofrecerá servicios útiles a los usuarios.
3. **Mantenimiento o Protección:** cuán probable es que el sistema causará daños a las personas o su ambiente, ello implica el prever que el sistema falle de manera inmediata. Dentro de sus dimensiones están:
 - **Disponibilidad:** habilidad de entregar el servicio solamente a usuarios autorizados, previstos en las especificaciones, cumple el mismo rol que la disponibilidad como atributo de confiabilidad.
 - **Confidencialidad:** habilidad de negar el servicio a usuarios no autorizados.
4. **Seguridad:** cuán probable es que el sistema pueda resistir intrusiones accidentales o deliberadas. A su vez la seguridad tiene los siguientes campos asociados:
 - Confidencialidad: prevención de la divulgación no autorizada de la información.
 - Integridad: prevención de cualquier modificación de la información de manera que no sea autorizada.
 - Disponibilidad: prevención de la retención no autorizada de la información.
 - Autenticación: todas las personas, programas y sistemas deben ser previamente identificados.
 - Sin desconocimiento: los mensajes recibidos deben de provenir realmente de personas, programas o sistemas emisores aparentes.

No todas esas propiedades o atributos de la confiabilidad son aplicables a todos los sistemas o tienen la misma influencia, por ejemplo, si se considera un sistema de bomba de insulina, las propiedades más importantes son la disponibilidad, la fiabilidad y la protección, sin embargo, la seguridad no es importante porque la bomba no tiene información confidencial o no puede ser atacada de manera maliciosa. Sin embargo, para un sistema meteorológico a campo abierto, la disponibilidad y fiabilidad son las propiedades más importantes, porque los costos de reparación suelen ser muy altos. Mientras que, para un sistema de información de pacientes, la seguridad es importante, porque se deben mantener los datos de manera privada.

Además de estas cuatro propiedades básicas de la confiabilidad, también se pueden considerar:

5. **Reparabilidad:** las fallas son inevitables, pero se minimizan si el sistema se repara rápidamente (diagnosticar, acceder al componente y corregir). La reparabilidad en software requiere que la organización tenga acceso al código fuente (difícil si se reutiliza componentes)
6. **Mantenibilidad:** el uso constante genera nuevos requerimientos y se requieren cambio para satisfacerlos. El software mantenible es aquel que económicamente se adapta para lidiar con los nuevos requerimientos, y donde existe una baja probabilidad de que los cambios insertarán nuevos errores en el sistema.
7. **Supervivencia:** habilidad de un sistema para continuar entregando servicio en tanto está bajo ataque y mientras que, potencialmente, parte del sistema se deshabilita. El trabajo sobre supervivencia se enfoca en la identificación de los componentes clave del sistema y en la garantía de que ellos puedan entregar un servicio mínimo. Para mejorar la supervivencia se usan tres estrategias:
 - resistencia al ataque
 - reconocimiento del ataque

- recuperación del daño causado por un ataque.
8. Tolerancia *para el error*: propiedad parte de la usabilidad y refleja el diseño del sistema para evitar y tolerar los errores de entrada de usuario. Cuando ocurren errores de usuario, el sistema debe detectar dichos errores y corregirlos automáticamente o solicitar al usuario que reintroduzca sus datos.

La confiabilidad no es fácil de cuantificar porque depende de muchos factores que determinan el buen funcionamiento de sus atributos, sin embargo, hay dos maneras de **cuantificar** la confiabilidad:

- + Predicción de la confiabilidad: se realiza mediante un lineamiento de la evaluación segura del programa y fácilmente medible sobre las propiedades del código. Estos modelos de predicción están basados en acercamientos relativos que en un futuro asegurarán la eficiencia, de manera semejante a los modelos de predicción de confiabilidad del hardware
- + Estimación de la confiabilidad: son modelos utilizados para realizar la estimación se basan en la estimación de las tasas de fallos

En el caso del software los fallos o averías tienen un origen interno, aunque su manifestación es externa, dentro de los **tipos de fallos** tenemos

- Fallos transitorios: desaparecen luego de un tiempo
- Fallos permanentes: no desaparecen hasta la reparación
- Fallos intermitentes: fallos transitorios con cierta periodicidad

La presencia de estos fallos degrada la confiabilidad del sistema, por lo que deben desarrollarse **acciones para evitarlos**, estas acciones pueden ser:

- ✓ Prevención de fallos: evitarlos en el proceso de construcción
 - Evitar fallos: durante el diseño
 - Eliminar fallos: en el sistema ya construido ejecutar correcciones
- ✓ Tolerancia a fallos: aunque los fallos se produzcan, asegurar que el sistema siga funcionando. Algunas técnicas usadas en esta área son:
 - En el proceso de diseño: especificación rigurosa de requisitos, aplicación de técnicas de diseño formales, uso de lenguajes abstractos y modulares, implementación en base a componentes.
 - En el proceso de testing: revisiones frecuentes, inspecciones rigurosas al código, verificación de funcionalidades.

Dado que los resultados no son absolutos se puede lograr:

- + Tolerancia completa por un intervalo de tiempo
- + Degradación aceptable, por un intervalo de tiempo el sistema funciona con menores prestaciones hasta la reparación
- + Parada segura, se para en un estado que salvaguarda la integridad hasta la reparación.

La tolerancia en los sistemas solo es posible por la redundancia, que implica el uso de componentes destinados a la detección y recuperación de las fallas, aunque la complejidad del sistema aumenta. En este caso se puede considerar:

- Redundancia estática: N versiones

- Redundancia dinámica: con un manejo dinámico de los fallos por parte del programador, generando también N versiones

Garantizar la confiabilidad genera mayores costos en el proceso de implementación y validación en una relación exponencial.

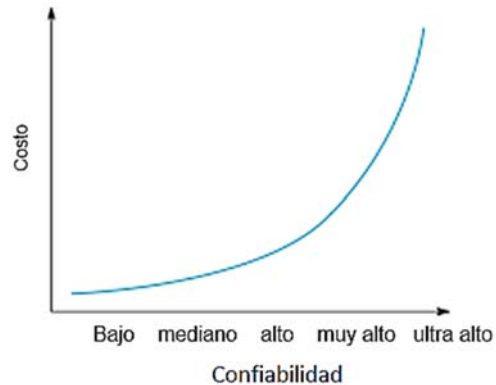


Figura 1.3. Relación confiabilidad/costo

En el caso del desarrollo de software, son buenas prácticas para garantizar la confiabilidad:

- Evitar la entrada de errores accidentales en el sistema durante la especificación y el desarrollo del software.



Figura 1.4. Mapeo entrada/salida

- Diseñar procesos de verificación y validación para descubrir errores residuales que afecten la confiabilidad del sistema.
- Desarrollar mecanismos de protección contra ataques externos que comprometan la disponibilidad o la seguridad del sistema.
- Configurar correctamente el sistema utilizado y el software de apoyo según el entorno operacional.

Una falta de confiabilidad puede ocasionar:

- Rechazo en los usuarios
- Costos de los fallos de funcionamiento del sistema pueden ser enormes.
- Pérdida de información.

El elevado costo de un fallo de funcionamiento en los sistemas críticos requiere el uso de todos los métodos y técnicas en el desarrollo propuesto por la Ingeniería de Software, asimismo es común que los desarrolladores se inclinen por las más usadas porque sus debilidades son también conocidas. La mayoría de sistemas críticos son sistemas socio-técnicos en los que existen profesionales en funciones de monitorización capacitadas para responder a problemas inesperados, sin embargo, sus propias respuestas podrían introducir errores. Existen tres tipos de componentes del sistema que pueden generar fallos:

1. El hardware del sistema por errores en el diseño.
2. El software del sistema por errores en las especificación, diseño o implementación.
3. Los usuarios del sistema debido a un uso incorrecto del mismo.

1.2.2 Disponibilidad y Fiabilidad

La **fiabilidad** de un sistema es la probabilidad de que el sistema funcione correctamente tal y como se ha especificado, mientras que la **disponibilidad** de un sistema es la probabilidad de que el sistema esté en disposición de funcionar para proporcionar los servicios ofertados a los usuarios que lo soliciten.

Ambas condiciones dependen del número de fallos que el sistema pueda presentar en su funcionamiento. La fiabilidad considera las siguientes situaciones de amenaza:

- Error humano: comportamiento humano que tiene como consecuencia la introducción de fallas en el sistema. Por ejemplo, en una estación meteorológica un programador podría decidir que la forma de calcular la hora para la siguiente transmisión es agregar una hora a la hora actual. Esto funciona salvo cuando la hora de transmisión es entre 23:00 y medianoche (medianoche es 00:00 en el reloj de 24 horas).
- Fallo del sistema: evento que tiene lugar en algún instante cuando el sistema no funciona como esperan sus usuarios, debido a una característica del sistema. En el ejemplo anterior si en el código no hay una verificación para saber si la hora es mayor o igual a 23:00
- Error del sistema: estado erróneo del sistema que puede dar lugar a un comportamiento del mismo inesperado por el usuario. En el ejemplo anterior, si se establece la hora de transmisión en 24:xx en vez de 00.xx
- Defecto o caída del sistema: característica de un sistema software que puede dar lugar a un error del sistema o que no se entregue un servicio, en el ejemplo si no se transmiten datos por una hora inválida

La fiabilidad y disponibilidad se ven afectadas por estas cuatro situaciones, aunque en diferente grado, así un error humano puede no ocasionar el fallo del sistema si fue previsto en el diseño, un defecto puede corregirse, los errores pueden descubrirse y también corregirse. Asimismo, la percepción de fiabilidad es distinta para cada usuario porque cada uno lo usa de manera diferente. Estas ambigüedades se deben a las siguientes razones:

1. No todo el código de programa se ejecuta siempre, por lo que una falla en el desarrollo (ejemplo: equivocarse al inicializar una variable) tal vez nunca se ejecute debido a la forma en que se usa el programa.
2. Los errores son transitorios (ejemplo: una variable puede tener un valor incorrecto causado por la ejecución de un código defectuoso, pero antes de que se acceda a ésta y se origine una caída del sistema, es factible procesar alguna otra entrada del sistema que restablezca el estado a un valor válido).

3. El sistema puede incluir mecanismos de detección de fallas y de protección, que aseguran que el comportamiento erróneo se descubra y corrija antes de que resulten afectados los servicios del sistema.

Son enfoques complementarios para mejorar la fiabilidad:

- ✓ *Evitación de defectos o fallas de desarrollo*: son técnicas para minimizar la posibilidad de equivocaciones i/o fallas o la detección de las mismas, antes de que produzcan defectos en el sistema. Ejemplos: evitar códigos del lenguaje de programación proclives al error, como punteros y el uso de análisis estático para descubrir anomalías del programa.
- ✓ *Detección y eliminación de defectos o fallas de desarrollo*: técnicas de verificación y validación, aumentando la posibilidad de detectar defectos antes de la utilización del sistema. Ejemplos: pruebas y depuración sistemática, puntos de control.
- ✓ *Tolerancia a defectos o fallas de desarrollo*: son aquellas técnicas para asegurar que los defectos en el sistema no conduzcan a errores en el sistema o estos no generen caídas del sistema

Problemas con la fiabilidad no influyen como con la confiabilidad, los usuarios pueden aprender a eludir los problemas que estos defectos pueden generar.

1.2.3 Seguridad

Es la propiedad del sistema de operar normal o anormalmente, sin peligro de causar daño humano o causar daño al entorno del sistema. La mayoría de los sistemas o dispositivos con fallas críticas, sustentan su seguridad en el software a partir del cual implementan sistemas de control.

Son **términos de seguridad**:

- Activo: algo que tiene valor y requiere ser protegido, puede ser también software y datos
- Exposición: posible pérdida o daño
- Vulnerabilidad: debilidad que se puede usar para causar pérdida o daño
- Ataque: aprovechamiento de una vulnerabilidad, suele ser externo y deliberado
- Amenaza: circunstancia que puede causar pérdida o daño
- Control: medida de protección para reducir la vulnerabilidad

Existen tres tipos de amenazas:

- Amenazas a la confidencialidad del sistema y sus datos
- Amenazas a la integridad del sistema y sus datos
- Amenazas a la disponibilidad del sistema y sus datos

En el proceso de diseño del software, los requerimientos de seguridad son de tipo exclusivo (situaciones indeseables), muy rara vez implican requerimientos de servicios, estos se convierten entonces en requerimientos de seguridad funcionales.

En base a la criticidad de la seguridad se definen:

- *Sistemas de seguridad críticos primarios*: sistemas de software integrados cuyas fallas pueden causar que el hardware asociado falle y amenace a gente de manera directa. Por ejemplo, el sistema de control de suministro de insulina.
- *Sistemas de seguridad críticos secundarios*: sistemas cuyas fallas resultan en fallos en otro sistema (socio-técnico), y estos podrían tener consecuencias en su seguridad. Por ejemplo, MHC-PMS (patient information system for mental health care) es crítico de la seguridad ya que una falla puede llevar a una prescripción de tratamiento inapropiada.

El desarrollo de sistemas seguros implica considerar las siguientes recomendaciones:

- Muchos de los servicios de seguridad pueden satisfacerse con etiquetas autoexplicativas de una sola palabra: confidencialidad, autenticación, no rechazo o integridad.
- Al desarrollar un mecanismo o algoritmo de seguridad, hay que considerar posibles ataques a esas características de seguridad, ya que estos explotan una debilidad en el mecanismo.
- Muchos procedimientos usados para proporcionar servicios de seguridad pueden ser intuitivos, complejos y obvios en la declaración de un requisito particular del sistema.
- Es importante también la ubicación de los mecanismos de seguridad implementados. Físicamente (por ejemplo, en qué puntos de una red) i/o lógicamente (por ejemplo, en qué capa o capas de una arquitectura como TCP/IP).
- Los mecanismos de seguridad incorporan más de un algoritmo o protocolo que requieren que los usuarios manejen alguna información secreta (por ejemplo, una clave de cifrado) y ambas cosas deben ser consideradas y organizadas.
- La seguridad de la computadora y la red es un proceso permanente, una lucha entre el perpetrador que intenta encontrar agujeros y debilidades y el diseñador o administrador que trata de cerrarlos.
- Muchos usuarios y administradores solo invierten en seguridad hasta que ocurre un fallo de seguridad, por lo que buenas prácticas son importantes en el diseño e implementación inicial.
- La seguridad requiere un monitoreo regular y constante.
- La seguridad suele ser difícil de incorporar al sistema después de que el diseño se completó.
- Muchos usuarios e incluso los administradores interpretan una fuerte seguridad como un impedimento para el funcionamiento eficiente y fácil uso de un sistema.

Un sistema fiable no necesariamente es seguro, ello se puede deber a:

- Una especificación incompleta en el sentido de que no describe el comportamiento requerido del sistema en algunas situaciones críticas. Es decir, existe un error de especificación y no de diseño.
- Un mal funcionamiento del hardware que genera un comportamiento impredecible, hace que el software enfrente un entorno inesperado.
- Los operadores del sistema pueden generar entradas que no son individualmente correctas, pero que, en situaciones particulares, pueden dar lugar a un mal funcionamiento del sistema.

La clave para garantizar la seguridad es asegurar que los accidentes no ocurran o que las consecuencias de estos sean mínimas. Son enfoques para mejorar la seguridad:

- *Evitación de contingencias o vulnerabilidades:* en el diseño del sistema
- *Detección y eliminación de contingencias o ataques:* el sistema se diseña para que las contingencias se detecten y eliminen antes de que provoquen un accidente.
- *Limitación de exposición (daños) y recuperación:* el sistema incluye características de protección que minimizan el daño que puede resultar de un accidente.

1.2.4 Protección

Es el atributo del sistema que refleja su capacidad de protegerse de ataques externos sean accidentales o provocados. Este atributo es fundamental en sistemas abiertos, lo más común, conectados a Internet, estos sistemas aumentan la funcionalidad, pero pueden ser atacados con intenciones hostiles, esta es la razón de versiones y parches. Un ejemplo de estos ataques son los virus, el uso no autorizado de servicios y la modificación no autorizada del sistema o sus datos. La protección es importante para todos los sistemas críticos. Sin un nivel razonable de protección, la disponibilidad, fiabilidad y seguridad del sistema pueden fracasar.

Un punto crucial aquí lo juega el sistema operativo, si este se vulneró, entonces todos los métodos para asegurar la disponibilidad, fiabilidad y seguridad pueden fallar y el sistema de software puede entonces corromperse y comportarse de forma impredecible. El S asegura entonces condiciones iniciales

En segunda instancia están los errores en el diseño e implementación los que pueden provocar agujeros de protección. Ejemplo de ello, es cuando el sistema no responde a entradas inesperadas o si los límites de un vector no se verifican, entonces los atacantes pueden explotar estas debilidades para tener acceso al sistema. Los incidentes de protección más importantes tales como el gusano de Internet original (Spafford, 1989) y el gusano Code Red (Berghel, 2001) se aprovecharon de que los programas en C no incluyen verificación de los límites de los vectores. Los gusanos sobrescribieron parte de la memoria con código que permitió el acceso no autorizado al sistema.

El control de hardware de los sistemas críticos para la protección es más fácil de implementar y analizar que el control del software. A pesar de ello, ahora se construyen sistemas de tal complejidad que no pueden controlarse tan sólo con el hardware. El control del software es esencial debido a la necesidad de manejar gran cantidad de sensores y actuadores con leyes de control complejas. Por ejemplo, una aeronave militar avanzada, aerodinámicamente inestable, requiere ajuste continuo, controlado por software, de sus superficies de vuelo para garantizar que no se desplome. El software crítico para la protección se divide en dos clases:

- *Software primario crítico para la protección* sirve como controlador en un sistema. El mal funcionamiento de este puede repetirse en el hardware, lo cual derivaría en una lesión humana o daño ambiental.
- *Software secundario crítico para la protección* podría repercutir indirectamente en una lesión. Por ejemplo, los sistemas CAD

Existen tres tipos de daños que pueden ser causados por ataques externos:

- *Denegación de servicio:* el sistema entra en un estado en que sus servicios normales no están disponibles.
- *Corrupción de programas o datos:* los componentes software pueden ser alterados de forma no autorizada, lo que puede afectar la fiabilidad y la seguridad.

- *Revelación de información confidencial:* la información gestionada puede ser expuesta a personas no autorizadas.

En torno a la protección se definen los siguientes términos:

- *Exposición:* posible pérdida o daño en un sistema informático.
- *Vulnerabilidad:* debilidad en un sistema que se puede aprovechar para provocar pérdidas o daños.
- *Ataque:* aprovechamiento de la vulnerabilidad de un sistema.
- *Amenazas:* circunstancias que potencialmente pueden provocar pérdidas o daños.
- *Control:* medida de protección para reducir la vulnerabilidad del sistema.

Son enfoques para mejorar la seguridad:

- *Evitar la vulnerabilidad*
- *Detección y neutralización de ataques*
- *Limitación de exposición*

Estos enfoques nos dicen que la protección está más en el uso de los sistemas que en sus características técnicas



Investigación formativa 1.2

De manera individual debe reportar al menos tres Sites donde se monitorea la seguridad y las amenazas que aparecen en tiempo real, identifique tres ataques e indique que servicio de seguridad ha sido vulnerado

1.3 POLÍTICAS Y ESTÁNDARES

La estructura del SGSI (Sistema de Gestión de Seguridad de la Información), considera cuatro procesos básicos (PAVH)

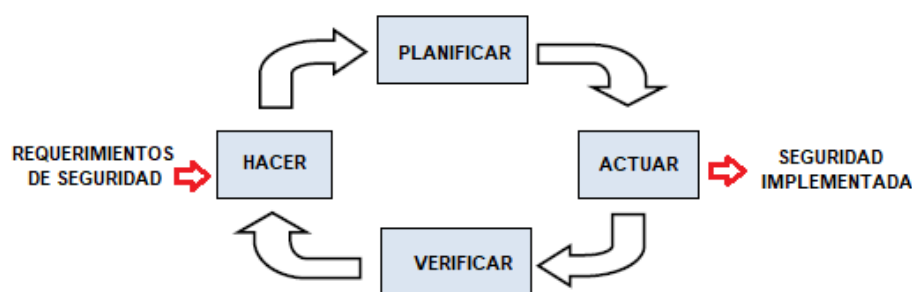


Figura 1.5. Arquitectura SGSI

- Planificar: es el proceso de establecer políticas, objetivos, procesos y procedimiento de gestión de riesgos, según los requerimientos de la organización. Para el éxito en este proceso hay que caracterizar el sistema informático, identificar las amenazas, estimar los riesgos y evaluar el estado actual de la seguridad realizando una evaluación costo/beneficio
- Hacer: son los procesos de control necesarios durante la operación con el objetivo de reducir los riesgos, estos deben ser considerados en la etapa de especificación de requisitos en el diseño de los sistemas
- Verificar: es la evaluación de los aplicado, auditoría

d) Actuar: considera acciones correctivas y preventivas necesarias

Es crítica en esta estructura la **gestión de riesgos**, la que debe considerar:

- Evitar riesgos: en los cambios bruscos en los procesos, a través del control
- Reducir los riesgos: al nivel más bajo posible, mediante la optimización de procedimientos
- Retener: reduciendo riesgos residuales
- Transferir riesgos a terceros: con respaldos contractuales con otras entidades

La funcionalidad del Sistema, se traduce en **POLÍTICAS Y ESTÁNDARES** que es el conjunto de medidas, metodologías, normas y políticas definidas con el objetivo de garantizar la seguridad informática, que se plasman en manuales organizacionales de estricto cumplimiento para los profesionales del área y los usuarios generales y deben considerar:

- Alcance del documento
- Resultado del análisis de riesgos realizado
- Lineamientos generales de administración y organización de las TICs (responsabilidades y funciones administrativas)
- Vigencia de los procedimientos
- Tipos y obligaciones de los usuarios, niveles de responsabilidad y sanciones
- Seguridad física y medioambiental de la información y bienes informáticos, controles de acceso, seguridad en áreas de trabajo, ubicación de equipos, mantenimiento, acciones ante daños o pérdidas de equipos
- Administración de los centros de cómputo, respaldo de la información, adquisición de hardware y software, administración y seguridad de las redes, administración de sistemas de mensajería y correo electrónico, controles ante virus, malware, software malicioso, acceso a internet
- Planes de contingencia
- Manejo del acceso lógico, perfiles de usuario, contraseñas, accesos remotos
- Propiedad intelectual

Hay diferentes estándares para el manejo de la seguridad en una organización, la siguiente tabla es un resumen comparativo de alguno de ellos