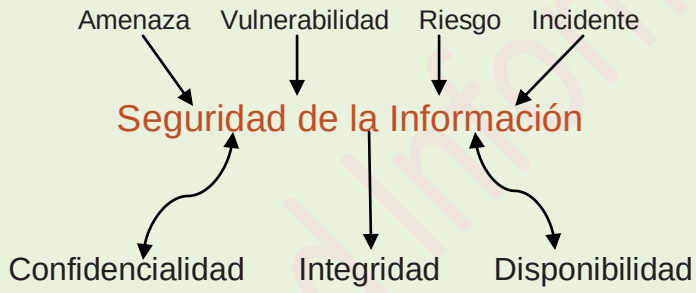
Conceptos fundamentales:

La información es un activo importante con el que cuentan las organizaciones para satisfacer sus objetivos y es crítica para su desempeño y subsistencia.

Por este motivo, es fundamental tener presente que existen amenazas que pueden afectarla. Es por ello que deben tomarse recaudos e implementar controles para protegerla.
Para abordar la complejidad del proceso de seguridad de la información, deben tenerse presente ciertos conceptos que explican cómo puede originarse un riesgo y qué efectos puede provocar.
El siguiente esquema muestra las nociones centrales que se relacionan con la temática de la seguridad de la información y serán desarrolladas a continuación:



Cuando en el ámbito de la seguridad informática mencionamos el concepto de incidentes nos referimos a aquellos eventos adversos en un entorno informático, que pueden comprometer o comprometen la confidencialidad, integridad y/o disponibilidad de la información así como también las amenazas inminentes de violación o las violaciones concretas de una política de seguridad de la información, de políticas de uso aceptable o de mejores prácticas de seguridad.

Principios de seguridad: confidencialidad, integridad y disponibilidad

¿Qué podría ocurrir si en la dependencia donde trabajamos alguien accediera a la información personal que se tiene de los ciudadanos o de los empleados del organismo (por ejemplo, datos personales de agentes, ingresos anuales, domicilio o legajos etc.), sin la debida autorización?

Podemos imaginar una serie de riesgos que afectan a las instituciones y cómo podrían impactar negativamente en la vida cotidiana de las personas.
En estos casos, se entiende que debe protegerse no solo la información en su totalidad, sino también las piezas individuales que pueden ser utilizadas para inferir otros elementos de información confidencial.

Propiedad por la cuál se autoriza el acceso a la información, a solo aquellas personas autorizadas **Confidencialidad.**

¿Qué ocurriría si se alteraran los datos contenidos en nuestras PC o se cambiara su configuración, sin la debida directiva o autorización?
Seguramente en muchos casos, esto tendría graves consecuencias para nosotros, para el organismo y/o para terceros.
Es necesario proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida incluye no sólo la que está almacenada directamente en los sistemas de cómputo sino que también se deben considerar otros elementos como respaldos, documentación, registros de contabilidad del sistema, tránsito en una red, etc.

Propiedad por la que se garantiza la protección contra modificaciones no autorizadas para evitar su modificación. **Integridad.**

Supongamos ahora que un organismo publica información importante en su sitio web, como por ejemplo vencimientos de pagos, instrucciones para realizar un trámite complicado como la presentación en línea de declaraciones juradas, y alguien impide que se pueda acceder a dicho sitio.
De nada sirve la información si se encuentra intacta en el sistema pero los usuarios no pueden acceder a ella.

Proteger la información también significa que la misma esté disponible en tiempo y forma para todas aquellas personas autorizadas a su uso. **Disponibilidad.**

Riesgos para la seguridad de la información

Las "buenas prácticas" en seguridad de la información protegen a este activo contra una amplia gama de amenazas, tanto de orden fortuito –destrucción parcial o total por incendio inundaciones, eventos eléctricos, etc. - como de orden deliberado – fraude, espionaje, sabotaje, vandalismo, etc.
Las amenazas a la seguridad de la información son sucesos que atentan contra la confidencialidad, integridad y/o disponibilidad de la información. Existen diferentes tipos de amenazas y distintas formas de clasificarlas. El esquema que sigue presenta una posible clasificación:

- Externas
- Internas

- Impericias
- Maliciosas
- No Maliciosas

- Naturales
- Humanas

Las amenazas naturales son fortuitas, y su origen se asocia a catástrofes naturales: huracanes, terremotos, tormentas de nieve, erupciones volcánicas, inundaciones, etc.
Las amenazas humanas pueden ser tanto fortuitas o accidentales como intencionales. En el primer caso se consideran amenazas no maliciosas. Estos eventos accidentales pueden deberse a explosiones, incendios, cortes de energía u otros suministros, rotura de tuberías, desastres nucleares, choques de vehículos.

Estos eventos se explican más por la impericia que por la intención de causar daños.
Las amenazas maliciosas, en cambio, se vinculan con eventos intencionales, deliberados, como las posibilidades de robo de equipamiento, sabotaje, suplantación de identidad, interrupción deliberada de servicios, etc. y pueden provenir de integrantes de la organización o de personas externas a ella.

Una amenaza implica una violación potencial a la seguridad. Luego la amenaza puede o no materializarse, explotando una vulnerabilidad.
Una vulnerabilidad es una debilidad en un control, o la inexistencia de este. Por ejemplo, si una oficina no cuenta con los extintores de incendios reglamentarios, entonces decimos que presenta una vulnerabilidad, ya que no existe el control necesario para tratar posibles incendios.
El riesgo resulta de la combinación de la probabilidad de que una amenaza explote una vulnerabilidad y del impacto resultante en la organización. En el ámbito de la seguridad informática, nos referimos a impacto en términos de los posibles efectos negativos sobre la seguridad de la información.
Un incidente de seguridad ocurre en el preciso momento en que una amenaza explota una vulnerabilidad existente.
Un incidente puede afectar a recursos físicos (ej.: impresoras, servidores de archivos), recursos lógicos (ej.: bases de datos) y servicios (ej.: correo electrónico, página Web).

Existen cuatro tipos de incidentes en el modelo de relación productor consumidor de información.

1. El primer tipo de incidente que muestra el esquema es la interrupción. En este caso resulta afectada la disponibilidad de la información. Esta alteración se observa por ejemplo cuando alguien da de baja el servidor y se ve afectado el servicio de correo electrónico, lo que impide enviar correos. En otros casos la interrupción puede deberse a la falta de energía eléctrica que impide encender la impresora y por lo tanto, imprimir un documento y tenerlo disponible en formato papel.
2. El segundo tipo de incidente se denomina intercepción y pone en riesgo la confidencialidad de la información que un productor transmite a un consumidor. Por ejemplo, con el objetivo de leer información, una persona no autorizada a hacerlo, puede implantar un programa que duplique los correos electrónicos de una dirección y envíe la copia de cada correo a otra dirección.
3. Un tercer caso de incidentes se conoce como modificación y afecta directamente la integridad de los datos que le llegan al consumidor. Por ejemplo, si alguien logra ingresar al servidor Web como webmaster (ADMINISTRADOR) y cambia los contenidos, los datos que mostrará la Web (Página) no serán los reales. Otra modificación puede darse sobre la base de datos de pagos en cuentas corrientes de un banco, al implantarse un programa que redondea en menos los pagos y carga los redondeos a una cuenta corriente predeterminada.
4. El cuarto y último tipo de incidentes es el de la producción impropia de información.

En este caso la información que recibe el consumidor es directamente falaz y por lo tanto se afecta a la integridad. Esta situación puede darse si alguien se apropia de la contraseña del webmaster, ingresa al servidor y modifica el direccionamiento de manera que se cargue, en lugar de la página original de la organización, otra página Web.