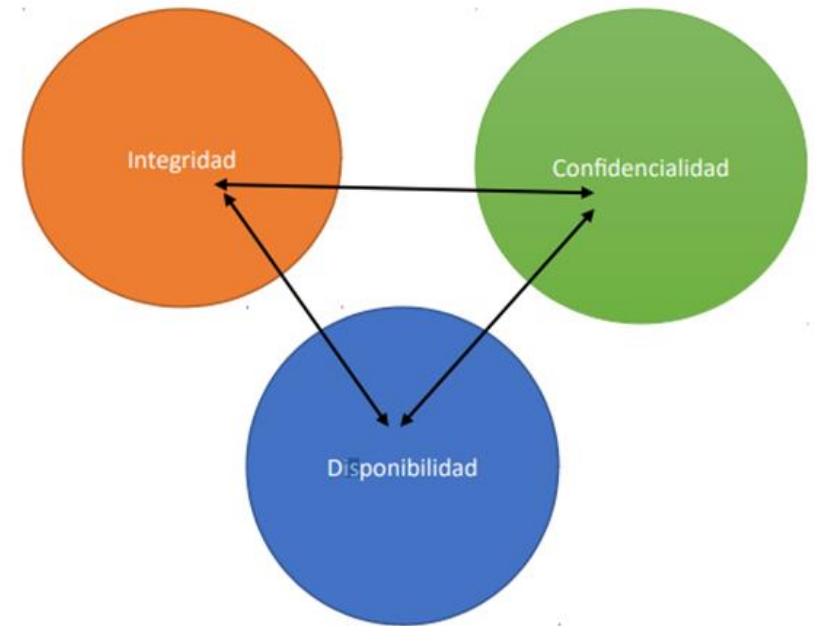


Principios de Ciberseguridad

Conceptos sobre Ciberseguridad

Introducción al módulo

- Conceptos sobre Ciberseguridad
 - Generalidades de la seguridad informática
 - El valor de la información
 - Definición y tipos de seguridad informática
 - Objetivos de la seguridad informática
 - Gestión y evaluación del riesgo



Generalidades Seguridad Informática

- Tres personas distintas poseen un bien muy valioso para cada una de ellas. Un estudiante, un hombre de familia y una empresaria



Generalidades Seguridad Informática

- Considerando los ejemplos anteriores las personas piensan en el riesgo que corren los activos más valiosos para ellos; ya sea la familia o la información.
- Poseer activos o cualquier cosa valiosa implica también el riesgo de perderlos.
- La protección de cualquier activo contra los riesgos: algún tipo de daño o pérdida total, tiene un costo, el cual es directamente proporcional al tipo de protección que se otorgue al activo.
- Activo, desde el punto de vista de la contabilidad, se define como cualquier cosa de valor, tangible o intangible, propiedad de una empresa.



El valor de la información

- En 1948, Norbert Wiener, matemático estadounidense, acuñó por primera vez el término cibernética. “Cibernética o el control y comunicación de animales y plantas”.
- El tema fundamental de las investigaciones de Wiener era el funcionamiento fisiológico de los seres vivos en cuanto al control interno que éstos tienen para que sus funciones corporales se regulen en forma autónoma y para comunicarse con su medio circundante



El valor de la información

- Sienta las bases para el desarrollo de la teoría del control y la teoría de sistemas.
- Descubrió que estas ideas se pueden aplicar tanto a sistemas físicos como sociales y determinó que los sistemas complejos, como los seres vivos, primero afectan y luego se adaptan a su medio ambiente; no obstante, **los seres vivos logran esta adaptación con base en la información que reciben, procesan y a cuyos resultados reaccionan para adaptarse.**
- Por tanto, la idea más brillante de Wiener radica en que fue el primero en observar una similitud entre el funcionamiento de un ser vivo y una empresa.

El valor de la información

- En aquel tiempo, en Estados Unidos de América y Europa ya existían enormes y complejas organizaciones que, desde el momento de su creación, afectaban al medio ambiente en muy diversas formas, recibían y procesaban información, y reaccionaban a esa información, se adaptaban a las condiciones cambiantes del medio ambiente, social y empresarial y eventualmente crecían o desaparecían. Este “ciclo de vida” es similar al de un ser vivo..
- La información es entonces el activo más valioso de cualquier empresa, después del activo humano. El hombre genera las órdenes y la información, pero ésta necesita fluir hacia las partes ejecutoras para que las compañías cobren vida y comiencen su actividad.

El valor de la información

- El problema es que esa información, tanto en los seres vivos como en las empresas, corre el riesgo de ser dañada, o su flujo puede ser obstruido, lo que da lugar a un mal funcionamiento del ser vivo o de la organización
- En el entorno empresarial, se define la información como un activo que posee valor para una organización y requiere, por tanto, de una protección adecuada para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio

El valor de la información

- Por tanto, es imperativo tener la certeza de que los datos están seguros en cualquiera de los procesos mencionados: recepción, envío, almacenamiento y análisis de datos; y que al ser procesados se convierten en información.
- **Informática** es la ciencia que estudia la transmisión (recepción y envío), el almacenamiento y el análisis de datos, que al ser procesados se convierten en información, realizando estos procesos con la ayuda de un dispositivo automático.
- Es la ciencia que estudia todos los procesos que se pueden hacer sobre la información, pero con la ayuda de dispositivos automáticos.

Definición y tipos de seguridad informática

- La **seguridad informática** es la disciplina que con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta.
- Es el **conjunto de herramientas, técnicas, dispositivos y procedimientos** orientados a conseguir, mejorar o garantizar determinados **niveles de confidencialidad, disponibilidad, integridad, autenticidad y/o no repudio** de la información con la que trabaja un sistema informático

Definición y tipos de seguridad informática

- La seguridad informática se puede clasificar según dos criterios:
 - **Dependiendo del momento** en el que se aplique
 - Seguridad **ACTIVA**: la que se aplica con el objeto de detectar y/o prevenir amenazas.
 - Seguridad **PASIVA**: aquella que, una vez producido el ataque, error o daño, se aplica para reducir al máximo los efectos producidos y, en la medida de lo posible, recuperar el sistema.

Definición y tipos de seguridad informática

- La seguridad informática se puede clasificar según dos criterios:
 - **Dependiendo de la naturaleza** de los componentes a proteger
 - Seguridad **FÍSICA**: cuando se protege la parte hardware del sistema informático de amenazas materiales, ya sean provocadas o accidentales.
 - Seguridad **LÓGICA**: cuando es el software lo que se protege, es decir, programas y datos.

Objetivos de la seguridad informática

- Preservar las siete características que señala COBIT (efectividad, eficiencia, confidencialidad, integridad, disponibilidad, apego a estándares, confiabilidad).
- Identificar las amenazas a las cuales está expuesta la información y formular un plan para prevenir los principales tipos de ataque interno, externo, físico o electrónico sobre la información.
- Minimizar los riesgos de esa exposición y gestionar la adecuada utilización de las TIC que tiene la empresa

Objetivos de la seguridad informática

- En caso de que llegara a suceder cualquier daño a la información, ya sea alteración o robo, también se debe contar con planes para la recuperación de esa información en su totalidad de forma inmediata e integral.
- Cumplir con el marco legal que se exige por el manejo de datos personales y empresariales de los clientes y socios de la empresa.

Gestión y evaluación del riesgo

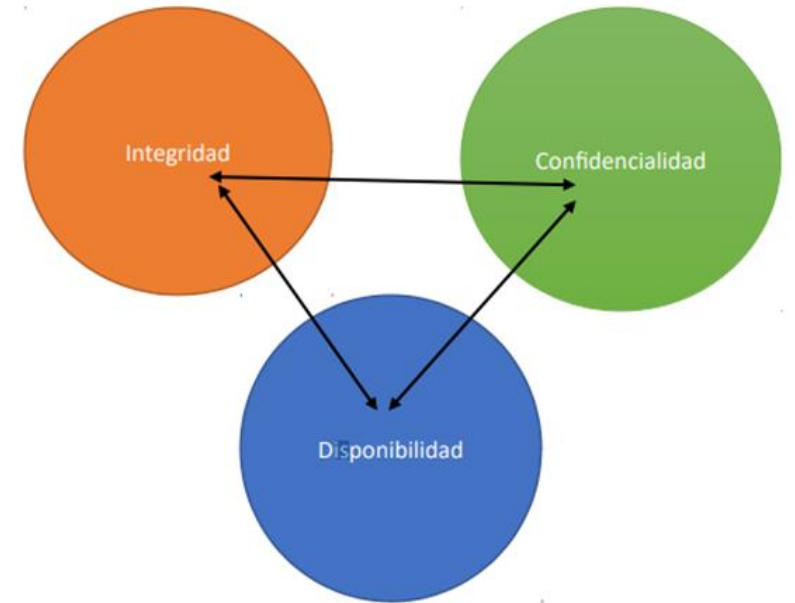
- En términos generales, el **riesgo** se define como la posibilidad de que no se obtengan los resultados deseados.
- Las empresas siempre están amenazadas de sufrir algún daño en su sistema informático, **las amenazas son mayores cuando los sistemas presentan ciertos puntos débiles llamados “vulnerabilidades”**, de manera que se tiene mayor o menor riesgo dependiendo de la cantidad y número de vulnerabilidades que se tengan.

Gestión y evaluación del riesgo

- Lo ideal es evitar riesgos mediante una buena planeación en seguridad informática. Dicha planeación implica identificar las vulnerabilidades y medir el daño que pueden causar, de manera que al disminuir las vulnerabilidades, también disminuirá el riesgo de sufrir daños, no sólo en el aspecto informático, sino en toda la empresa.
- El proceso general de Análisis del Riesgo sería:
 - Identificación de la Amenaza o Vulnerabilidad
 - Definir la probabilidad del riesgo
 - Definir el impacto del riesgo
 - Generar la matriz calórica
 - Definir la estrategia de mitigación
 - Cuantificación Económica

Culminación del módulo

- Conceptos sobre Ciberseguridad
 - Generalidades de la seguridad informática
 - El valor de la información
 - Definición y tipos de seguridad informática
 - Objetivos de la seguridad informática
 - Gestion y evaluación del riesgo





Gracias

