CONCEPTOS GENERALES DE LA SEGURIDAD INFORMATICA

RUBIEL LEAL BERNAL

ING. DE SISTEMAS

UNIVERSIDAD DE NARIÑO

Conceptos Generales

SEGURIDAD DE INFORMACIÓN

- Es la protección de ventajas de información de la revelación no autorizada, de la modificación, o destrucción accidental o intencional, o la incapacidad para procesar esta información.

SEGURIDAD DE RED

- Se compone de las medidas tomadas para protege una red del acceso no autorizado, interferencia accidental o intencional, con operaciones normales, o con la destrucción; inclusive la protección de facilidades física, del software, y de la seguridad del personal.

Conceptos básicos de la seguridad

- Entender la importancia de la información en los negocios de hoy en día para actuar con **mayor prontitud en su protección**.
- Identificar las diferencias entre los conceptos de **seguridad de la información en las empresas actuales** y **la seguridad de los objetos tangibles** para posteriormente definir posibles alternativas de protección.
- En la actualidad la información es el objeto de mayor valor para las empresas.
- La seguridad de la información tiene como propósito **proteger la información** registradas, independientemente del lugar en que se localice: Impresos en papel, en los discos duros de las computadoras, o inclusive en la memoria de las personas que la conocen.

Conceptos básicos de la seguridad

ACTIVO.

- Un activo es todo aquel elemento que compone el proceso de la comunicación, partiendo desde la información, **su emisor, el medio por el cual se transmite, hasta su receptor**.
- Los Activos son elementos que la seguridad de la información busca proteger
- Los activos poseen valor para las empresas y como consecuencia de ello, necesitan recibir una protección adecuada para que sus negocios no sean perjudicados

Conceptos básicos de la seguridad

- Es necesario identificar los elementos que la seguridad de la información busca proteger:
  - La información
  - Los equipos que la soportan
  - Las personas que la utilizan

TIPOS DE ACTIVOS

- La Información
- Los Equipos que la Soportan
  - Software, Hardware, Red, etc.
- Las personas que los utilizan

I. La Información

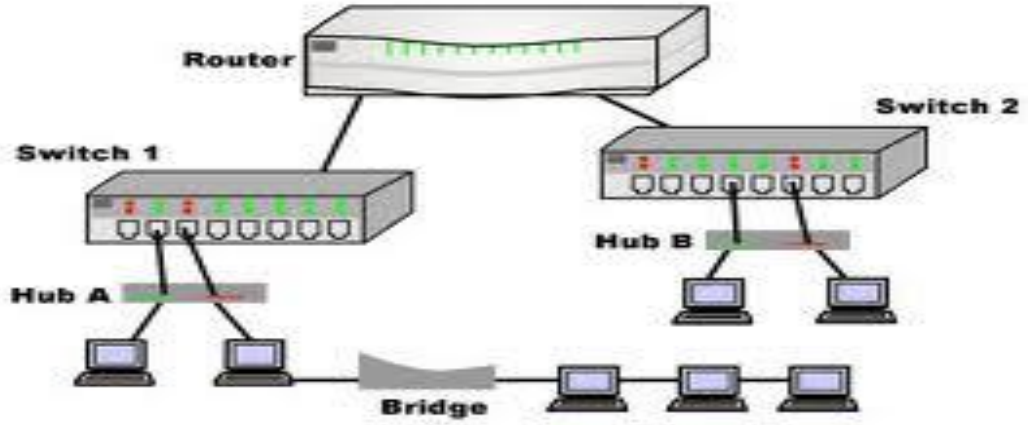
- Elementos que contienen información registrada, en medio electrónico o físico:
  - Documentos, Informes, Libros, Manuales
  - Correspondencia
  - Patentes
  - Código de Programación, Líneas de comandos, Archivos de configuración
  - Información de mercadeo,
  - Plantillas de personal, organización
  - Planes de Negocios, etc.
- Posibles Vulnerabilidades: Robo de documentos, perdida de información o archivos.

2. Software

- Programas de computador que se utilizan para la automatización de proceso, acceso, lectura, transito y almacenamiento de la información:
  - Aplicaciones comerciales
  - Sistemas operativos,
- Posibles vulnerabilidades:
  - Fallas publicadas o no publicadas y no reparadas, que pueden representar accesos indebidos a los equipos.
  - Configuración no adecuada de los sistemas que puedan implementar puertas traseras de acceso.

3. Hardware

- Representa toda la infraestructura tecnológica que brinda soporta a la información durante el uso, transito y almacenamiento.
  - Computadores
  - Servidores
  - Medios de Almacenamiento
  - Equipos de Conectividad, enrutadores, switchs, y cualquier otro elemento de una red por donde transita la información



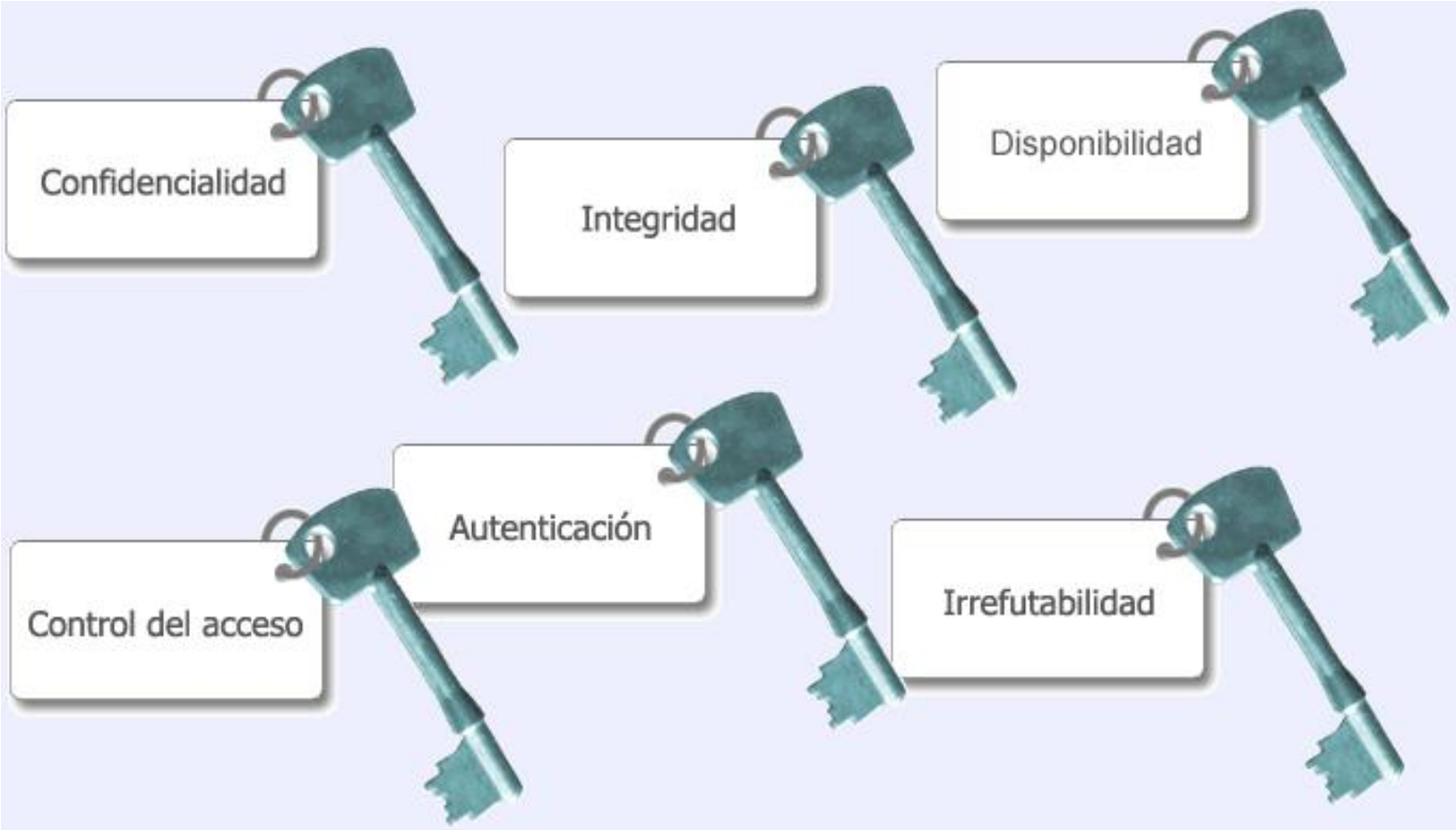
4. Usuarios

- Individuos que utilizan la estructura tecnológica y de comunicación de la empresa y que manejan la información:
  - Empleados del áreas de contabilidad, sistemas
  - Directivos de la empresa
  - Aéreas técnicas
- El enfoque de seguridad en los usuarios, esta orientado hacia la toma de **conciencia de formación del hábito de la seguridad** para la toma de decisiones y acción por parte de todos los empleados de la empresa.
- Posibles vulnerabilidades:
  - Ubicación insegura de documentos, equipos o personas
  - Falta de cooperación de los usuarios
  - Descuido por parte de los usuarios en el manejo de la información, olvido de contraseñas

Principios básicos de la Seguridad

- Proteger los activos significa mantenerlos seguros contra amenazas que puedan afectar su funcionalidad:
  - Corrompiéndola
  - Accediendo indebidamente
  - Eliminándola o hurtándola
- Seguridad Informática es el conjunto de procedimientos, estrategias y herramientas que tiene como objetivo proteger a estos activos con base a tres principios básicos:
  - La integridad: Intacta
  - La disponibilidad: Oportuna
  - La confidencialidad: Usuarios autorizados

Principios básicos de la Seguridad



Principios básicos de la Seguridad

INTEGRIDAD

- Garantizar que la información no ha sido alterada de forma indebida o no autorizada
- Asegurar que solo las personas autorizadas puedan realizar alteraciones en la forma y contenido de una información
- La perdida de la integridad puede acabar en fraude, decisiones erróneas o como paso a otros ataques

CONFIDENCIALIDAD

- Asegurar que solo la persona correcta acceda a la información
- La perdida de la confidencialidad significa la perdida del secreto
- Una información secreta se debe guardar con seguridad y no deber ser divulgada a personas no autorizadas

Principios básicos de la Seguridad

Grado de Sigilo

- La información generada por las personas tiene un fin específico y se destina a un grupo de personas en específico
- Por lo tanto la información necesita una clasificación en lo que refiere a su confidencialidad
- El Grado de Sigilo es el nivel de clasificación atribuido a cada tipo de información, con base en el grupo de usuarios que tienen permiso de acceso:
  - Confidencial
  - Restricto
  - Sigiloso
  - Púbico

Principios básicos de la Seguridad

DISPONIBILIDAD

- Corresponde a la disponibilidad de la información y de toda la estructura física y tecnológica que permite el acceso, transito y almacenamiento.
- Esta asociada a la adecuada estructuración de un ambiente tecnológico y humano que permita la continuidad de los procesos de una entidad.
- No basta estar disponible, la información debe ser **Accesible de forma segura** para que se pueda usar en el momento en que se solicita y se garantice su integridad y confidencialidad.
- La perdida de disponibilidad puede implicar la perdida de productividad

Amenazas y puntos débiles

AMENAZA

- Son agentes capaces de explotar los fallos de seguridad, que se denominan puntos débiles, y como consecuentica de ello, causar perdidas o daños a los activos de una entidad.
- Las amenazas siempre existirán y están relacionadas con causas que representan riesgos
  - Causas naturales o no naturales
  - Causas externas o internas

Un primer objetivo de la seguridad de la información es impedir que las amenazas exploten puntos débiles y afecten algunos de los principios básicos de la información como son:

Integridad, Confidencialidad, Disponibilidad

Amenazas y puntos débiles

Amenazas y puntos débiles

RIESGO

La relación **Frecuencia-Tiempo**, se basa en el concepto de **riesgo**, el cual representa la probabilidad de que una amenaza se concrete por medio de una vulnerabilidad o punto débil.

TIPOS DE AMENAZAS

- Naturales: Inundaciones, terremotos
- Intencionadas: Fraudes, vandalismo, sabotaje, espionaje, hurtos, invasiones, ataques de información
- Involuntarias: Virus electrónicos, falta de conocimiento en el uso de los activos, errores, accidentes de los usuarios.

VULNERABILIDADES O PUNTOS DEBILES

- Son elementos que al ser explotados por amenazas afectan la confidencialidad, integridad y disponibilidad de la información.

Amenazas y puntos débiles

VULNERABILIDADES O PUNTOS DEBILES

- Uno de los primeros pasos para la implementación de la seguridad es rastrear y eliminar los puntos débiles.

Uno Segundo objetivos de la seguridad de la información es corregir las vulnerabilidades existentes en el ambiente en que se usa la información, con el objeto de reducir los riesgos a que está sometida, evitando así que una amenaza se concrete.

LA SEGURIDAD ES UNA PRACTICA ORIENTADA HACIA LA ELIMINACIÓN DE LAS VULNERABILIDADES, PARA EVITAR O REDUCIR LA POSIBILIDAD QUE LAS POTENCIALES AMENAZAS SE CONCRETEN EN EL AMBIENTE QUE SE QUIERE PROTEGER

Amenazas y puntos débiles

TIPOS DE VULNERABILIDADES

- **Físicas:** Instalaciones inadecuadas, ausencia de planes de contención de incendios, disposición desorganizada de cables de energía, de red, ausencia de identificación de usuarios y locales
- **Naturales:** Infraestructura incapaz de resistir terremotos, huracanes; Humedad, polvo que causan daños al hardware-electrónico; edificaciones próximas a ríos propensos, zonas de derrumbos
- **De Hardware:** Defectos de fabricación o configuración de equipos que permitan el ataque o alteración de los mismos, conservación inadecuada de los equipos.
- **De Software:** Sistemas Operativos, aplicación que permitan accesos indebidos , instalaciones y configuración no adecuada

Amenazas y puntos débiles

TIPOS DE VULNERABILIDADES

- **De medios de almacenaje:** Cd-Roms, cintas magnéticas, discos duros de los servidores y bases de datos ; registros en papel, archivos.
- **De comunicación:** Abarca todo el transito de la información, cableado estructurado, fibra óptica, ondas de radio, salidas de conexión.
  - Ausencia de sistemas de encriptación en las comunicaciones
  - Medio de transmisión vulnerable.
- **Humanas:** Falta de conocimiento, capacitación y conciencia del personal interno en lo referente a la seguridad de la información, y el compromiso con el cargo dentro de la entidad

Riesgos, medidas y ciclo de seguridad

RIESGO:

Es la probabilidad de que las **amenazas exploten puntos débiles**, causando perdidas o daños a los activos de la empresa

MEDIDAS DE SEGURIDAD:

- Son acciones orientadas hacia la **eliminación de las vulnerabilidades**, teniendo en la mira evitar que las amenazas se vuelvan realidad
- Ya que existe una variedad de clases de puntos débiles que afectan la disponibilidad, confidencialidad, e integridad de la información, deberán existir **medidas de seguridad específicas** para cada caso.

Riesgos, medidas y ciclo de seguridad

TIPOS DE MEDIDAS DE SEGURIDAD:

- **Preventivo:** Buscando evitar el surgimiento de nuevos pintos débiles y amenazas
- **Perceptivo:** Orientado hacia la revelación de actos que pongan en riesgo la información.
- **Correctivo:** Orientado hacia l corrección de los problemas de seguridad conforme su ocurrencia

Riesgos, medidas y ciclo de seguridad

MEDIDAS DE SEGURIDAD:

- Las medidas de seguridad son un conjunto de prácticas que, al ser integradas, constituyen una solución global y eficaz de la seguridad de la información:
- Entre las principales medidas de seguridad se destacan:
  - **Análisis de riesgos:** Medida que busca rastrear vulnerabilidades en los activos que pueden ser explotados por amenazas.
  - **Políticas de seguridad:** Medida que busca establecer los estándares y normas de seguridad a ser seguidos por todos los involucrados con el uso y mantenimiento de los activos
  - **Especificación de seguridad:** Medidas que tiene en mira instruir la correcta implementación de un nuevo ambiente tecnológico, por medio del detalle de sus elementos constituyentes y la forma con que los mismos deben estar dispuestos.

Riesgos, medidas y ciclo de seguridad

MEDIDAS DE SEGURIDAD:

- Administración de seguridad: Son medidas integradas para producir la gestión de los riesgos en un determinado ambiente. Involucra todas las medidas anteriores en forma preventiva, perceptiva y correctiva con base en el **ciclo de seguridad**

Ciclo de Seguridad:

- Se inicia con **la identificación de las amenazas** a las cuales esta sometida la empresa
- Esto permite la visualización de las vulnerabilidades que se podrán explotar, exponiendo los activos a **riesgos de seguridad**
- Para que el impacto de estas amenazas se puedan reducir se toman **medidas de seguridad** para impedir la ocurrencia de puntos débiles