

Conceptos generales

Agenda

- I. Seguridad, Seguridad de la Información y Seguridad de Sistemas de TI
- II. La tríada C-I-A
- III. Conceptos de seguridad

Agenda

- I. Seguridad, Seguridad de la Información y Seguridad de Sistemas de TI
- II. La tríada C-I-A
- III. Conceptos de seguridad

I. Seguridad, seguridad de la información y seguridad de sistemas de ti

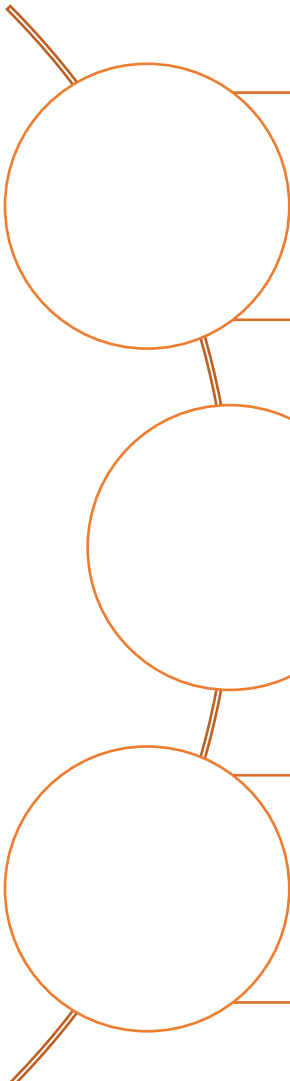
Seguridad de la Información

- Es la **especialidad** que busca **proteger la información en todas sus formas**, ya sea hablada, escrita o en medios informáticos, **de las amenazas a las que esta expuesta**. La seguridad busca proteger la **confidencialidad, integridad y disponibilidad** de la información.
- Son un conjunto de **acciones alineadas** entre sí e implementadas, con la intención de **restringir y evitar el mal uso de la información** de una organización en todas sus formas.
- Requiere de la **participación de todos los integrantes** de la organización.

¿Qué no es Seguridad de la Información?

- Una forma de **garantizar** que **nada va a afectar** a la información.
- Una **receta que se pueda copiar** de otra organización.
- Una **relación de HW y SW** con los que se debe contar.
- Un **gasto de dinero** que no se puede justificar.

¿Qué está cambiando en el mundo hoy?

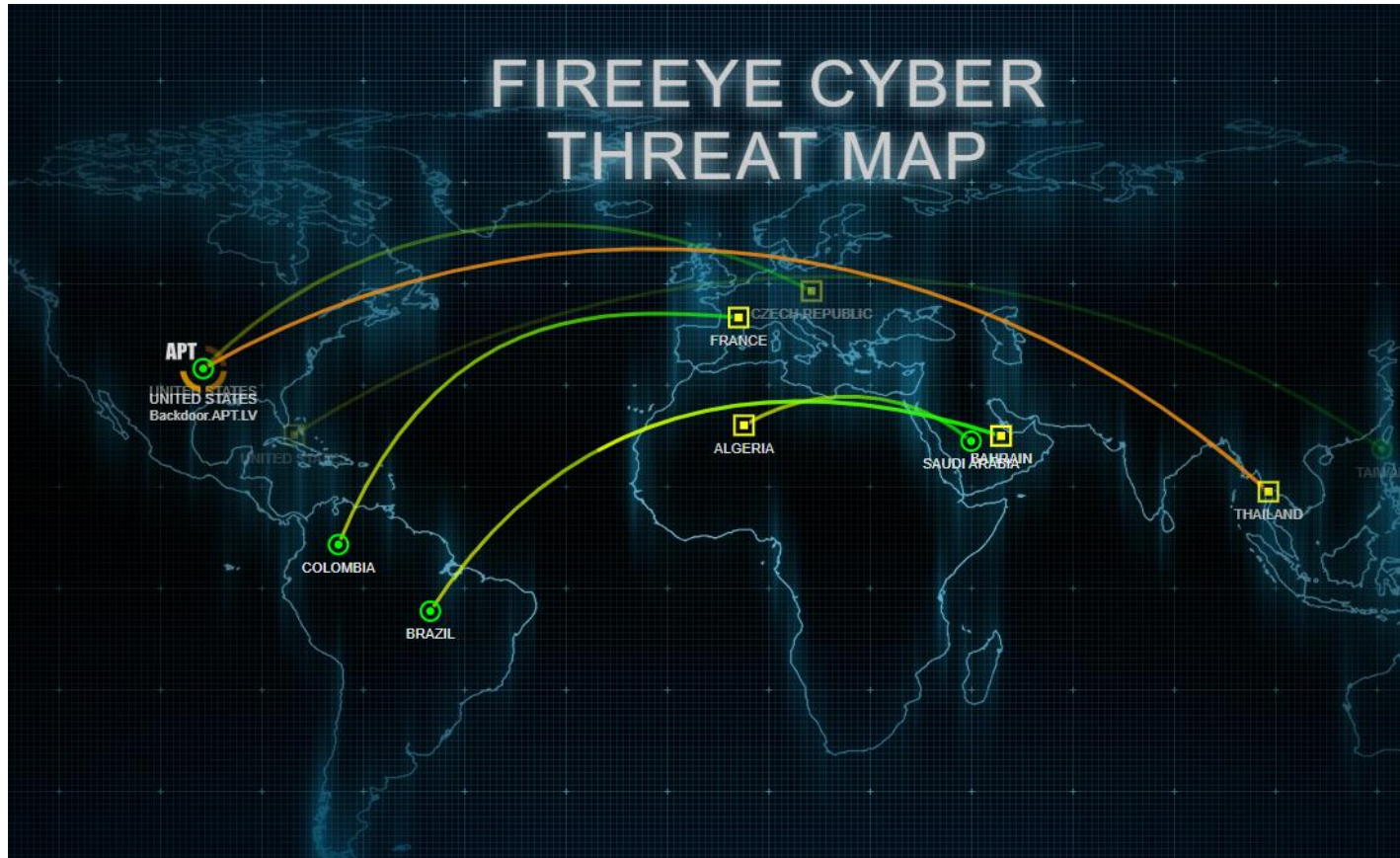


Muchas organizaciones han puesto en su agenda el tema de **“seguridad de la información”** ya sea con un enfoque “proactivo” ó “reactivo”, especialmente, por la pandemia.

No cumplir con las regulaciones y obligaciones puede ser **más costoso** de lo pensado (por multas, por pérdida de información, daño de imagen, etc.)

Atender el tema de **“Seguridad de la Información”** dejó de ser una **“opción”** para convertirse en una **“obligación”** porque busca proteger el **valor del negocio**.

Los Problemas



<https://www.fireeye.com/cyber-map/threat-map.html>

Relación entre la Seguridad de la Información y la Seguridad de TI

- La **Seguridad de TI** trata la seguridad de la **Tecnología** y, por lo general, se maneja desde el nivel del director de información (CIO) o de una Jefatura de Seguridad TI.
- La **Seguridad de la Información** abarca la totalidad de riesgos, beneficios y procesos que están relacionados con la **Información** y debe ser impulsada por la dirección ejecutiva y respaldada por el consejo de dirección

Relación entre la Seguridad de la información y la Seguridad de TI

Seguridad de la información

Es una función de negocio

Instaura las políticas de seguridad y elementos de control en materia de seguridad de información

Se encarga de los aspectos físico, lógico y legal de la seguridad de información de la empresa

Busca garantizar la tríada CIA, la autenticidad, auditabilidad y no repudio de la información

Seguridad de TI

Es una función técnica

Incorpora ó trata a los sistemas de información y telecomunicaciones

Asegura que los sistemas carezcan de riesgos perniciosos

Garantiza que los sistemas y sus activos de información asociados se empleen para lo que fueron concebidos

La Seguridad de Sistemas de TI (I)

- La **Seguridad de Sistemas de TI** generalmente consiste en asegurar que los recursos del **Sistema de Información** (material informático ó programas) de una organización sean utilizados de la manera que se decidió y que la información que se considera importante no sea fácil de acceder por cualquier persona que no se encuentre acreditada .

Elementos de la seguridad

Tecnologías

Procesos

Personas

II. La triada CIA

La Tríada CIA

Una inyección SQL afecta a toda la triada.- Primero a la confidencialidad porque se pued

Confidencialidad: Propiedad de la información para que no sea divulgada a personas, entidades o procesos no autorizados (ISO 27000:2018).

- Ej. Que no ingresen a mi correo otros usuarios

Integridad: Propiedad de exactitud de la información (ISO 27000:2018).

- Ej. Que no sea modificada de manera no autorizada

Disponibilidad: Propiedad de la información de estar accesible y usable a demanda por una entidad autorizada (ISO 27000:2018).

- Ej. Que cuando solicitemos un recurso digital, pueda ser usado en ese momento.

La información solo puede ser vista por

La información debe de ser modificada

La información debe de estar disponibl

No Repudio

- Se logra la capacidad de “No Repudio” (**no rechazo de una transacción**) cuando se despliegan mecanismos internos ó externos que **permiten asignar de manera inequívoca la autoría de una transacción/operación** a determinada persona.

Manera en la que uno no puede negar que hizo algo.

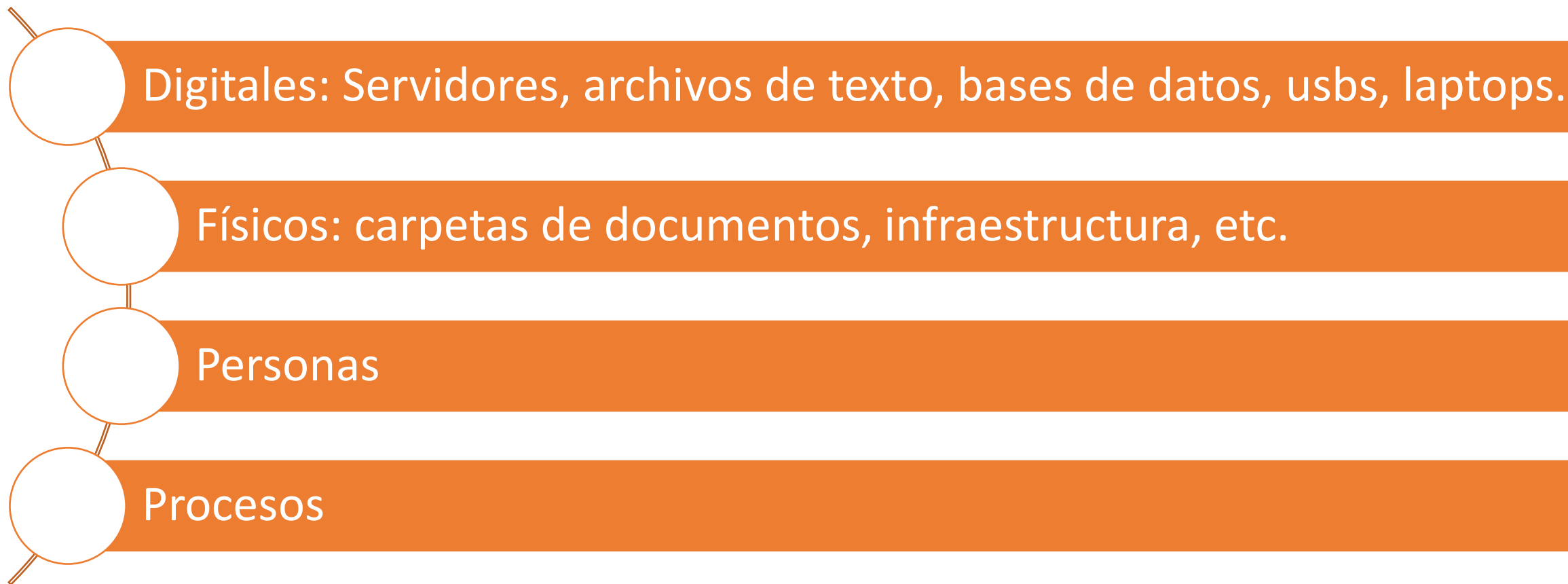
Activo de información

El activo de información es algo que tiene valor y **transporta, procesa o almacena información.**

En ciberseguridad se busca proteger la **confidencialidad, integridad y disponibilidad** de los activos digitales que se conectan al ciberespacio.

Los activos críticos digitales son los **activos que tienen mayor relevancia para la organización**, sin ellos, se afecta la operación del negocio. Ej. Servidores, aplicaciones, bases de datos.

Ejemplos de activos de información



Amenaza

- Una Amenaza, para Seguridad de la Información, es cualquier actividad, agente ú entidad que represente un **posible peligro** para su información.
- Las amenazas pueden tomar diversas formas, pero una amenaza constituye un **peligro para la tríada C-I-A.**
- Pueden desencadenar un **incidente en la organización**, produciendo daños materiales o pérdidas inmateriales en sus activos.

Ejemplo de “Amenaza”

- Un ladrón “a la caza” de laptops
- El retiro de un empleado
- Otra persona que está en el Starbucks
- El señor que está de pie en el paradero
- El técnico del proveedor de telecomunicaciones

Ataque

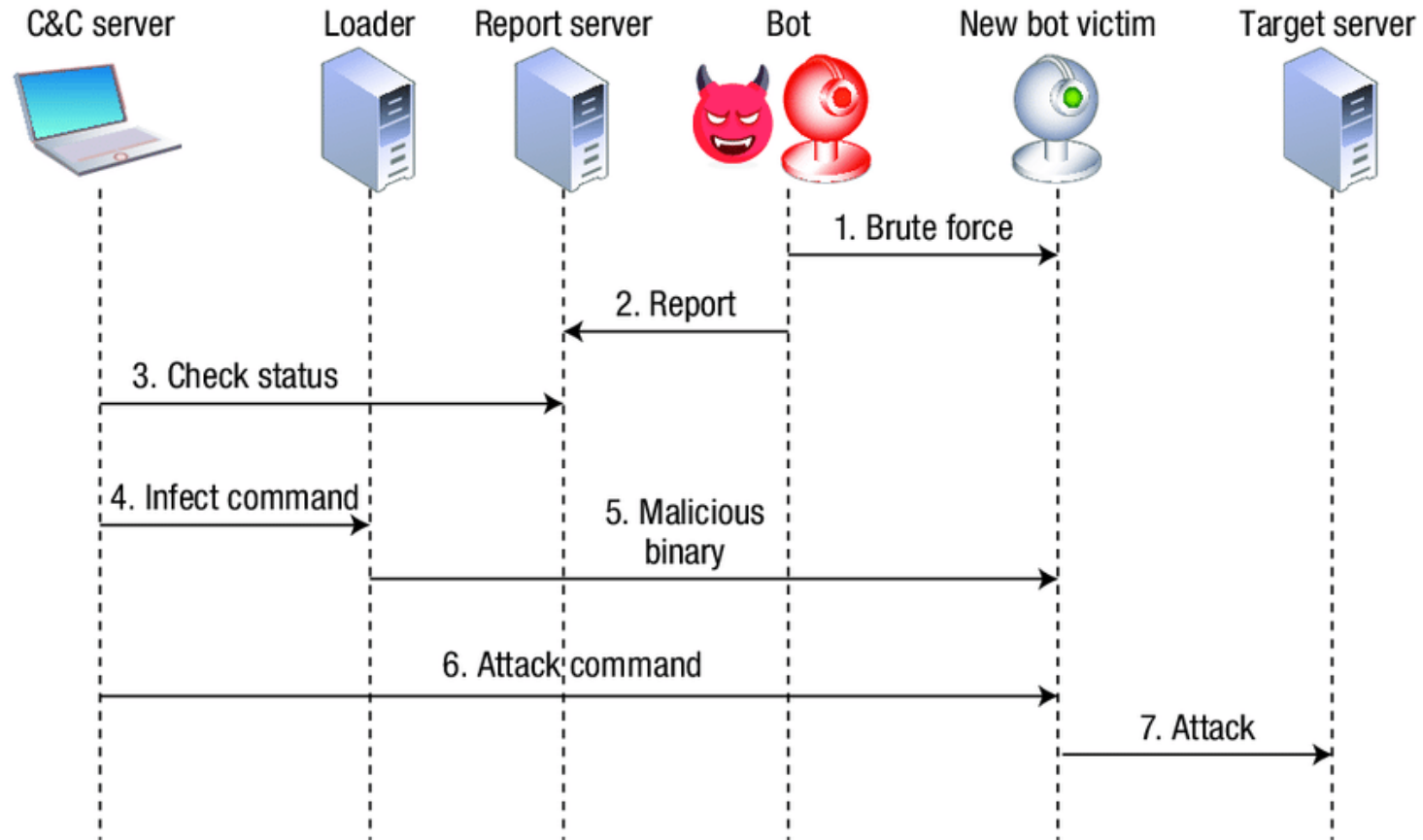
- Evento, exitoso ó no, que atenta sobre el buen funcionamiento del sistema.
- Intento, exitoso ó no, de vulnerar un “control” de seguridad del sistema.

Ciberataque Wannacry

- Shadow Brokers extrae ciberarmas de la NSA
- 12 de Mayo 2017 inicia el ataque Wannacry
- + 230k ordenadores en 150 países (Rusia, Ucrania, India y Taiwan)
- NHS, Telefónica, Fedex, Latam, ISA, Banco de China, Banco Nacional de India
- Exploit EternalBlue (CVE-2017-0144) - smb
- Parche ms17-010
- Secuestro de información por 300 USD en bitcoins



Botnet IoT - Mirai



Amenazas cibernéticas



Impactos de incidentes de ciberseguridad

Incremento del **10%**
del costo de una
brecha de datos

El costo de
la brecha de
seguridad
aumento de
\$3.86 m a
\$4.24 m

La diferencia de costo
del incidente por
trabajo remoto es
\$1.07 m

El costo
promedio
del
incidente
fue **\$1.07 m**
más alto

El costo por datos
personales por
registro es de **\$180**

Los datos
personales
son el tipo
de registro
más costoso
\$180

Los costos son dólares americanos

Impactos de incidentes de ciberseguridad

38% de pérdida de participación de mercado por brecha de datos

La pérdida de participación de mercado aumento de \$1.52 m a \$1.59 m



Gestión Integral de las Amenazas

Digitales

Malware

Sniffing

Hacking

Humanas

Fraude

Robo de
información

Naturales

Terremotos

Inundaciones

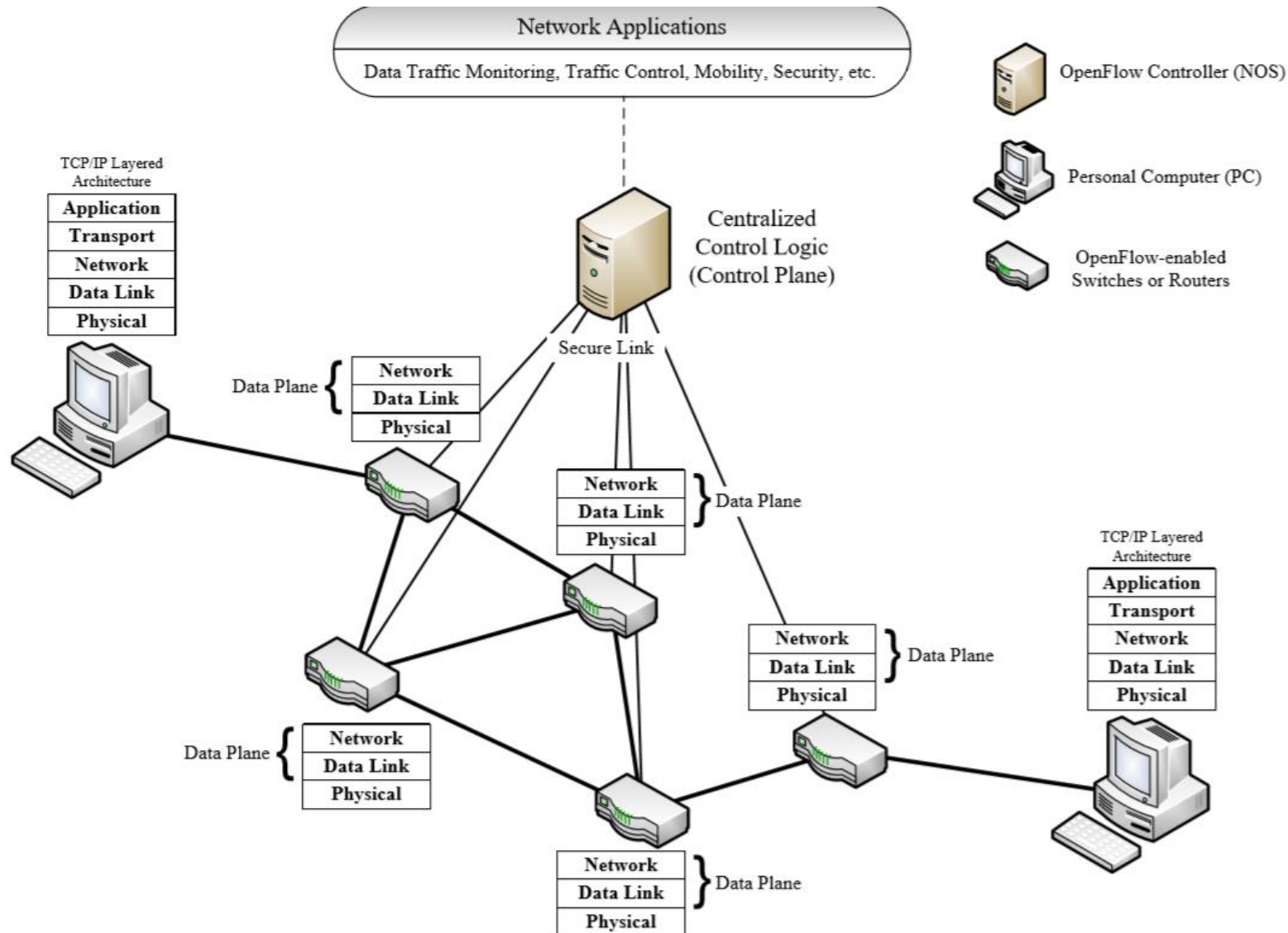
Vulnerabilidad

- Una Vulnerabilidad es una **debilidad** en la seguridad de la información que **podría ser explotada por una amenaza**; esto es, una debilidad en la seguridad de su red, sistemas, procesos y/o procedimientos.
- **Posible materialización de una amenaza** sobre un activo de información.

Una vulnerabilidad puede presentarse a - TI- Procesos- Hum

Cuando un proceso procesa varias funciones

¿Qué puede ser Vulnerable?



¿Qué puede ser Vulnerable?




← → ↻ ⚠ No es seguro | demo.testfire.net

🔍 📄 ⚙️ ⚡ 🔌 🌐 📶



[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search



ONLINE BANKING LOGIN	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
<p>PERSONAL</p> <ul style="list-style-type: none">Deposit ProductCheckingLoan ProductsCardsInvestments & InsuranceOther Services <p>SMALL BUSINESS</p> <ul style="list-style-type: none">Deposit ProductsLending ServicesCardsInsuranceRetirementOther Services <p>INSIDE ALTORO MUTUAL</p> <ul style="list-style-type: none">About UsContact UsLocationsInvestor RelationsPress RoomCareersSubscribe	<p>Online Banking with FREE Online Bill Pay</p> <p>No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.</p>  <p>Real Estate Financing</p> <p>Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it</p>	 <p>Business Credit Cards</p> <p>You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.</p> <p>Retirement Solutions</p> <p>Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.</p>	<p>Privacy and Security</p> <p>The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.</p>  <p>Win a Samsung Galaxy S10 smartphone</p> <p>Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.</p>

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2022 Altoro Mutual, Inc.

This web application is open source! [Get your copy from GitHub](#) and take advantage of advanced features.

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www-142.ibm.com/software/products/us/en/subcategory/SWI10>.

Copyright © 2008, 2022, IBM Corporation, All rights reserved.

<http://demo.testfire.net/>

Ejemplo de Vulnerabilidad

- Una Contraseña “típica”
- Un Sistema Operativo que no ha sido parchado
- Un Antivirus con firmas desactualizadas
- Un “Access Point” instalado por un empleado
- Una PC desatendida

Riesgo

- Incertidumbre en la consecución de los objetivos.
- En seguridad de la información, el riesgo es la **exposición a una posible pérdida o daño** sobre los activos de información que puede ser ocasionada desde dentro o fuera de la organización.

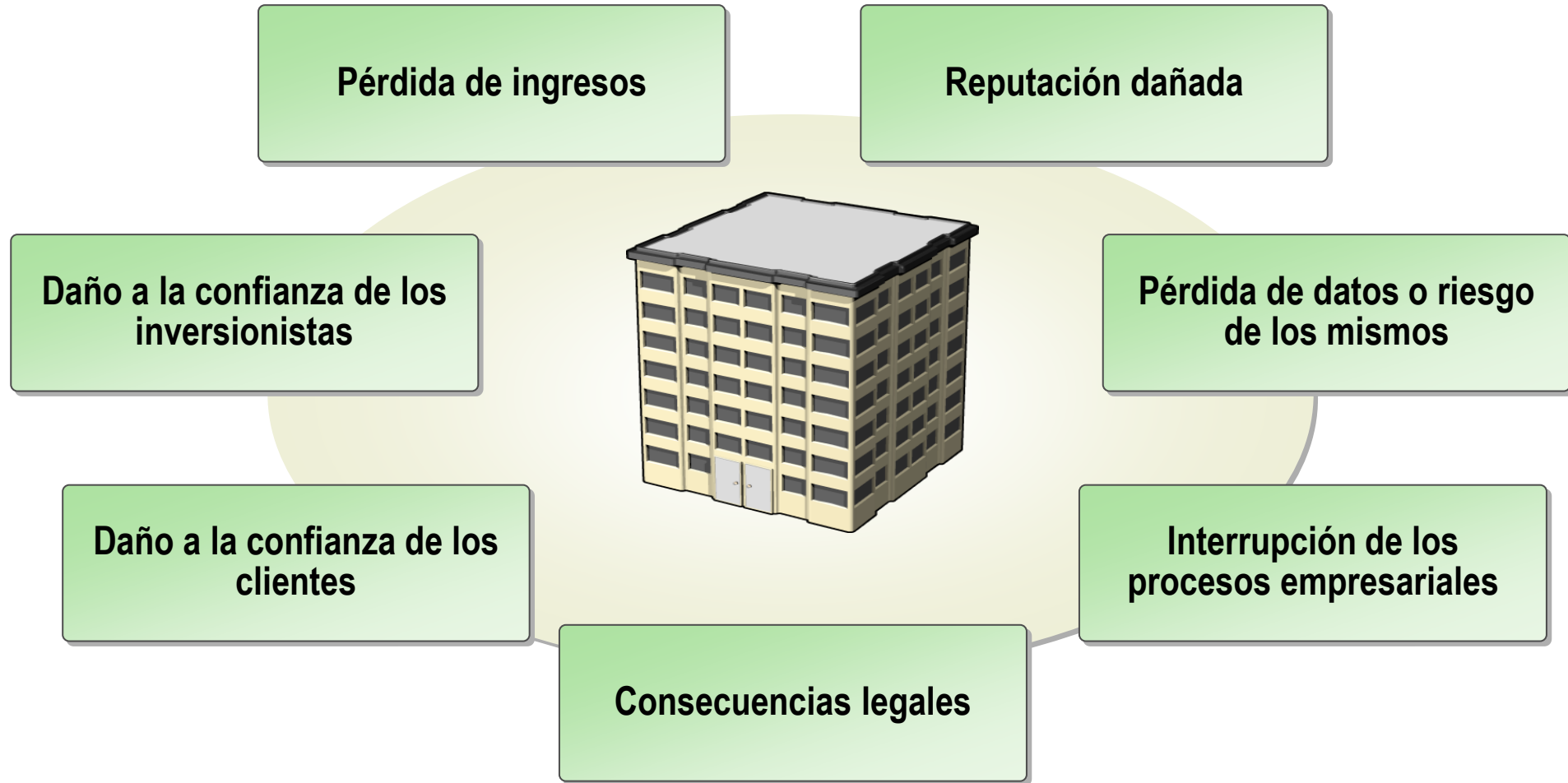
Frecuencia o Probabilidad

- Los riesgos que se pueden materializar en un periodo de tiempo.
 - Frecuencia: Cantidad de eventos materializados en un periodo de tiempo.
 - Probabilidad: Estimación de ocurrencia de un evento.

Impacto

- Consecuencia de la materialización de una amenaza.
- Puede ser de carácter **tangible** ó **intangible**.
- Puede estar limitado a un activo, un sistema, un entorno operativo ó abarcar la organización y comprometer el negocio (**BIA, Business Impact Analysis**).

Impacto de las infracciones de Seguridad



Desastre ó Contingencia

- **Interrupción de la capacidad de acceso** a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio


Control

- Es un mecanismo que modifica el nivel de riesgo. (ISO 27000:2018)



III. conceptos de seguridad

Control de acceso

- Consiste en asegurar el acceso a los activos SOLO a personas autorizadas según las reglas de negocio y requisitos de seguridad.
- Los componentes del control de acceso son:
 - Identificación
 - Autenticación 
 - Autorización
 - Auditabilidad o Trazabilidad

Autorización

- Una vez que se ha “autenticado” a un usuario, se pasa a asignar **“permisos”** para el acceso a los recursos y para determinar el nivel de operaciones que puede llevarse a cabo.
- La asignación de permisos puede ser bastante complicada por la cantidad de usuarios ó de sistemas en operación
- Suele emplearse sistemas de **Gestión de Identidad** para mejorar la “autenticación” y la “autorización”

Autenticación

- Es el proceso de validar ó verificar que alguien es "**quien dice ser**"
- Puede emplear diversas estrategias de un factor ó multifactor:
 - Algo que sabes. Ej. La contraseña
 - Algo que tienes. Ej. Una tarjeta, un token.
 - Algo que eres. Ej. La voz, la retina, huella dactilar.

Trazabilidad

- Es la capacidad de poder establecer, con un nivel de confianza, la **procedencia**, realización ó autoría de una **transacción/operación** en determinado sistema
- Requiere el despliegue de mecanismos de **registro de actividad, bitácoras**, etc.
- A fin de ser aceptable por terceros, debería ser de carácter automático, de difícil manipulación

