INFO 2017 Tercer Congreso Internacional de Ingeniería Informática
RETOS Y PERSPECTIVAS DEL MUNDO DIGITAL

100 años PUCP

Taller:
Seguridad Digital (Normas Peruanas)

Mas allá de la Seguridad Digital….
SEGURIDAD DE LA INFORMACIÓN

Carlos Trigo Pérez

Sesión 2

Agenda

- Activos de información
- Análisis de riesgos de seguridad de la información
- Taller 2

¿Qué es un Activo?

- Cualquier cosa que tenga valor para la empresa.
  [ISO/IEC 27000]

¿Qué es un Activo de Información?

- Es todo aquello que genera, procesa y/o almacena la información necesaria para la operación y el cumplimiento de los objetivos de la empresa.
  - Tiene valor para la empresa.

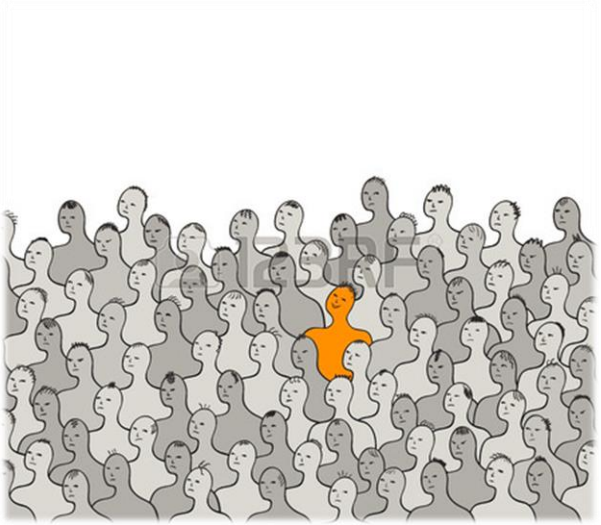
- Existen varios tipos:
  - Procesos
  - Documentos físicos y electrónicos
  - Software
  - Hardware
  - Personas

¿Cuáles son los recursos a proteger?

- La información es un activo, que como otros activos importantes, tiene un valor para la empresa y requiere en consecuencia una adecuada protección.

- La información adopta diversas formas:
  - Impresa o escrita en papel.
  - Almacenada electrónicamente.
  - Transmitida por correo o email.
  - Mostrada en video.
  - Hablada en conversación.

¿Una persona en particular puede ser un activo de información?



¿Los servicios de terceros son activos de información?

Categorías de Activos

Personas

conocimiento de las personas

Servicios

internet, correo, energía o de terceros

Físicos

computadoras, medios removibles

Software

aplicativos y software de sistemas

Información

contratos, guías, resoluciones, base de datos

Intangibles

imagen y marca, reputación

Atributos de los Activos

- Clasificación
- Marcado
- Ubicación
- Valorización
- Propietario
- Custodio

Propietario de la Información

- Es aquella persona o entidad que tiene la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

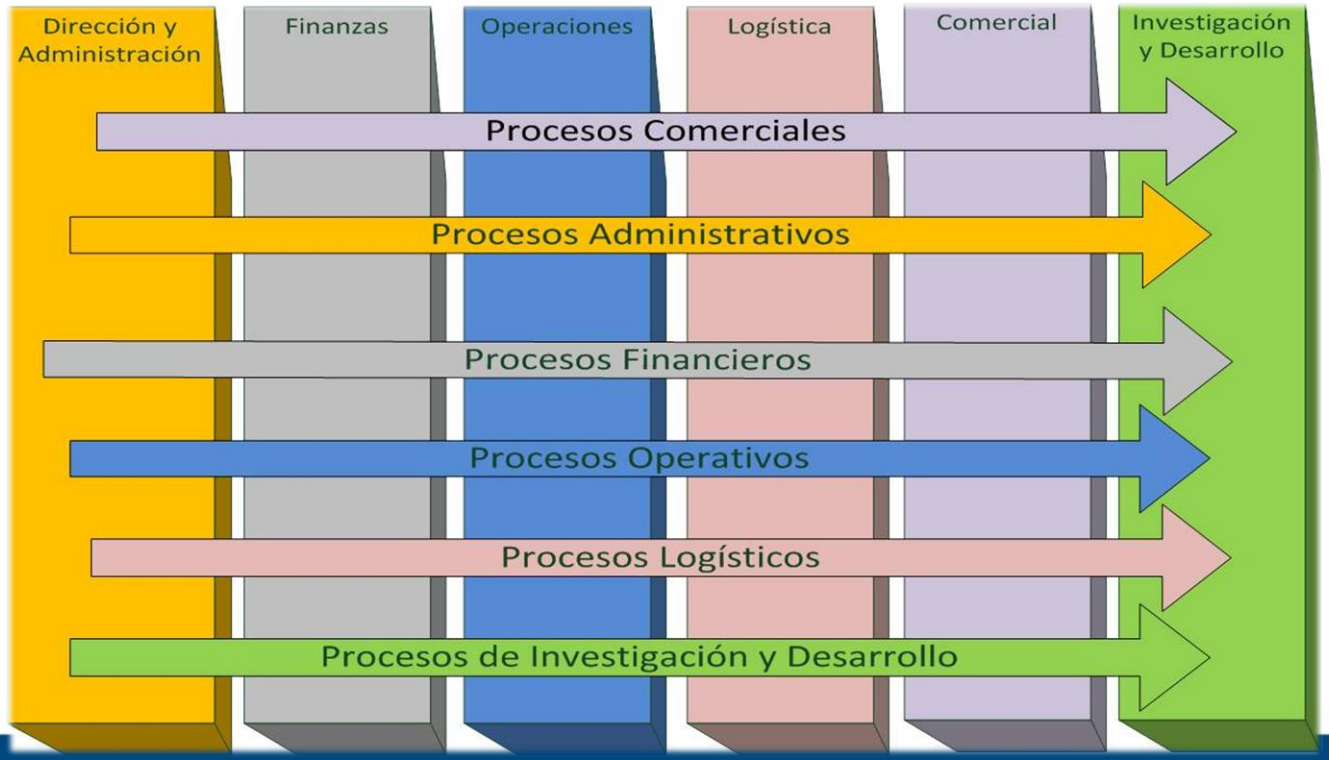
- Además es el responsable por definir apropiadamente la clasificación y los derechos de acceso a los activos de información, estableciendo los controles apropiados.

Custodio de la Información

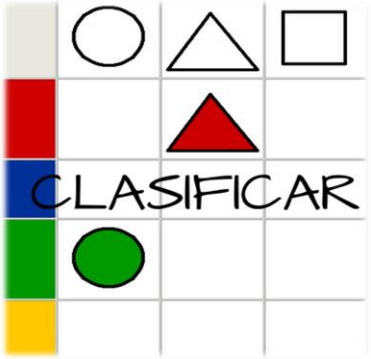
- Es aquella persona o entidad que mantiene bajo su responsabilidad, activos de información de la cual NO es el dueño o propietario.

Activos Transversales

- Los *Activos de Información Transversales* son identificados por sus respectivos propietarios y revisados por cada proceso, siguiendo lo establecido en la Metodología de Gestión de Riesgos.



¿Por qué es importante clasificar?



¿Cuáles son las clasificaciones de los activos de información?

Criterios de Clasificación de la Información

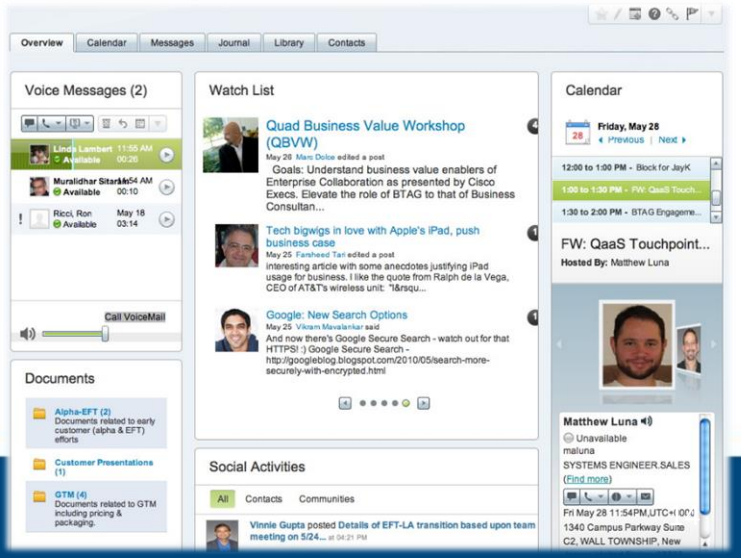
USO PUBLICO

- Es toda aquella información que ha sido explícitamente aprobada por la empresa para su diseminación publica.
- Ejemplos Genéricos: boletines de noticias, comunicados internos, presupuestos, memorandos, informes de prensa, entre otros.

Criterios de Clasificación de la Información

USO INTERNO

- Es toda aquella información cuya revelación no causaría daños a la empresa y su acceso es libre para los empleados.
- Ejemplos Genéricos: información publicada en la intranet de la organización, reglamento interno de trabajo, entre otros.



Criterios de Clasificación de la Información

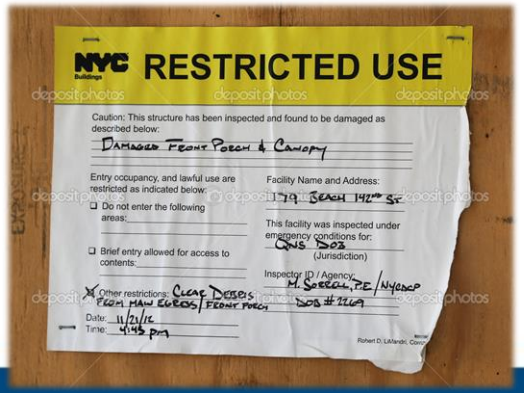
USO CONFIDENCIAL

- Es toda aquella información que debe ser estrictamente restringida basándose en el concepto de "necesidad de saber", su revelación requiere la aprobación de su propietario, es de uso exclusivo de la empresa, en el caso de terceros se deberá firmar acuerdo de confidencialidad y no divulgación.

Criterios de Clasificación de la Información

USO RESTRINGIDO

- Es toda aquella información cuyo acceso se da a un número reducido de personas. Usualmente, debe ir acompañada del principio de CONFIDENCIALIDAD.
- Esta debe ser manejada con todas las precauciones y controles posibles determinando exactamente que personas tienen acceso a la misma y vigilando su uso, transporte y almacenamiento.



ANALISIS DE RIESGOS

Conceptos

¿Qué es una AMENAZA?

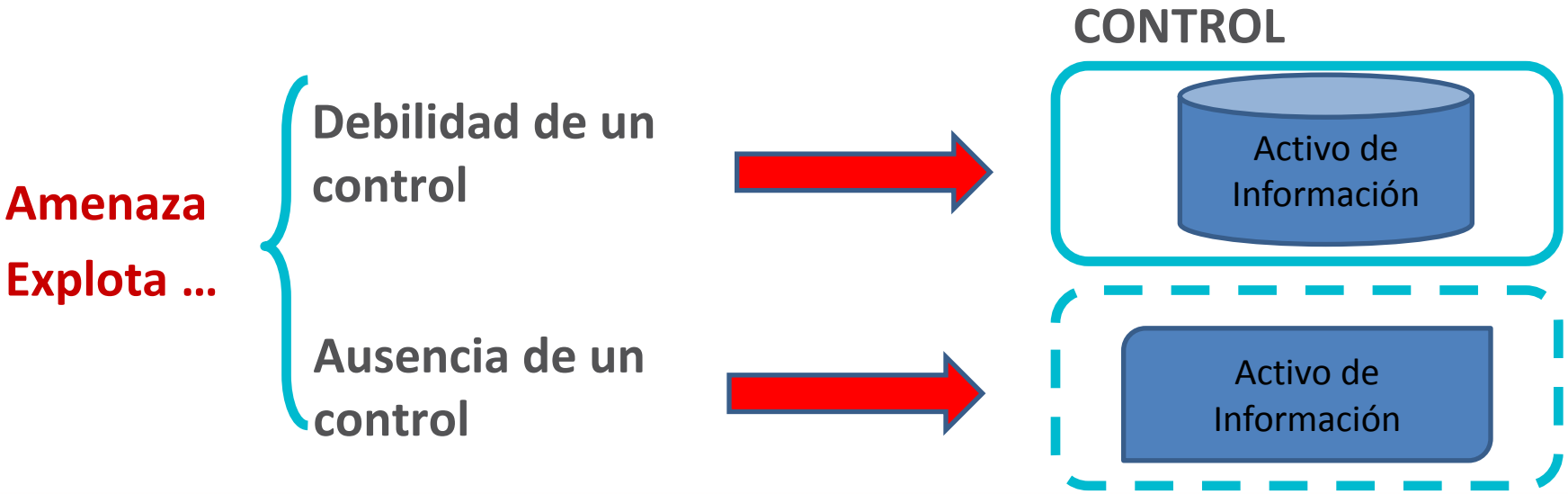
- Causa Potencial de un incidente no deseado que puede resultar en daño al Sistema, a la Organización o a sus Activos.
- Puede ser accidental o intencional.
- Los activos están sujetas a muchos tipos de amenazas:
  - *Desastres Naturales*: Terremoto, inundación, etc.
  - *Humanas*: Errores de Mantenimiento, huelga, etc.
  - *Tecnológicas*: Caída del Sistemas, falla de hardware.

¿Qué es una VULNERABILIDAD?

- Es la debilidad o ausencia de control de un Activo de Información que puede ser aprovechada (explotada) por una Amenaza.
- Son ejemplos de vulnerabilidad:
  - Control de acceso físico inadecuado
  - Falta de conciencia en Seguridad
  - Ausencia de Sistemas contra incendio

¿Qué es un VULNERABILIDAD?

- Las vulnerabilidades deben ser coherentes con la amenaza.
- Las vulnerabilidades pueden ser “explícitas” cuando se trata de ausencia de control o “implícitas” cuando existiendo el control éste puede fallar (debilidad del control).



¿Qué es un EVENTO DE RIESGO?

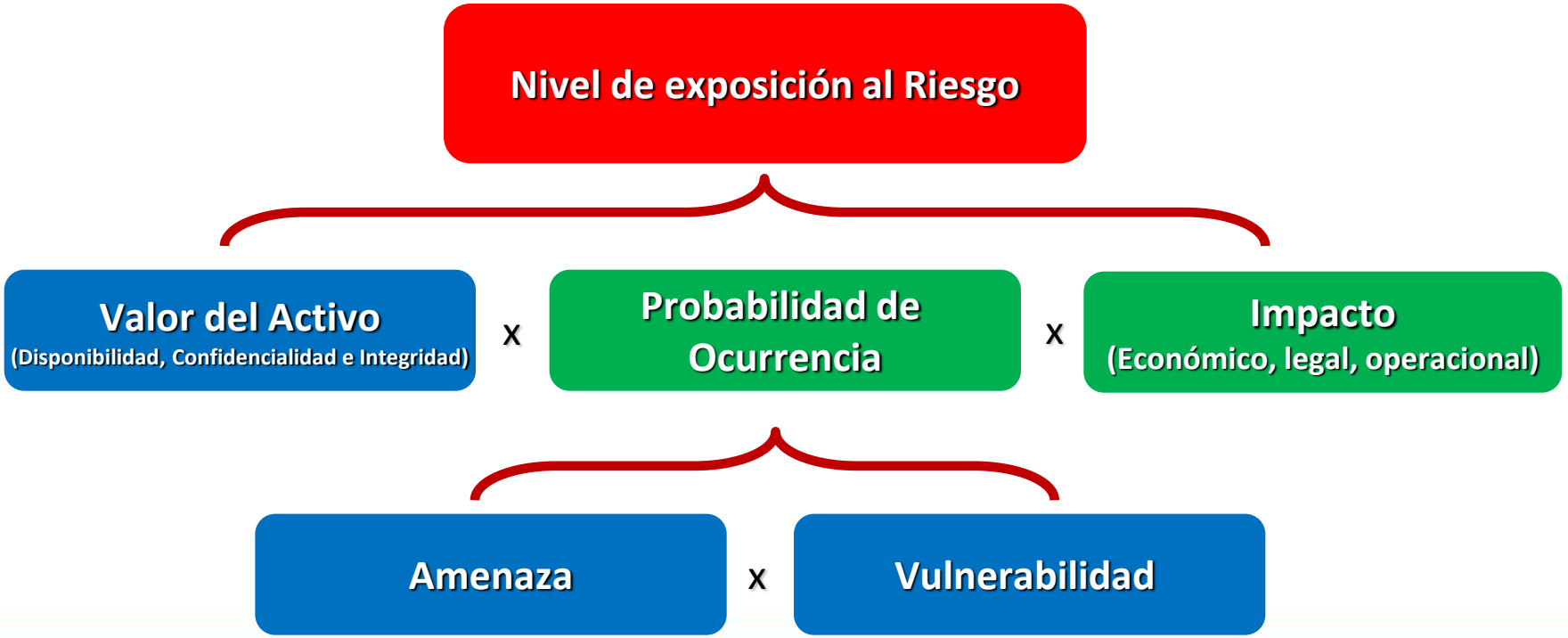
- Es la probabilidad de que una Amenaza vulnere un Activo, causando un impacto negativo.

PROBABILIDAD: Es la *frecuencia* con que se podría producir el *RIESGO* en un plazo determinado de tiempo.

IMPACTO: Son las *consecuencias* posibles al momento de materializarse un RIESGO.

¿Qué es un EVENTO DE RIESGO?

- Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar pérdida o daño en un activo de información (Según ISO 27001).



Probabilidad de ocurrencia

Probabilidad de Ocurrencia del Riesgo

Amenaza x **Vulnerabilidades**

Niveles de Amenaza	
Clasificación	**Descripción**
Muy Alto (5)	Una vez a la semana
Alto (4)	Una vez al mes
Medio (3)	Una vez cada 6 meses
Bajo (2)	Una vez al año
Muy Bajo (1)	Una vez cada 3 años

Niveles de Vulnerabilidad	
Clasificación	**Descripción**
Muy Alto (5)	No existen controles para contener la amenaza
Alto (4)	Existen controles pero no están documentados
Medio (3)	Existen controles documentados pero no son medibles
Bajo (2)	Existen controles medibles pero no son mejorados continuamente
Muy Bajo (1)	Existen controles mejorados continuamente

¿Cómo estimo el nivel de riesgo?

¿Cuántos valores hay según la metodología?

Nivel de Riesgo

Probabilidad de Ocurrencia del Riesgo

Niveles de Riesgo
Clasificación
Muy Alto (21-25)
Alto (16-20)
Moderado (11-15)
Menor (6-10)
Mínimo (1-5)

Amenaza x **Vulnerabilidades**

Niveles de Amenaza	
Clasificación	**Descripción**
Muy Alto (5)	Una vez a la semana
Alto (4)	Una vez al mes
Medio (3)	Una vez cada 6 meses
Bajo (2)	Una vez al año
Muy Bajo (1)	Una vez cada 3 años

Niveles de Vulnerabilidad	
Clasificación	**Descripción**
Muy Alto (5)	No existen controles para contener la amenaza
Alto (4)	Existen controles pero no están documentados
Medio (3)	Existen controles documentados pero no son medibles
Bajo (2)	Existen controles medibles pero no son mejorados continuamente
Muy Bajo (1)	Existen controles mejorados continuamente

"Se consideran los siguientes niveles de riesgos: **Muy Alto, Alto, Moderado, Menor y Minimo,** que establecen los criterios de aceptación del riesgo. Para la etapa de análisis y evaluación, se han considerado como aceptables los niveles **Moderado, Menor y Mínimo**"

Impacto

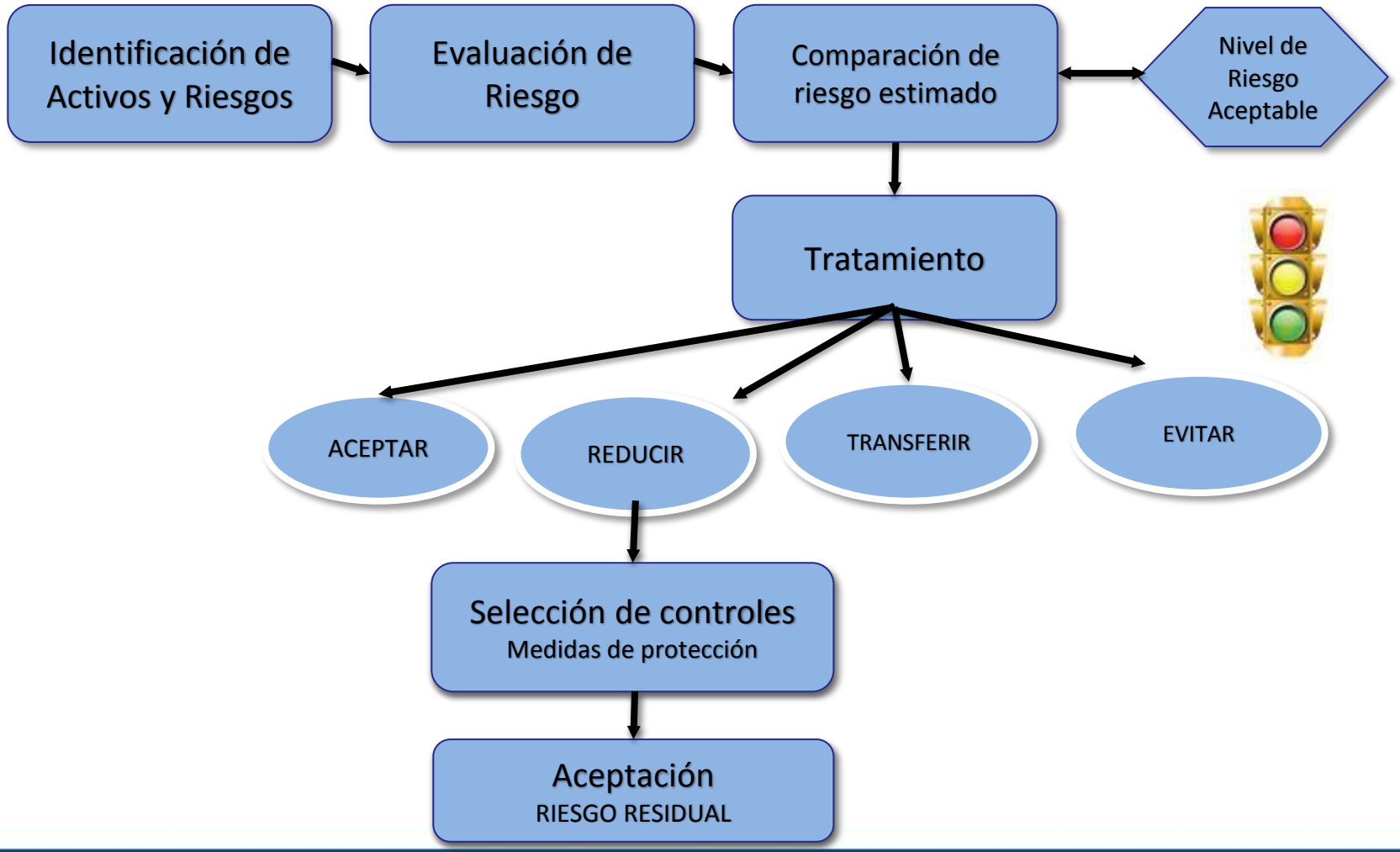
Impacto
(Económico, Legal, Operacional)

Niveles de Impacto			
Clasificación	**Legal**	**Operativo**	**Económico**
Muy Alto (5)	afecta irreversiblemente a la empresa	afecta irreversiblemente la operatividad de los procesos de la empresa	Afecta irreversiblemente a la empresa, ocasionando pérdidas cuantiosas, sin posibilidad de recuperación.
Alto (4)	afecta drásticamente a la empresa	afecta drásticamente la operatividad de los procesos de la empresa	Afecta drásticamente a la empresa con posibilidad de recuperación a costos elevados a largo plazo.
Medio (3)	afecta seriamente a la empresa	afecta seriamente la operatividad de los procesos de la empresa	Afecta seriamente a la empresa, con posibilidad de recuperación a costos intermedios a mediano plazo.
Bajo (2)	afecta parcialmente a la empresa	afecta parcialmente la operatividad de los procesos de la empresa	Afecta parcialmente a la empresa, con posibilidad de recuperación a bajo costo a corto plazo.
Muy Bajo (1)	no afecta a la empresa	no afecta la operatividad de los procesos de la empresa	No afecta económicamente a la empresa, con posibilidad de recuperación sin costo o con recursos disponibles.

Plan de tratamiento

- Plan de Acción que define las acciones para reducir los riesgos no aceptables e implementar los controles necesarios para proteger la información.

El análisis y evaluación de Riesgos



Control

- Todo elemento o medidas que permite reducir o eliminar la exposición al RIESGO de cada Activo.

¿Cómo desarrollar el Plan de Tratamiento de Riesgos?

- Comprender que los riesgos se tratan aplicando controles de seguridad de la información los cuales se encuentran contenidos en el anexo “A” de la norma ISO 27001.
- Comprender los criterios de tratamiento a fin de definir controles cuya implementación sea realista y responda positivamente a un análisis costo/beneficio.
- Trabajando en conjunto a fin de consensuar las expectativas de seguridad de la información.

Criterios a considerar para seleccionar controles

- Riesgo
- Grado vs impacto
- Facilidad de implementación (Tiempo, costo)
- Servicios asociados y riesgos comunes a diversos activos
- Exigencias legales y regulatorias
- Exigencias de clientes u otras relaciones contractuales
- Considerar el costo de mantenimiento del control
- Desarrollar opciones preventivas y previas a la planificación (costo/beneficio)
- Mejorar los controles existentes

Taller #2: Activos de información

- *Instrucciones*:

1) Con su grupo de hasta 5 miembros ya formado, y considerando como ambiente la Universidad, identifique y describa lo mas detallado que pueda por lo menos tres Activos de información que considere (subjetivamente) de importancia y valor para la universidad e indique en cual de las 6 categorías definidas se ubica cada uno (ver diapositiva 7).

- *Tiempo*: 35 minutos.

FIN

Carlos Trigo Pérez
trigoperezc@gmail.com