Riesgos

En este curso, a nivel general, se va a tomar en cuenta ciertos conceptos. Porque todo lo que se trata aquí está en función también del análisis de riesgos.

En la clase anterior hablábamos sobre algunos conceptos básicos: tipos de amenazas y cómo evitarlas o mitigarlas. Amenazas que pueden convertirse en incidentes relacionados con interrupciones, interceptaciones, modificaciones o incluso destrucción de información.

Todo eso responde a controles que se deben aplicar para prevenir eventos no deseados. La pregunta clave es: **¿Qué pasaría si se concreta una amenaza? ¿Cuál sería el impacto?** Ya sea por un ataque informático o la materialización de cualquier otra amenaza, la respuesta a esa pregunta constituye la base del tratamiento del riesgo.

El tratamiento del riesgo es esencial en toda organización, en todos los niveles. No se trata solo de riesgos informáticos: también hablamos de riesgos laborales, financieros, entre otros. El riesgo es un tema transversal. Lo van a ver en diferentes cursos, como Gestión de Proyectos (donde se habla de riesgos asociados a cronogramas, recursos, etc.) o Gestión de Servicios.

Análisis de Riesgos

En cualquier ámbito de una organización, siempre existirán riesgos, y para nuestro caso en particular, nos enfocamos en los riesgos asociados específicamente al **activo de información**.

Entonces, ¿qué es un riesgo?
¿Contra qué nos protegemos?
¿Qué pasaría si se concreta una amenaza?
¿Cómo mitigamos o reducimos ese riesgo?
¿Podemos eliminarlo completamente?

Técnicamente, sí se puede eliminar un riesgo... pero eso implicaría eliminar también el activo. Es decir, para que no exista ningún riesgo, no debería existir el activo, y eso no es viable. Por lo tanto, **el riesgo cero no existe**. Siempre habrá una posibilidad latente de que ocurra una amenaza, un ataque, un incidente o una falla.

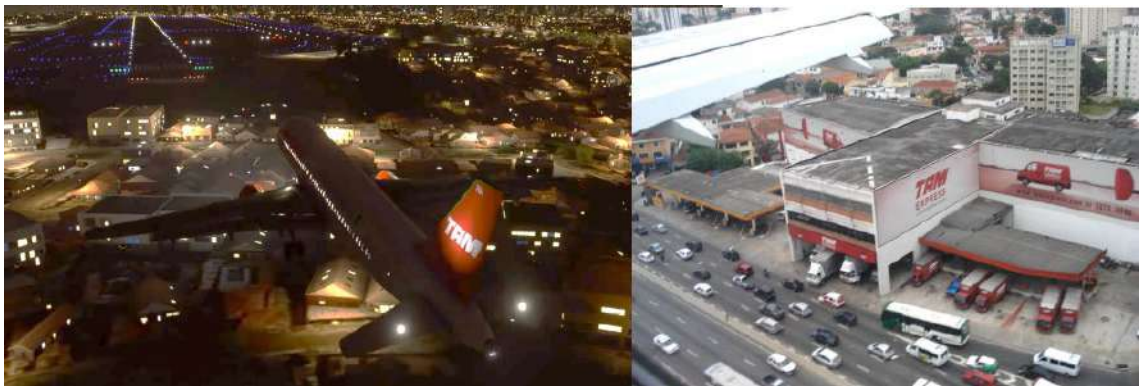
Sucesos

Y aquí es donde les hablaba de ciertos escenarios que representan esta idea de riesgo: por ejemplo, **los aeropuertos**.

¿Por qué muchos aeropuertos han sido construidos fuera de las ciudades?
Primero, por condiciones geográficas: se necesita una zona amplia para aterrizajes y despegues. Pero también se busca evitar posibles impactos si ocurriera un accidente. Recuerden que los momentos de más riesgo en un vuelo son el despegue y el aterrizaje.

Entonces, al construir un aeropuerto lejos del centro urbano, se busca proteger a la población de posibles daños colaterales.
Sin embargo, en muchas ciudades del mundo, con el paso del tiempo, las zonas urbanas se han expandido hasta rodear completamente el aeropuerto, como sucede en Surco, por ejemplo. Ahora los aviones pasan prácticamente sobre las casas, las tiendas, las autopistas.

Y si ocurre un accidente, no solo se afecta al avión o al aeropuerto, sino también a toda la zona alrededor. Esto es lo que se llama **impactos colaterales** o **daños adicionales**.



Bueno, entonces... ¿cómo se mitigan los impactos? ¿Qué se hace realmente para reducirlos? ¿En qué medida se toman acciones?

Aquí es donde entra otro concepto importante: **los controles**. ¿Qué controles o salvaguardas se aplican para mitigar riesgos o minimizar daños? La idea es reducir el impacto y asegurar que la organización o empresa siga funcionando.

PELIGRO PARA LOS NIÑOS

Mattel retira 18,2 millones de juguetes

Es la segunda vez en dos semanas que la multinacional alerta de la presencia de plomo en la pintura en algún modelo - En España se distribuyeron medio millón de artículos con imanes peligrosos

---

EFE | LILA PÉREZ GIL

Madrid / Nueva York - 14 AGO 2007 - 17.00 PET

Son muchas preguntas que quedan flotando, pero nos ayudan a ampliar el panorama. Existen diversos tipos de incidentes y riesgos, que pueden observarse en distintos niveles: desde la infraestructura y el transporte, hasta objetos cotidianos. Por ejemplo, los juguetes para niños con presencia de plomo representan un riesgo para la población infantil.

Ciberataque mediante *ransomware* al sistema de oleoductos Colonial Pipeline en Estados Unidos

Ciberataque a Colonial Pipeline

10 idiomas

Artículo Discusión Leer Editar Ver historial Herramientas

El **ciberataque de Colonial Pipeline** tuvo lugar entre el jueves 6 de mayo y el viernes 7 de mayo de 2021, cuando Colonial Pipeline sufrió un ataque de malware que los obligó a cerrar su sistema.[1] El ataque detuvo todas las operaciones del oleoducto.[2] Colonial Pipeline dijo que el ataque afectó a algunos de sus sistemas de información. El presidente Joe Biden declaró el estado de emergencia el domingo 9 de mayo.[3] Politico dijo que fue «lo que se cree que es el mayor ciberataque exitoso a la infraestructura petrolera en la historia del país» y una fuente le dijo que el ataque fue llevado a cabo por una empresa criminal de ransomware llamada DarkSide, y no por un gobierno extranjero.[4] Se cree que el mismo grupo robó 100 gigabytes de datos de los servidores de la empresa el día antes del ataque de malware.[5]

Ciberataque a Colonial Pipeline de 2021

Mapa de los oleoductos controlados por Colonial Pipeline y que se vieron afectados por el ciberataque.

Ahora, si nos acercamos más al ámbito de nuestra carrera, tenemos casos como **los ciberataques**. Un ejemplo es el ocurrido en la red de oleoductos de EE. UU. en 2021. No solo se atacan páginas web o bancos, también se comprometen **infraestructuras críticas**.

¿Qué es una infraestructura crítica? Son aquellas que sostienen el funcionamiento básico de un país: telecomunicaciones, agua potable, energía eléctrica, petróleo, etc. Muchas de estas infraestructuras están controladas por dispositivos informáticos conectados entre sí mediante redes industriales (también llamadas redes operacionales).

Estas redes operacionales suelen tener una **interfaz con la red informática**, lo que puede exponer ciertos dispositivos a internet. No necesariamente se expone el equipo que controla directamente un proceso industrial, pero sí aquellos que actúan como **interfaz hombre-máquina**. Es decir, dispositivos desde donde se puede monitorear o interactuar con los sistemas.

Un ejemplo de exposición es el de las **cámaras conectadas al internet de las cosas (IoT)**. Hace unos años, era común encontrar cámaras de videovigilancia accesibles desde internet simplemente con buscar su IP y acceder vía HTTP o HTTPS, ya que muchas usaban credenciales por defecto (como "admin / admin").

Aunque hoy muchas marcas han mejorado su seguridad, **todavía se encuentran dispositivos mal configurados** o con accesos inseguros.


Sucesos

PORTADA / ACTUALIDAD

Reniec denunció al Mininter y MTPE por uso indebido de su información

Forbes Staff | abril 5, 2025 @ 8:28:58 am

COMUNICADO

RENIEC desmiente hackeo y denuncia al Ministerio del Interior por uso indebido de datos

El Registro Nacional de Identificación y Estado Civil (RENIEC) se dirige a la ciudadanía para aclarar lo siguiente:

1. No ha existido hackeo ni ataque a nuestros servidores informáticos. La exposición de datos reportados recientemente **no fue producto de una vulneración a la seguridad del RENIEC**, sino del uso indebido de un usuario del Ministerio del Interior (Mininter).
2. **RENIEC actuó de inmediato.** A inicios de marzo, al detectar esta grave irregularidad, suspendimos el servicio al Mininter y denunciamos los hechos ante la Fiscalía de la Nación y la Autoridad Nacional de Protección de Datos Personales del Ministerio de Justicia. Asimismo, comunicamos esta situación a la Presidencia del Consejo de Ministros (PCM), la Secretaría de Gobierno y Transformación Digital (SGTD) y al propio Ministerio del Interior, entidad a la que también hemos denunciado por estos hechos.
3. Actualmente, el Mininter **no cuenta con acceso al servicio**, hasta que incorpore las medidas de seguridad de información exigidas por el RENIEC.
4. Asimismo, hacemos de conocimiento que el RENIEC también cortó este servicio al Ministerio de Trabajo y Promoción del Empleo por el **uso indebido de uno de sus usuarios**, hecho que ya fue denunciado ante las autoridades correspondientes.

Continuaremos fiscalizando a todas las entidades que por Ley acceden al servicio en línea del RENIEC; por lo que, les demandamos nuevamente adoptar todas las medidas de seguridad de la información y supervisar el uso que sus usuarios hacen de esta data; caso contrario, ante la detección de un mal uso se realizará el corte definitivo de consultas de información del RENIEC.

Lima, 4 de abril de 2025

RENIEC

Estas vulnerabilidades permiten ataques o incidentes que afectan directamente a las organizaciones. Un caso reciente ocurrió en Perú, donde se descubrió que **datos personales estaban siendo vendidos o expuestos en foros de la web**. Se trató de una exposición indebida a través del uso de una API del Ministerio, que accedía a datos de RENIEC. Al parecer, esa API fue mal utilizada y permitió acceder a información sensible.

Lo que se conoce hasta ahora es que se utilizó una cuenta asociada al Ministerio para consumir datos de manera indebida. Aquí surgen preguntas como:

- ¿Qué tipo de datos se estaban accediendo?
- ¿Qué nivel de responsabilidad tiene la institución al compartir esta información vía API?

Como ya comentamos en clases anteriores, estos incidentes de **exposición innecesaria de datos** revelan los riesgos que enfrentamos en el manejo de información sensible. Y en este caso específico, el riesgo no está en la imagen del DNI como tal, sino en **la exposición de los datos personales de los ciudadanos**, debido a la forma en que se comparte y se accede a dicha información.

Y así… datos como: voto, fecha de nacimiento, estado civil, dirección, nombre del padre, nombre de la madre… incluso, en algunos casos, hasta la **firma digital**. Todo esto representa una afectación directa a los **datos personales**.

Vamos a continuar con algunas definiciones adicionales. Hablábamos de los **activos**. ¿Qué son los activos?
Un activo es **cualquier componente o funcionalidad que puede verse afectado, dañado o impactado, pero que tiene valor para la organización**.

“no sería un activo de información si no tuviese valor para la empresa”.
Si no tiene valor, simplemente **no se invierte nada en su protección**. En cambio, si tiene valor, se le asignan recursos: presupuesto, tiempo, mecanismos de seguridad, etc.

La cantidad de recursos que se le va a dedicar depende **del valor del activo**. Cuanto más valioso sea, mayor será la inversión en soluciones, mecanismos y controles. En cambio, si no tiene ese valor, se descarta.

Otro concepto es la **amenaza**, que se define como **todo factor o posibilidad que puede causar un daño a un sistema**, especialmente a un activo o sistema de información.

Y luego está el **impacto**, que es lo que realmente se siente si esa amenaza se concreta.
Es decir:

- ¿Qué tanto daño genera?
- ¿Qué tan fuerte golpea a la empresa u organización?
- ¿Qué consecuencias trae si una amenaza se vuelve real?

La **salvaguarda** o **control**, por su parte, es el mecanismo aplicado para mitigar ese riesgo. Puede ser un control tecnológico, legal, normativo, operativo, software, hardware, etc.

Su objetivo es claro:

- Prevenir que la amenaza se concrete.
- O, si no puede evitarse, **minimizar el daño** o **controlar el impacto**.

¿Y qué salvaguardas aplicamos nosotros a nivel personal? Por ejemplo:

- Vitaminas
- Vacunas
- Buena alimentación
- Abrigarse en climas fríos
- Dormir bien
- Lavarse las manos
- No exponerse innecesariamente a contagios

Todas estas medidas son **controles o salvaguardas que aplicamos para no enfermarnos o evitar consecuencias mayores**.
Cuanto más vulnerable sea alguien, más controles se aplican. Algunos son más resistentes al frío o a enfermedades, otros necesitan cuidarse más. Lo mismo pasa con los **sistemas informáticos y los activos de información**.

Definiciones

Activos

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. (UNE 71504:2008)

Los activos de información deben ser protegidos porque son esenciales para la organización. Aplicamos controles para que las amenazas que circulan en el entorno **no generen un daño grave**.

Amenaza

Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. (UNE 71504:2008)

Si una amenaza se concreta, los sistemas con buenas salvaguardas **resisten mejor**, se recuperan más rápido o sufren menos daño.

Esto nos lleva a la idea de **resiliencia**, es decir, la capacidad de un sistema (o persona) para recuperarse ante una adversidad.

En resumen, el **riesgo** es eso:
Es **la probabilidad de que algo pase** y **la magnitud del daño si pasa**. Todo lo que hacemos en seguridad informática **gira en torno al riesgo**.

Impacto

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. (MAGERIT v3)

Salvaguarda

Se definen las salvaguardas o contra-medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se controlan simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otras, seguridad física y, también, las políticas de personal.

Medidas de protección desplegadas para que aquellas amenazas no causen [tanto] daño.

Si no sabemos qué cuidar, no sabremos **a qué aplicar salvaguardas o controles**.
Y si no identificamos las amenazas, no podremos proteger adecuadamente los activos.

Riesgo(lo que probablemente pase)

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización (MAGERIT v3).

El riesgo surge de la incertidumbre y genera más incertidumbre (PMI, 2022)

Apetito de Riesgo

El apetito al riesgo expresa el nivel de riesgo que la organización está dispuesta a asumir en pos de los objetivos. A medida que las organizaciones crecen, se expanden y evolucionan, también lo hacen los riesgos que enfrentan. El tipo, la prominencia y el apetito por los riesgos cambian en diferentes momentos del ciclo de vida de una organización.

Entonces tenemos:

- El **activo**: lo que queremos proteger
- La **amenaza**: lo que puede afectarlo
- La **salvaguarda** o **control**: lo que aplicamos para evitar o minimizar el impacto
- El **riesgo**: la combinación de probabilidad y consecuencia
- Y el **apetito o tolerancia al riesgo**: cuánto está dispuesta una empresa o persona a aceptar o asumir un impacto si se concreta una amenaza

Por ejemplo, algunos bancos optan por recomendar, pero no exigir, el uso del segundo factor de autenticación en sus aplicaciones web. Eso refleja su **nivel de tolerancia al riesgo**.

Por ejemplo, Hacer que algunos usuarios no se sientan cómodos o convencidos de usar la app, por lo que algunas empresas optan por **quitar esa exigencia** y dejar el sistema con factores menos seguros, como solo el correo electrónico o una contraseña básica.

¿Qué sucede entonces?
Esa decisión implica **asumir un mayor riesgo**. Están priorizando la experiencia del usuario por encima de la seguridad. Esa es su **posición frente al riesgo**.

Esta postura refleja su **nivel de apetito o tolerancia al riesgo**. Si deciden no implementar controles estrictos, están diciendo: *"Estoy dispuesto a asumir las consecuencias de un incidente"*. Esto eleva el nivel de riesgo.

En contraste, otras organizaciones son menos tolerantes al riesgo. Implementan todos los controles posibles, buscando minimizarlo. La **tolerancia al riesgo cambia según factores como:**

- El sector donde opera la organización
- El valor de los activos que protege
- Su cultura institucional

No es lo mismo que una universidad proteja los datos personales de sus alumnos, a que una fuerza armada proteja la identidad de sus agentes. El nivel de protección y tolerancia es diferente.

Cálculo del Riesgo

¿Cómo se calcula el riesgo?

El riesgo se calcula a partir de dos variables:

1. **La probabilidad de ocurrencia** de una amenaza: que te roben, que haya una lluvia intensa, un ataque informático, una intrusión física, un malware, etc.
2. **El impacto**: el nivel de daño que causaría si esa amenaza se concreta.

Fórmula general del riesgo:

Riesgo = Probabilidad x Impacto

Cuanto mayor sea la probabilidad y cuanto más grave sea el impacto, **mayor será el riesgo**. Esta es una relación directamente proporcional.

Este análisis permite determinar qué riesgos son **críticos, altos, medianos, bajos o mínimos**. Para ello, se pueden usar **enfoques cualitativos** (como alto, medio, bajo), pero también se pueden traducir a **valores cuantitativos**, asignando números a cada nivel. Eso facilita cálculos y define **umbrales para priorizar riesgos**.

¿Qué es el "apetito de riesgo"?

El **apetito de riesgo** es el nivel de riesgo que una organización está dispuesta a aceptar. No todas tienen el mismo. Algunas lo minimizan al máximo; otras lo asumen con más apertura.

La **inteligencia de amenazas** es una disciplina de la seguridad informática que busca **anticiparse a posibles amenazas**, incluso aquellas **desconocidas o poco evidentes**, mediante monitoreo, análisis de patrones y aprendizaje constante.

Análisis de Riesgos

Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Gestión de Riesgos

Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

El análisis y gestión de riesgos no es un FIN en sí mismo, es parte de las actividades de GESTION DE LA SEGURIDAD

Tratamiento o Respuesta al Riesgo

Tratamiento o respuesta al riesgo

Existen **cuatro formas** básicas de tratar o responder a un riesgo:

1. **Evitar el riesgo**
   Eliminar la amenaza o el activo. Como normalmente **no podemos eliminar una amenaza** (por ser externa), la forma más efectiva de evitar el riesgo es **eliminar el activo**.
   Ejemplo: si no quieres que te roben la laptop, no lleves la laptop. Suena extremo, pero es eliminar el riesgo al 100%.
2. **Transferir**

Entonces, el punto es que, si bien **evitar el riesgo** es una forma de tratamiento, **no siempre es posible**. No podemos simplemente eliminar nuestros activos o información valiosa solo para decir: "Ya no hay riesgo". Eso no es viable.

Lo real es que muchas veces **tenemos que enfrentar el riesgo**, y para eso necesitamos recursos: tecnología, personas, tiempo. Si no los tenemos, debemos buscar otras formas de mitigar el impacto.

Por ejemplo, imaginemos que tenemos un **centro de datos** con servidores, equipos y mucha información. ¿Qué pasa si ocurre un incendio, un terremoto o una inundación? ¿Cómo se recupera todo eso? ¿Cuánto costaría?

En casos como estos, lo que se suele hacer es **contratar un seguro**. Eso significa que estamos **transfiriendo el riesgo**: si algo pasa, no somos nosotros directamente los que nos encargamos de los daños, **sino la aseguradora**.

Lo mismo ocurre con los **seguros de vida**, **seguros contra accidentes**, incluso **seguros para mascotas**, autos o bienes materiales. Si ocurre un incidente, **el afectado no asume toda la carga**, sino que **la empresa aseguradora** se hace cargo, ya sea compensando, reponiendo o restaurando lo que se ha perdido.

Este tipo de tratamiento del riesgo (la **transferencia**) se utiliza cuando **no contamos con los medios necesarios** (tecnología, infraestructura, logística) para afrontar una amenaza de manera directa.

Entonces, pagamos una póliza mensual o anual, cuyo monto depende del valor del activo que se quiere asegurar.

4. Aceptar

En cambio, también existe otro tratamiento: la **aceptación del riesgo**.

Esto ocurre cuando, evaluando el posible daño, decidimos que **no vale la pena invertir** en mitigación. Es decir, aceptamos que algo puede pasar, pero **el impacto sería tan pequeño que no compensa el gasto en controles**.

3. Mitigar

Este tratamiento se aplica únicamente a riesgos con **impacto mínimo o tolerable**.

Ejemplo: imagina que no compras un seguro para tu tarjeta de débito porque sabes que **no tienes mucho dinero en ella**. Si te la roban, pierdes poco. En ese caso, pagar un seguro saldría **más caro que la posible pérdida**, así que **aceptas el riesgo**.

Lo mismo podría pasar con otros objetos o servicios de bajo valor: preferimos **no invertir en protección** y asumimos la posible pérdida.

En resumen, **aceptar el riesgo significa no tomar acciones adicionales**, no invertir en recursos, tecnología ni controles, porque **el costo de hacerlo supera el valor del activo o el impacto esperado**.

Como decía, antes usábamos celulares antiguos que solo servían para llamar, no almacenaban información personal. En ese caso, si perdías el equipo, el **riesgo era menor**. No había mucho que proteger, por lo tanto, se **aceptaba el riesgo**.

Esto aplica igual para cualquier activo. **Si el activo tiene valor, se le asignan recursos** para protegerlo: controles, salvaguardas, medidas tecnológicas. Pero si no tiene valor o si se considera que la pérdida no afectará, se opta por **aceptar el riesgo**.

Por ejemplo, si una persona dice: “Yo solo usaba ese celular para llamadas, no guardaba nada importante", entonces acepta la pérdida del equipo sin mayor preocupación. No hay inversión en protección, porque el impacto es mínimo.

Lo mismo ocurre en el mundo empresarial. Hay cierta información que, **por su naturaleza**, no es prioritaria o valiosa. Entonces, no se invierte en su protección. Se hace una evaluación de **costo-beneficio**: lo que podrían perder si ocurre un incidente **vs.** lo que ganan si no complican la experiencia del usuario.

Por eso muchas empresas, como bancos u operadoras, **trasladan el riesgo al cliente**. Si pierdes tu tarjeta o tus datos, lo pagas tú. Ellos no admiten fallas en sus aplicaciones; la responsabilidad siempre recae en el usuario. Pero en realidad, eso es una **estrategia de aceptación de riesgo**, donde el riesgo **reputacional y económico** se traslada parcialmente al cliente.

Aceptar el riesgo **no es hacer nada**. Es simplemente **calcular que el impacto será tolerable**, y por tanto, no vale la pena invertir en controles. Es decir: si **no duele**, se acepta.

Por ejemplo, tus documentos personales. Si tú mismo no les das ninguna protección (ni digital ni física), entonces estás dejando el riesgo **sin tratamiento**. Pero si aplicas algún **control o salvaguarda**, como vigilancia, contraseñas, cifrado o respaldo, entonces ya estás mitigando el riesgo.

En el caso de documentos digitales o contraseñas, una forma de mitigación es:

- **Cifrado**
- **Certificados digitales**
- **Respaldos**
- **Contraseñas seguras**
- **Sesiones cerradas o sin guardar información sensible**

Si pierdes tu laptop, pero todo está cifrado y respaldado, entonces solo pierdes el equipo material. Pero si no tomaste ninguna medida, pierdes también **toda tu información**: accesos, contraseñas, sesiones abiertas... y eso puede ser un desastre.

Por eso, mitigar el riesgo implica:

- Aplicar cifrado
- Establecer toques de seguridad (como doble autenticación)
- Hacer respaldos periódicos

¿Qué nivel de apetito de riesgo tiene este sistema?

El **apetito de riesgo** se refiere al nivel de riesgo que una organización está dispuesta a aceptar. En este caso:

- El sistema **no implementa un segundo factor de autenticación**, lo cual indica que hay cierto grado de riesgo aceptado.
- Sin embargo, **sí implementa otras medidas** como CAPTCHA y sesión limitada, lo que demuestra una intención de mitigar.

Por tanto, **el apetito de riesgo del sistema no es muy bajo, pero tampoco es alto**. Está en un nivel **medio o medio-alto**, dependiendo de cómo evolucione y se fortalezcan sus controles.

Nivel estimado de apetito de riesgo:
MEDIO hacia MEDIO-ALTO
No es indiferente al riesgo, pero tampoco aplica los controles más estrictos posibles.

Cuadro comparativo: Tratamientos del Riesgo

Tratamiento	Definición	Ejemplo	Cuándo se aplica
Evitar	Eliminar el riesgo eliminando el activo o la causa.	No usar una laptop para evitar que te la roben.	Riesgos inaceptables que no se pueden controlar de otra forma.
Transferir	Pasar la responsabilidad a un tercero.	Contratar un seguro para el centro de datos.	Cuando el riesgo es muy alto y no se cuenta con los medios propios para enfrentarlo.
Mitigar	Reducir la probabilidad o el impacto del riesgo.	Usar CAPTCHA, cifrado, contraseñas seguras.	Riesgos que no se pueden evitar ni transferir, pero sí reducir.
Aceptar	Asumir el riesgo sin aplicar controles.	No asegurar una tarjeta con poco saldo.	Cuando el impacto del riesgo es mínimo o tolerable.

Eso siempre se va a aplicar.
Si en algún sistema no se menciona explícitamente, **igual deben considerarse los cuatro tratamientos del riesgo**: **mitigación, transferencia, aceptación y evitación**.
Evitar implica no tener ni el activo ni la amenaza.

¿Qué significa transferir el riesgo en un sistema?

Pregunta del estudiante:
— Ingeniero, disculpe. La parte de "transferir" se explicó con el ejemplo de la póliza de seguro. Pero, ¿cómo se transfiere el riesgo en un sistema informático?

Respuesta:
Cuando hablamos de **tratar un riesgo**, estamos hablando de asignar recursos: logística, presupuesto, controles, personal capacitado, etc. Por ejemplo, si yo quiero mantener mi propio **data center**, necesito:

- Energía eléctrica continua y estable
- Climatización para evitar sobrecalentamiento
- Conectividad a internet
- Sistemas de contingencia
- Personal calificado para administrar servidores
- Equipos de respaldo y mantenimiento
- Previsión de fallos (discos que se queman, piezas que se deprecian, etc.)

Todo eso es **responsabilidad mía** si decido mantener mi infraestructura local.

Pero si **no quiero asumir esa carga**, lo que hago es **trasladar ese riesgo a un tercero**, como por ejemplo:

- **Contratar servicios en la nube (cloud computing)**
- Pagar por un proveedor de hosting
- Usar plataformas como servicio (PaaS), software como servicio (SaaS), o infraestructura como servicio (IaaS)

Ahí el proveedor se encarga de la infraestructura, el data center, la red, el hardware, la climatización, la electricidad... **yo solo uso el servicio**. Así, **le transfiero los riesgos físicos y operativos** a ese proveedor.

¿Es como contratar una empresa para que se encargue de la seguridad?

Exactamente.
Es como **tercerizar la seguridad**. En vez de que tú controles todo, contratas una empresa que lo haga. Ellos se hacen cargo de la protección, de las configuraciones, de los respaldos, de los incidentes.

¿Y cómo funciona eso con seguros?

Lo mismo pasa con las **pólizas de seguro**.
Cuando tú contratas un seguro, por ejemplo para un vehículo, estás diciendo:

“Si ocurre un accidente, **yo no me preocupo por cómo pagar los daños**. Eso lo cubrirá la aseguradora”.

Eso es **transferencia del riesgo**.
La amenaza (el accidente) sigue existiendo.
Pero el **tratamiento del riesgo** ya no lo asumes tú directamente, sino que lo gestiona otra entidad (el seguro).

Esto aplica también para **seguros de salud**, **seguros de vida**, **seguros para equipos tecnológicos**, etc.
En todos los casos, si ocurre una pérdida o daño, la póliza te da una **compensación o reposición** del bien o servicio afectado.

¿Existen pólizas de seguro para sistemas informáticos?

Sí.
Algunos sectores críticos como el **bancario** o **financiero** contratan **seguros para ciberincidentes**.
Incluso hay pólizas que **garantizan la devolución del dinero** a los clientes si se produce un robo o fraude electrónico.

Por ejemplo, algunos bancos promocionan:

“Tu dinero está asegurado. Si ocurre un robo digital, nosotros lo repondremos”.

Esto implica que la **empresa ha transferido parte del riesgo** financiero hacia una aseguradora, y a su vez transmite confianza al cliente.

Otro ejemplo podría ser lo que ofrece Google o Microsoft, como servicios de notificación o recuperación de cuentas.
Si un usuario pierde su cuenta, Google, por ejemplo, tiene un sistema que permite recuperarla. Y aunque es gratuito por defecto, al final beneficia tanto al usuario como al sistema, porque genera confianza.

Este tipo de situaciones están relacionadas más que nada con **el tratamiento de seguridad**, distinto de lo que mencionó tu compañero, que hablaba más sobre **pagar por un seguro para que te repongan algo** en caso de pérdida o daño. Eso sí está más vinculado a las **pólizas de seguro**.

Lo que hemos conversado hasta ahora es, en parte, un ordenamiento de lo que ustedes ya saben. Lo primero que se necesita para hacer un **análisis de riesgos** —es decir, estimar o calcular a qué riesgos está expuesta una organización— es saber **qué activos se van a proteger**.

Si no sabes qué activos tienes, todo lo demás **pierde sentido**:
No podrás priorizar adecuadamente, ni decidir qué tipo de tecnología comprar, ni qué capacidades debe tener tu personal, ni cómo distribuir la logística.

Esto se aplica en todos los niveles: **personal, familiar, institucional, empresarial o nacional**.
Si no sabes **cuáles son tus activos**, no vas a poder darles el tratamiento de protección adecuado.

También puede ocurrir que:

- **Sobrevalores** un activo y le asignes más recursos de los necesarios.
- O **subestimes** otro activo importante y lo descuides completamente.

Esto sucede también en las universidades.

Ejemplo: universidad y activos críticos

¿Cuál es el activo más importante de una universidad?
Además de la investigación y la proyección social, **la enseñanza** es su actividad primaria.
Por tanto, los **profesores y los estudiantes** son los activos clave.

Por eso, **los recursos deberían asignarse prioritariamente** a garantizar el buen funcionamiento de esa actividad. Esto implica:

- Salones adecuados
- Laboratorios equipados
- Capacitaciones para los docentes
- Acceso a plataformas y recursos para los estudiantes

¿Y qué pasa en la realidad?
Muchas veces el sector **administrativo** tiene oficinas con computadoras de última generación, pantallas grandes...
Mientras que los docentes o estudiantes trabajan con equipos básicos, antiguos, en malas condiciones.

Entonces, ahí **no se está asignando correctamente el valor de los activos**.

Seguridad y protección de información

Lo mismo ocurre en **seguridad informática**.
Si una institución tiene como activos la **información personal de sus empleados, docentes o estudiantes**, eso debe estar protegido.

Pensemos, por ejemplo, en los **perfiles socioeconómicos** que entrega un estudiante al ingresar a la universidad:
¿Dónde están guardados? ¿Quién tiene acceso a ellos? ¿Quién los procesa? ¿Quién los puede imprimir o ver?

Muchas veces **no se sabe exactamente quiénes tienen acceso**, y eso ya representa un riesgo.

Lo mismo sucede con la información de los docentes:
Todos sus datos personales, cuentas bancarias, contratos, plazos, historial, etc., terminan en Recursos Humanos o en Planillas.
¿Y quién garantiza que esa información está siendo protegida?

Por eso, lo **primero es identificar los activos**, y luego, una vez identificados, responder:

¿Contra qué amenazas los debo proteger?

Identificación de amenazas

Una vez que sabes qué activos tienes y cuáles son más valiosos, el siguiente paso es identificar las **amenazas**.
Por ejemplo:

- **¿Tenemos que protegernos de una erupción volcánica?** No, si no hay volcanes en la zona.
- **¿De tsunamis?** Tampoco, si no estamos cerca del mar.
- Pero sí podría haber amenazas como:
    - Huaicos
    - Inundaciones
    - Tormentas eléctricas
    - Fallas eléctricas o incendios

Cada región tiene **sus propias amenazas locales**.
Así se pueden identificar **los riesgos físicos o naturales** de forma más precisa.

En el contexto informático

En informática, el contexto es **más global**.
Un virus informático o una vulnerabilidad puede afectar tanto en Perú como en cualquier otro país del mundo.

Sin embargo, **algunos factores sí pueden variar**, como el **acceso físico** a los sistemas.

Por ejemplo:

¿Pueden ustedes entrar a cualquier oficina de la universidad?

Eso ya depende de cada institución. Si cualquiera puede entrar sin control, entonces hay una amenaza **física** directa.

Accesos físicos y amenazas reales

Pregunta: ¿Se puede acceder a cualquier oficina dentro de la universidad?

Obviamente no deberías poder, pero en la práctica, muchos sí pueden entrar. ¿Qué pasa si alguien **se hace pasar por un estudiante**? ¿O simplemente **pregunta por otra persona**? ¿Te piden alguna identificación?

En muchos casos, **no se solicita ninguna verificación**. Basta con saber el nombre o el código de la persona, y ya te dan información. No te piden tu carnet, ni ningún otro medio para validar tu identidad.

Entonces, eso demuestra que **las amenazas físicas varían de institución en institución**.

Comparación con otros entornos

En un **banco**, por ejemplo, no entras así nomás.
Te piden identificarte, escanean tu documento, te preguntan a qué piso vas, te asignan una tarjeta temporal, etc. Si no cumples con eso, **no entras**.

En cambio, en algunas universidades, **el acceso es mucho más laxo**. Incluso hay instituciones que usan tarjetas para validar que eres estudiante, pero muchas otras **no lo aplican**.

Entonces, si cualquiera puede entrar a una universidad, **¿qué tan protegida está realmente esa institución?**
Pensemos: alguien malintencionado podría dejar un objeto peligroso, como un coche bomba, o incluso sustraer información o dispositivos.

Las amenazas varían según el contexto

Por eso decimos que **las amenazas no son siempre las mismas**.
Cada institución enfrenta **diferentes tipos de riesgo**, y el **grado de probabilidad de ocurrencia también cambia**.

Entonces, ¿cómo se debe hacer el análisis?

Pasos para un análisis de riesgo

1. **Identificar activos:**
   ¿Qué tengo que proteger? Información, equipos, personas, aplicaciones, etc.
2. **Identificar amenazas:**
   ¿Qué eventos o situaciones pueden poner en peligro mis activos?
   Ejemplos: robos, accesos físicos no autorizados, desastres naturales, ciberataques, etc.
3. **Identificar vulnerabilidades:**
   ¿Qué debilidades tienen mis activos?
   - ¿Qué fallas tiene mi sistema, plataforma o servidor?
   - ¿Qué carencias tienen mis procesos, personas o infraestructura?

Las vulnerabilidades pueden ser:

- **Tecnológicas**
- **Físicas**
- **Humanas**
- **De negocio**

Aplicación de controles

Luego de identificar activos, amenazas y vulnerabilidades, toca responder:

¿Qué controles aplico para reducir el riesgo?

No todos los controles son válidos para todos los casos.
Depende del contexto, del tipo de activo y del tipo de amenaza.

Existen diferentes **estándares de seguridad** para aplicar controles, entre ellos:

- **ISO 27001**
- **NIST**
- **CIS Controls**
- **PCI DSS**

Por ejemplo, **CIS** propone inicialmente 18 controles, pero cada uno incluye subcontroles. Al final, puedes tener más de 80 controles sugeridos. Algunos hablan de "Top 10", pero incluso esos pueden dividirse en muchos más elementos según el contexto.

Por lo tanto, **es fundamental identificar qué control se aplicará a cada activo**.
El proceso de gestión de riesgos **no es tan sencillo ni rápido** como parece. Se trata de un **trabajo amplio, constante y permanente**.

¿Qué ocurre si cambia el entorno?

- ¿Qué pasa si adquiero un nuevo activo?
- ¿O si un activo deja de usarse o se da de baja?

Por ejemplo, si actualizo mi infraestructura, cambio hardware, instalo un nuevo *firewall* o una nueva aplicación, **debo repetir el análisis**:

- Identificar nuevas amenazas
- Detectar vulnerabilidades
- Evaluar el riesgo

Este proceso **debe repetirse cada vez que cambian los activos**, porque cada cambio puede implicar **nuevos riesgos o exposiciones**.

Caso real: pandemia

Durante la pandemia, se lanzaron muchas aplicaciones **de manera urgente y sin evaluación de seguridad**.

La prioridad era salir rápido al mercado, pero **muchas de estas aplicaciones tenían múltiples vulnerabilidades**.
No se realizó un análisis por activo, ni pruebas de seguridad adecuadas.

Análisis del riesgo

Para cada nuevo activo, se deben seguir estos pasos:

1. **Identificación del activo**
2. **Identificación de amenazas**
3. **Identificación de vulnerabilidades**
4. **Estimación del riesgo**

¿Cómo funciona el riesgo?
Se considera la **probabilidad de que la amenaza ocurra** y el **impacto que tendría** si se concreta.

Esto nos da un **riesgo cualitativo**, por ejemplo: bajo, medio, alto.
Puede expresarse en escalas simples, como del 1 al 5.

También existen métodos **cuantitativos**, pero requieren datos históricos, estadísticos, y más sofisticación.
En la mayoría de casos, se trabaja con estimaciones cualitativas, **basadas en el juicio experto** o en la experiencia de los **dueños de los activos**.

No se trata de adivinar cuánto le importa algo a una persona, sino de conversar con los responsables de cada área y evaluar el valor de sus activos.

Luego de evaluar el riesgo, ¿qué sigue?

Toca decidir **la respuesta al riesgo**. Entre las opciones están:

- **Mitigar**: aplicar controles o tecnologías que reduzcan el riesgo
- **Transferir**: por ejemplo, contratando seguros
- **Eliminar**: dejar de usar el activo
- **Aceptar**: si el impacto es bajo, puede decidirse no hacer nada

---

Consideraciones finales

Es importante entender que **no se pueden tratar todos los riesgos**.
¿Por qué? Porque los **recursos (tiempo, dinero, personal) son limitados**.
Por eso, es fundamental **priorizar**.

¿Cómo se prioriza un riesgo?

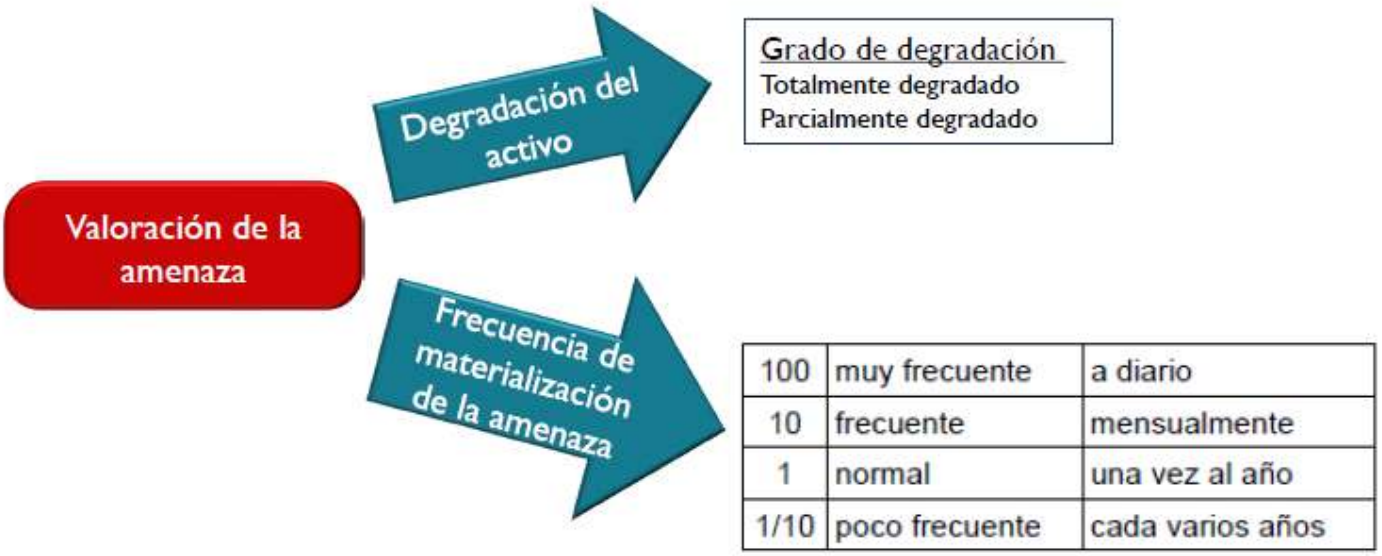
A través de dos criterios principales:

1. **Probabilidad** de que la amenaza ocurra
2. **Impacto** que tendría si se concreta

Ambos se cruzan en una matriz de riesgo.
Ejemplo:

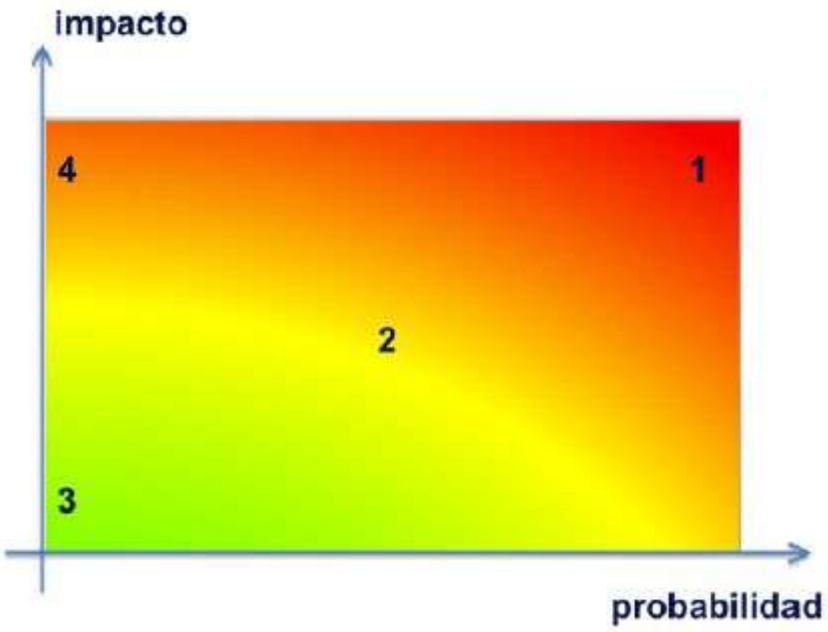
- Si la amenaza es **muy probable** y el **impacto es alto**, el riesgo será **alto**.
- Eso ubica el riesgo en la **zona roja**, donde **sí o sí** debe ser tratado con urgencia.

Valoración de amenazas



100	muy frecuente	a diario
10	frecuente	mensualmente
1	normal	una vez al año
1/10	poco frecuente	cada varios años

Riesgo potencial



zona 1 –riesgos muy probables y de muy alto impacto

zona 2 –franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo

zona 3 –riesgos improbables y de bajo impacto

zona 4 –riesgos improbables, pero de muy alto impacto

Matriz de Riesgos

La Matriz la basé en el método de Análisis de Riesgo con un grafo de riesgo, usando la formula**Riesgo = Probabilidad de Amenaza x Magnitud de Daño**

La Probabilidad deAmenazay Magnitud de Daño pueden tomar los valores y condiciones respectivamente1 =**Insignificante**(incluido Ninguna)

2 =**Baja**

3 =**Mediana**

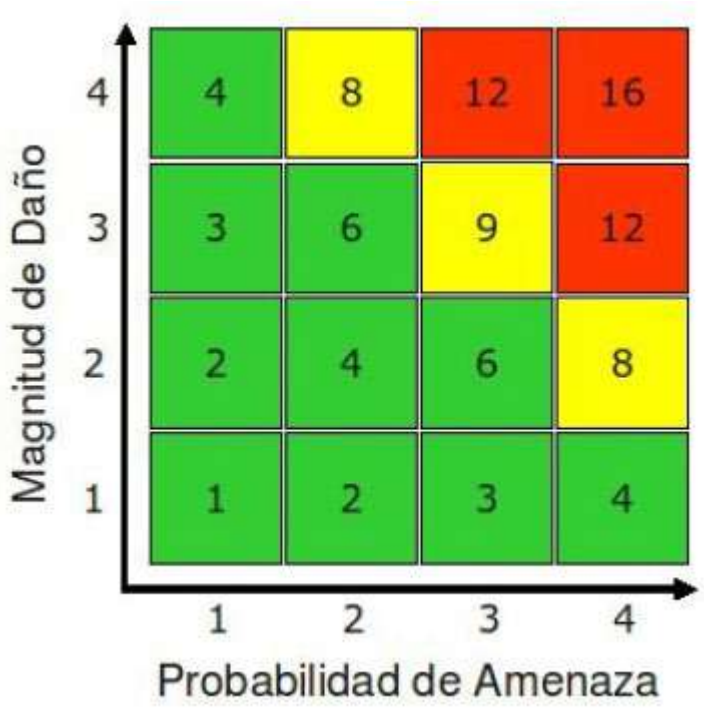
4 =**Alta**

El Riesgo, que es el producto de la multiplicación Probabilidad de Amenaza por Magnitud de Daño, está agrupado en tres rangos, y para su mejor visualización, se aplica diferentes colores.

Bajo Riesgo= 1 –6 (verde)

Medio Riesgo= 8 –9 (amarillo)

Alto Riesgo= 12 –16 (rojo)



Matriz de Análisis de Riesgo		Probabilidad de Amenaza					
Elementos de Información	Magnitud de Daño	Criminalidad		Sucesos físicos		Negligencia	
		Robo	Virus	Incendio	Falta de Corriente	Compartir contraseñas	No cifrar datos críticos
		3	4	2	3	4	3
Datos e Información							
RR.HH	3	9	12	6	9	12	9
Finanzas	4	12	16	8	12	16	12
Sistema e Información							
Computadoras	2	6	8	4	6	8	6
Portátiles	3	9	12	6	9	12	9
Personal							
Coordinador	4	12	16	8	12	16	12
Personal técnico	3	9	12	6	9	12	9

La matriz se puede adaptar a una realidad específica

Se debe tener mucho cuidado al editar la matriz para no alterar y generar errores de cálculo y presentación

Zona de riesgos bajos

Por el contrario, si tenemos una **baja probabilidad** de ocurrencia y **poco impacto**, estamos ante riesgos que, aunque puedan explotar o materializarse, **no representan una amenaza crítica**.

Por ejemplo, una **interceptación de internet** en un contexto donde no se maneja información sensible. Eso entra en la **zona de riesgos improbables y de bajo impacto**.

Y si algo **muy poco probable ocurre**, pero **no genera daños significativos**, la sensación que se tiene es de **seguridad**.

En ese caso, estos riesgos **no justifican el uso de recursos** para mitigarlos o transferirlos.
Por eso, el **tratamiento usual es la aceptación del riesgo**.

¿Qué tratamiento corresponde?

Entonces, ¿qué tratamiento corresponde a estos riesgos improbables y de bajo impacto?

✔ **Aceptación del riesgo**.

Aunque si el riesgo **pudiera eliminarse directamente**, entonces podríamos aplicar **eliminación del riesgo**, pero muchas veces eso implica decisiones mayores, incluso a nivel **legal o normativo**.

Zona de riesgos medios y altos

Ahora bien, tenemos casos como el siguiente:

“Un terremoto en esta zona… ¿Qué tan probable es?”

Probablemente, **muy bajo**. Pero si llegara a ocurrir, **el impacto sería catastrófico**.

Entonces, aunque el riesgo es **improbable**, su impacto **es muy alto**.
Esto nos ubica en una **zona crítica de análisis**, en la que el tratamiento más adecuado suele ser:

✔ **Transferencia del riesgo**, por ejemplo, contratando **seguros o pólizas**.

En algunos casos, también se puede aceptar el riesgo, pero **solo si se justifica por la falta de recursos o la baja viabilidad de mitigación directa**.

¿Cómo se calcula el riesgo?

El cálculo se realiza mediante la **multiplicación de dos factores**:

Riesgo = Probabilidad de la amenaza × Magnitud del impacto

Este resultado se clasifica cualitativamente para tomar decisiones.
Se suelen usar **tablas o matrices** que definen rangos como:

Resultado	Clasificación de riesgo	Zona de acción
1 a 5	Bajo	Verde (aceptar)
6 a 11	Medio	Amarillo (mitigar)
12 a 16	Alto	Rojo (mitigar o transferir)

Ejemplo:

- Si la **probabilidad es 4** (alta) y el **impacto es 4** (muy alto), entonces:

4 × 4 = **16** → Riesgo **alto** (zona roja)

- Si la **probabilidad es 2** y el **impacto es 3**, entonces:

2 × 3 = **6** → Riesgo **medio** (zona amarilla)

¿Es cuantitativo o cualitativo?

Aunque estamos usando **números**, el análisis sigue siendo **cualitativo**, porque:

- No se basa en datos históricos, monetarios o estadísticos reales.
- Se utiliza más bien como una **estimación rápida y operativa**, basada en el **juicio experto**.

El análisis **cuantitativo puro** es más preciso, pero también mucho más complejo, ya que **requiere datos estadísticos o históricos confiables**.

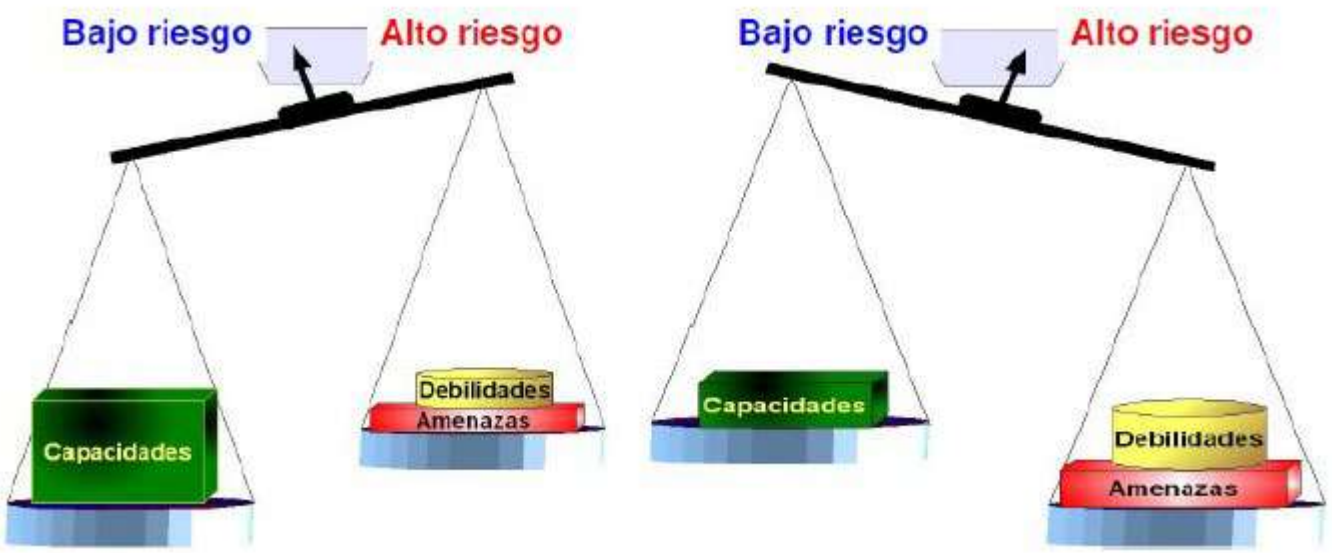
¿Qué se usa en la práctica?

En la mayoría de los casos, **se opta por lo cualitativo**, porque:

- Es más ágil
- Permite tomar decisiones inmediatas
- Es más adaptable a situaciones cambiantes
- Se puede aplicar constantemente

Además, **el análisis de riesgos es un proceso permanente**, no se hace una sola vez.
Debe actualizarse **cada vez que cambian los activos, las amenazas o las vulnerabilidades**.

Clasificación del riesgo



Entonces, con toda esta explicación, podemos entender **cómo se clasifican los riesgos** en una matriz:

- Zona **roja**: Riesgo **alto**
- Zona **amarilla**: Riesgo **medio**
- Zona **verde**: Riesgo **bajo**

¿Qué pasa en cada zona?

- Si **no tenemos recursos**, el riesgo quedará en la zona **roja**.
- Si **tenemos recursos limitados**, se evaluará si podemos **mitigar o transferir** el riesgo (zona **amarilla**).
- Si **tenemos suficientes recursos**, y el riesgo es tolerable, se puede **aceptar** (zona **verde**).

Estas zonas representan **opciones de tratamiento**:

- **Zona roja** → Mitigación urgente o transferencia
- **Zona amarilla** → Mitigación o aceptación parcial
- **Zona verde** → Aceptación del riesgo

Aplicación práctica

Esto puede aplicarse **en trabajos, informes o análisis de riesgo reales**.

Cada uno de ustedes podrá ir armando su propio esquema o tabla de riesgos. Tendrán una serie de resultados que clasificarán los riesgos según su probabilidad e impacto.

Análisis de capacidad

Si una organización tiene **buenas capacidades técnicas, personal capacitado y recursos suficientes**, sus **debilidades y amenazas serán menores**.

En ese caso, la **flechita del análisis** apunta hacia un entorno más **seguro y preparado**.

¿Y si no hay preparación?

Por el contrario, si la organización **no está preparada**, no tiene personal capacitado, ni tecnología, ni presupuesto, entonces las **amenazas se vuelven más latentes** y las vulnerabilidades aumentan.

Relación clave

Existe una **relación directa entre:**

- **Amenazas** (externas)
- **Vulnerabilidades** (internas)
- **Capacidades de respuesta** (preparación de la organización o persona)

Entre más preparación se tenga, **menos impacto tendrán las amenazas**.

¿Qué sigue ahora?

Hasta aquí todo ha sido **conceptual**, pero ahora pasaremos a un **ejercicio práctico**.

Vamos a construir una **tabla de riesgos** donde se aplicará todo lo que hemos conversado.
Pueden usar diferentes herramientas, como:

- **Tablas simples**
- **Plantillas en Excel**
- **Herramientas online** (Miro, Jamboard, Lucidchart, etc.)

Recomendaciones para el ejercicio

- **Editar los activos** según su caso real
- **Asignar las amenazas correspondientes**
- **Identificar vulnerabilidades**

No es necesario poner todos los activos o amenazas existentes. Solo **los que correspondan a su situación específica**.

Referencias útiles

Hay una metodología llamada **MARKETEST**, que cuenta con tres libros. En el segundo, si no me equivoco, se encuentra un **catálogo de activos** muy útil.

También en la norma **ISO/IEC 27005** está incluido un **catálogo de activos de información**.

La ISO 27005 se enfoca precisamente en la gestión de riesgos de seguridad de la información.

¿Qué contiene este catálogo?

Contiene una lista organizada de **activos esenciales**, clasificados y definidos, que sirven como punto de partida para identificar **qué debe protegerse**.

Este catálogo puede usarse como referencia para crear sus propias listas de activos, ya sea personales, empresariales o institucionales.

¿Tiene clases prácticas?

Sí, esto se va a aplicar de forma práctica. Por ejemplo, **puedes marcar si un sistema o entidad tiene o no tiene servicios**, pero no basta con eso:
Hay que **determinar qué tipo de servicios son**.
Por ejemplo:

- Correo electrónico
- Servidores de archivos
- Página web

- Aplicaciones informáticas, etc.

Se debe **detallar qué software o aplicaciones** maneja una empresa.
Y no se preocupen, no tienen que "imaginarse" todo desde cero: **ya existen guías y referencias** que pueden usar para identificar los activos que existen en una organización.

Fuentes y herramientas

Algunas de estas referencias son:

- La **norma ISO**, que incluye catálogos de activos y controles.
- **Pilar**, un software de análisis de riesgos (de pago, pero tiene versión de prueba).
- **MARISMA**, una aplicación web gratuita por 6 meses para estudiantes, que incluye plantillas y metodología para gestionar riesgos.
- También hay **plantillas Excel** que pueden usar, como las que se mostraron en clases anteriores.

Trabajo práctico

Lo que ustedes van a hacer ahora es **aplicar una matriz de análisis de riesgos a un caso individual**.
Ese caso puede ser:

- **Ustedes mismos**, como personas (estudiantes)
- **Su hogar**
- **Su empresa o negocio propio**
- O **una organización local o conocida** a la que tengan acceso

NO se trata de ir a inventar cosas. No sirve que se vayan a investigar a empresas a las que no tienen acceso real.
Si no hay información, el análisis no tiene sentido, porque se vuelve una suposición.

¿Qué activos usar?

Elijan **activos reales**.
Por ejemplo, si lo hacen desde su perspectiva personal, pueden usar como activos:

- Laptop
- Celular
- Moto

- Cuenta bancaria
- Casa

Y si lo hacen desde una empresa real, pongan solo **los activos que de verdad existen y conocen**.
No inventen 80 activos si solo tienen 10.

Es preferible un trabajo **sincero y realista** que una fantasía o exageración.

¿Qué deben incluir?

En su trabajo deben identificar:

1. **Activos**: lo que tienen o valoran.
2. **Amenazas**: lo que podría dañar esos activos.
3. **Vulnerabilidades**: debilidades en esos activos.

Importante:
No se trata de que un activo sea vulnerable "de verdad", sino que **existe la posibilidad** de que lo sea.
Por ejemplo: “Mi celular tiene un software desactualizado” o “creo que puede tener malware”.

¿Ejemplo de enfoque?

Sí, pueden enfocarse como estudiantes y analizar:

- Sus datos personales
- Su conexión a internet
- Sus dispositivos
- Su correo institucional
- Sus cuentas académicas

O pueden usar su casa como entorno, y analizar:

- Equipos electrónicos
- Seguridad física
- Información sensible
- Acceso de terceros

Pueden utilizar cualquiera de las herramientas disponibles. Puede ser en Excel, Word o incluso alguna aplicación específica como MARISMA. Lo que tienen que hacer es **identificar sus activos**.

En las hojas de cálculo que se les han mostrado, los activos pueden clasificarse por tipo:

- Software
- Hardware
- Organizativos
- Personas

Pero en sus casos personales, probablemente **no tengan todos esos tipos de activos**.
Por eso, lo más común será que trabajen con **hardware, software y tal vez datos personales**.

El **proceso puede variar**, pero lo importante es que expliquen **claramente** cuáles son sus activos.

Luego, deben explicar **las amenazas**.
En las plantillas van a encontrar amenazas de todo tipo.
Por ejemplo: amenazas de tipo **ambiental** como terremotos o tsunamis.
Pero si eso **no aplica a su caso**, simplemente lo eliminan y no lo consideran.

Solo se deben incluir las amenazas **reales y relevantes** para su situación.

Estándares y Frameworks para Riesgos

Estándares y marcos de referencia

Entre los más importantes está **COBIT**, un marco de gobierno y gestión de tecnologías de información en las empresas.
Este marco nació principalmente como **herramienta de auditoría**, pero ahora también incluye temas como **análisis de riesgos**.

A partir de **COBIT 5**, todo está integrado (antes, por ejemplo, los temas de riesgo estaban en módulos separados como Risk IT). Ahora está todo unificado.

En COBIT 5 se define claramente qué es una amenaza, qué es una vulnerabilidad, y cómo se debe tratar o responder al riesgo.

Además, se establece que **la forma de tratar los riesgos depende de la empresa**:

- Si decide mitigarlos, transferirlos, eliminarlos o aceptarlos
- Cuál es el valor estratégico del activo
- Quiénes son los responsables de decidir cómo tratarlo

Importante:
No es el área de TI la que define el valor de un activo, sino los **dueños de los procesos**.
Cada área o unidad define qué tan crítico es su propio activo.

Otros modelos

Además de COBIT, también existe el **modelo MIKE2.0**, un marco de seguridad de la información que considera cuatro elementos principales:

1. Personas
2. Procesos
3. Tecnología
4. Información

Este modelo analiza las **interacciones entre esos elementos**, y cómo de esas combinaciones surgen situaciones o riesgos nuevos.

Por ejemplo, cuando se combinan personas y tecnología, se deben considerar los **factores humanos**:

- ¿Las personas aceptan usar la tecnología?
- ¿Saben cómo usarla?
- ¿La rechazan por falta de capacitación?

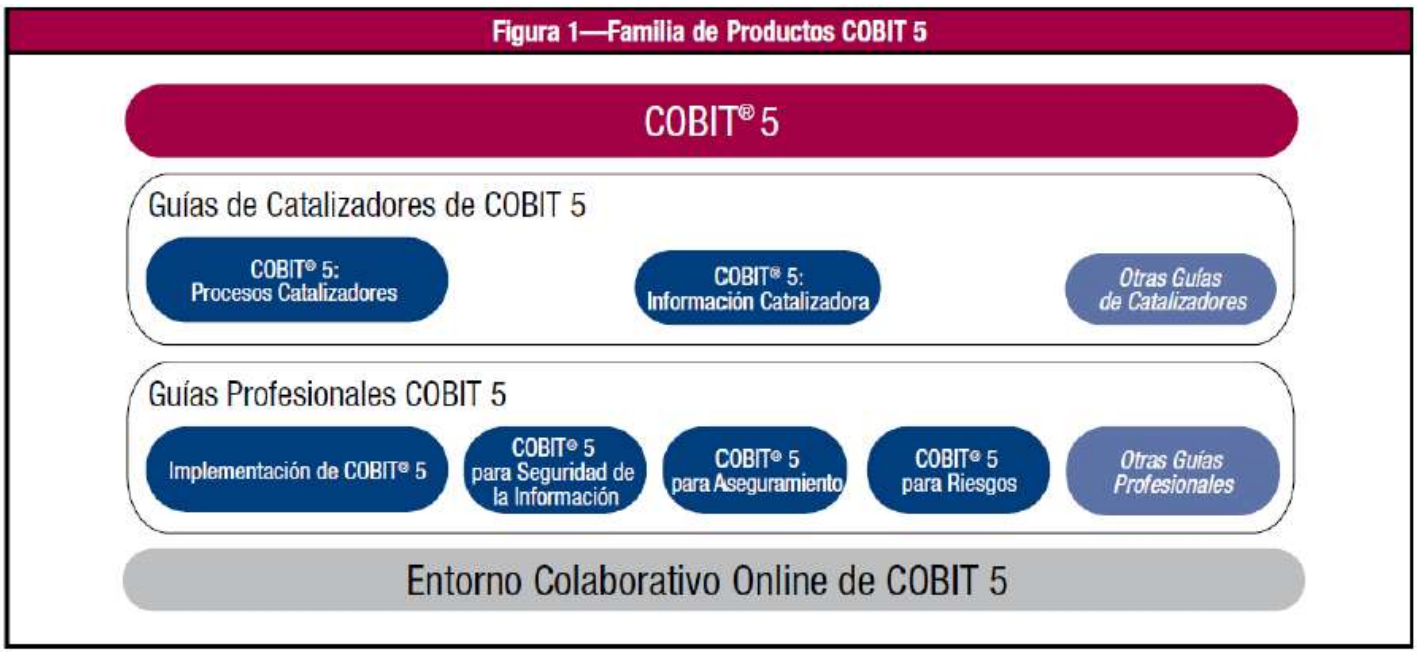
COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas)

El marco COBIT 5 se construye sobre cinco principios básicos, que quedan cubiertos en detalle e incluyen una guía exhaustiva sobre los catalizadores para el gobierno y la gestión de las TI de la empresa.

COBIT 5 es marco de referencia para el **Gobierno**y la **Administración**de la información y los Activos Tecnológicos de las Organizaciones.

Es una evolución de los principios de auditoria hacia el gobierno.

Integra diferentes guías y marcos de referencia de ISACA. La última versión es la quinta.



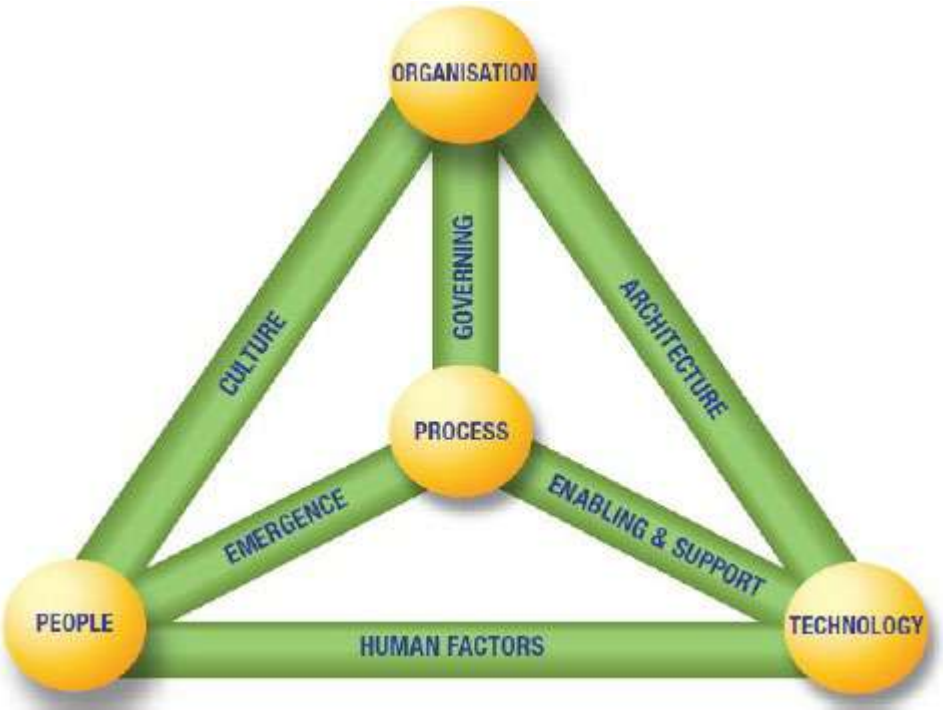
COBIT 5: Gobierno y Gestión

El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la

dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.

La Gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

BMIS (Business Model for Information Security)



¿Qué es BMIS?

El **Business Model for Information Security (BMIS)** es un marco conceptual que ayuda a las organizaciones a comprender que la **seguridad de la información** no depende solo de la tecnología, sino de un equilibrio integral entre:

- Personas,
- Procesos,
- Tecnología,
- y Organización.

📌 **Explicación de la Imagen BMIS**

La imagen muestra un **triángulo de interacción dinámica** que incluye:

🔶 Nodos o Pilares

1. **People (Personas)**
   Los usuarios, empleados y todas las personas que interactúan con los sistemas. Son un componente esencial porque sus acciones afectan directamente la seguridad.
2. **Organization (Organización)**
   Las políticas, estructuras, roles y cultura de la empresa que orientan el comportamiento y la toma de decisiones sobre seguridad.
3. **Technology (Tecnología)**
   Las herramientas, hardware, software y sistemas que permiten proteger, procesar y almacenar la información.
4. **Process (Proceso)**
   Es el **núcleo central** que une a los tres pilares. Los procesos son las actividades, flujos de trabajo y controles que aseguran el cumplimiento de las políticas de seguridad.

🔶 Conexiones o Factores Dinámicos

Estas son las interacciones que influyen en la seguridad de la información:

Conexión	Significado
Culture (Cultura)	Normas, valores y creencias que influyen en el comportamiento seguro.
Human Factors (Factores Humanos)	Comportamientos, errores y habilidades humanas que afectan la seguridad.
Architecture (Arquitectura)	Infraestructura tecnológica y organizacional que soporta la seguridad.
Emergence (Emergencia)	Resultados inesperados o no planificados producto de la interacción de los elementos.
Enabling & Support (Habilitación y Soporte)	Recursos y herramientas que facilitan la implementación de seguridad.
Governing (Gobernanza)	La forma en que se establecen políticas, normas y controles para la seguridad de la información.

ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection - Information security management systems - Requirements. **Certificable.**

ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection - Information security controls .

ISO/IEC 27003:2017. Information technology-Security techniques-Information securitymanagementsystems-Guidance. (Guía de diseño)

ISO/IEC 27004:2016. Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation.

ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection - **Guidance on managing information security risks**.

Normas ISO

La familia **ISO 27000** también es fundamental.
La más conocida es la **ISO/IEC 27001**, que es la única **norma certificable** en gestión de seguridad de la información.
Una organización puede certificarse, y también un profesional (como auditor o implementador).

Otras normas complementarias:

- **ISO 9001** (gestión de calidad)
- **ISO 14001** (medio ambiente)
- **ISO/IEC 27005** (gestión de riesgos de seguridad de la información)

La **27005** incluye un **catálogo de activos**, muy útil para identificar qué se debe proteger y cómo evaluarlo.

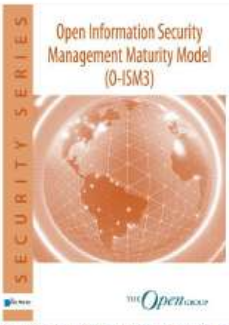
Otros estándares y *frameworks*

Project Management Body of Knowledge (PMBOK®),

https://www.pmi.org/pmbok-guide-standards/framework/practice-standard-project-risk-management

PRINCE2 Risk Management

bsi.
British Standards Institution



https://publications.opengroup.org/standards/security/c102

PRINCE2

PRojects IN Controlled Environments 2 (PRINCE2®),

Information Technology Infrastructure Library (ITIL®),

ITIL®

The Open Group Architecture Framework (TOGAF®),

TOGAF®