SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

Gestión de Riesgo Operativo

DGRV

VELÁSTEGUI
CONSULTORES

Instructor: Iván Velástegui

CONTENIDO

1. **Introducción al riesgo operativo**
2. **Metodologías y recomendaciones internacionales**
3. **Técnicas de identificación y medición del riesgo operativo**
4. **Técnicas control y seguimiento del riesgo operativo**
5. **Tecnología de la información**
6. **Plan de contingencia y continuidad de negocios**
7. **Riego Legal**

EXPERIENCIAS RIESGO OPERATIVO

Allied Irish Banks

Banco comercial

AIB

Baring Brothers

Compañia

Enron

Empresa

ENRON

JP Morgan Chase

Empresa

J.P.Morgan

Bernard Madoff

Daiwa Bank

RIESGO ?

- Entender el Riesgo

Conocer los objetivos
Comprender los objetivos

- Causas - Efectos
- Probabilidad - Impacto
- Vulnerabilidad - Amenaza

Tipos de Riesgos - Gestión del Riesgo

Tratamiento individual para cada riesgo

Riesgo operativo: Es la posibilidad de que se produzcan **pérdidas** para la entidad, debido a fallas o insuficiencias originadas en procesos, personas, tecnología de información y eventos externos

Tanginbles
Intangibles

El riesgo operativo en Instituciones

Probabilidad
Impacto

Mayor exposición al ROP

Causas

- Desregulación
- Globalización de servicios
- Sofisticación tecnología de servicios financieros
- Nuevas Actividades y Canales
- Fusiones
- Terrorismo

El riesgo operativo no es nuevo.

FACTORES DE RIESGO OPERATIVO:

Procesos

Personas

Tecnología

Eventos Externos

Legal

NO

Reputacional
Sistémico

Estratégico

Eventos de Riesgo Operativo

Fraude interno

- No informar intencionadamente de determinadas posiciones,
- infidelidades de empleados,
- Información privilegiada para enriquecimiento propio.

Fraude externo

- Robo,
- Falsificación,
- Daños de fanáticos informáticos (hackers), etc.

Empleo y seguridad

- Compensaciones a trabajadores por quejas, violaciones a normas de seguridad e higiene,
- Demandas por discriminaciones y por responsabilidades generales en el trabajo.

Daños de Activos

- Terrorismo, vandalismo, terremotos, fuegos e inundaciones.

Eventos de Riesgo Operativo

Interrupciones del software

- **Problemas de telecomunicaciones**
- **Apagones negocios y sistemas públicos.**

Ejecución de procesos de gestión

- **Errónea entradas de datos,**
- **Documentación legal incompleta,**
- **Accesos no aprobados a las cuentas de clientes, rupturas de contratos,**
- **Disputas con proveedores y daños colaterales.**

Prácticas con clientes, productos y negocios

- **Pérdida de información confidencial,**
- **Inapropiado manejo de cuentas,**
- **Lavado de activos,**
- **ventas no autorizadas de productos,**
- **Errores en contratos con clientes y proveedores.**

Eventos de Riesgo Operativo

Las **pérdidas causadas por personas** de manera intencional o no, son los riesgos que tratan de cubrir las entidades **a través de su organización interna.**

Estadísticas demuestran que los casos de fraude se han ido incrementando. **El fraude interno es 5 veces mayor que el fraude externo.**

Las transacciones no autorizadas son también un problema severo en las IFIS. En muchos casos estas se asocian a fraudes.

Manejo del Riesgo Operativo

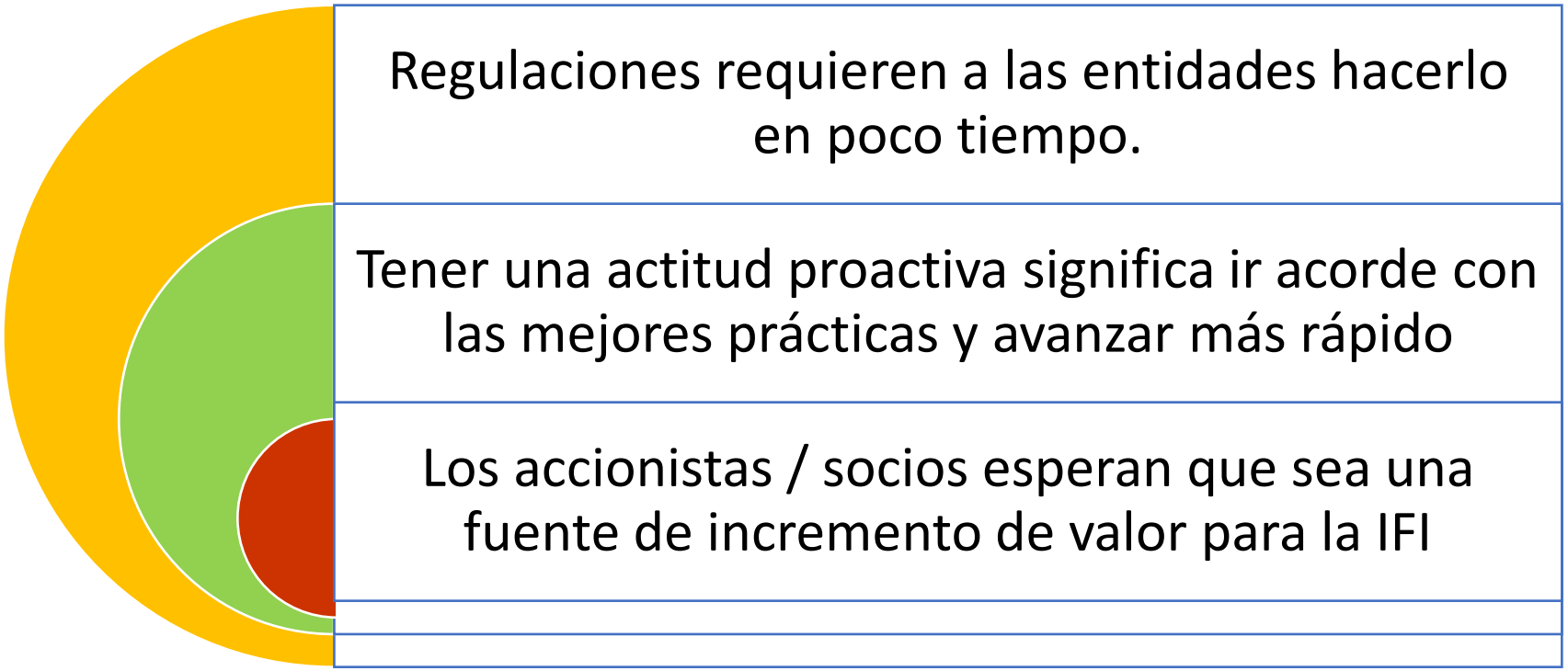
Un adecuado manejo de ROP significa minimizar los riesgos individuales, sin embargo **los diferentes riesgos interactúan entre sí**, por lo que es difícil minimizar todos.

Principios a tener en cuenta para un adecuado manejo del ROP

- Aceptar el ROP cuando los costos de gestión superan a los beneficios
- Decidir no tomar riesgos innecesarios
- Tomar las decisiones a un nivel apropiado (las personas que puedan distribuir el riesgo e implementar los controles)
- Integrar el manejo del ROP en todos los niveles

El riesgo operativo en Instituciones

Razones para que las entidades avanzan en programas de administración de ROP.



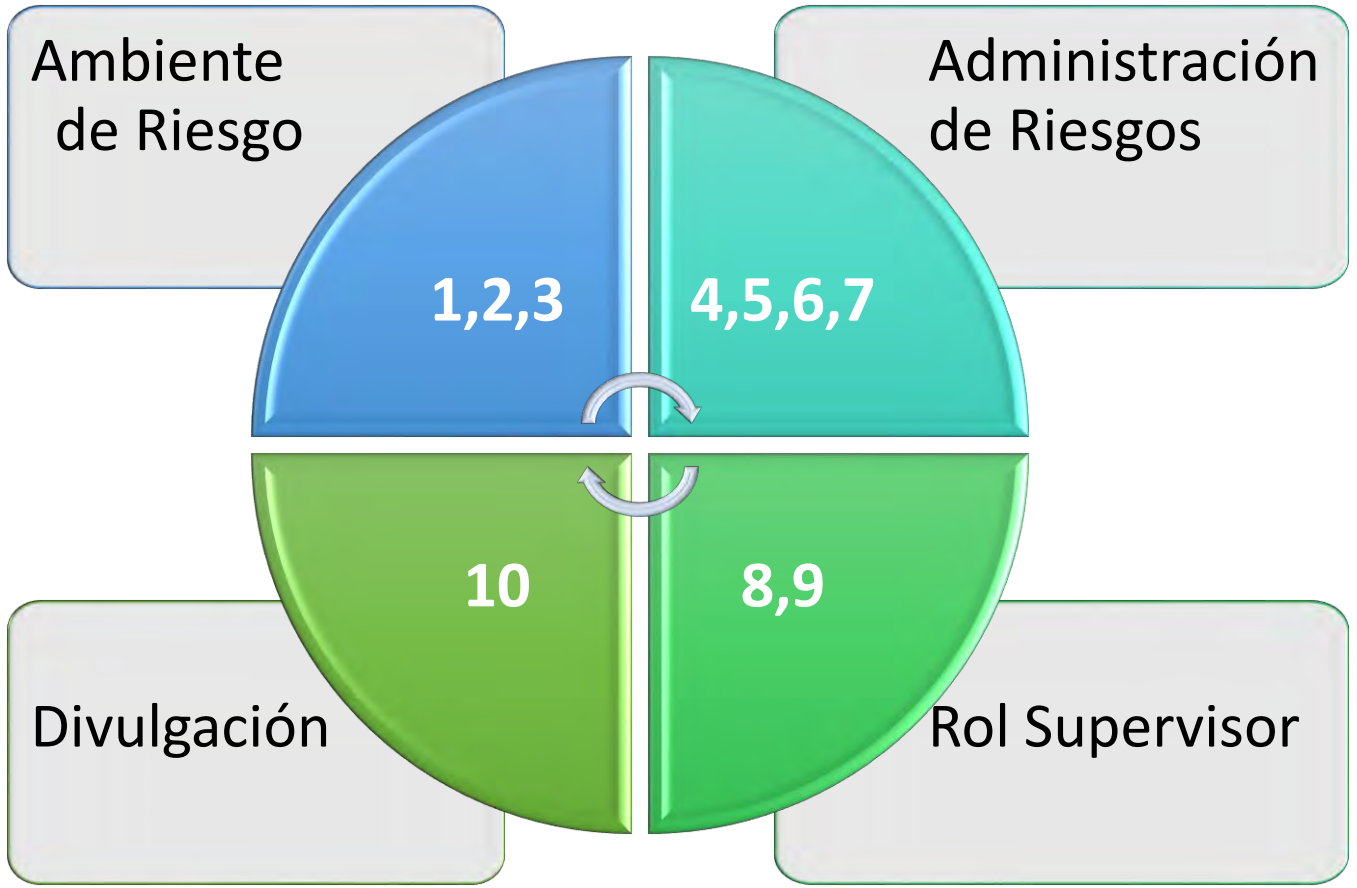
El ROP puede ser el más destructivo y el más difícil de prever.

CONTENIDO

1. Introducción al riesgo operativo
2. **Metodologías y recomendaciones internacionales**
3. Técnicas de identificación y medición del riesgo operativo
4. Técnicas control y seguimiento del riesgo operativo
5. Gestión de la tecnología e información
6. Plan de contingencia y continuidad de negocios
7. Riego Legal

Principios de Riesgo Operativo

Acuerdo de Basilea



P1- Ambiente de desarrollo de riesgos

El Consejo de Administración

Imágenes google

- Conocer los principales aspectos del ROP y tener en cuenta lo que el riesgo operacional debe gestionar.
- Deberá aprobar y evaluar periódicamente el proceso de gestión del riesgo.
- Dar una definición del riesgo operacional válido para toda la entidad y aprobar las metodologías para la identificación, evaluación, seguimiento y gestión del riesgo.

P2- Ambiente de desarrollo de riesgos

El Consejo de Administración

Imágenes google

- Asegurar que el marco para la gestión del riesgo operativo esté **sujeto** a un proceso de **auditoría** interna eficaz e integral por parte de personal independiente, capacitado y competente.

P3- Ambiente de desarrollo de riesgos

La Gerencia será responsable de:

- Poner en práctica el **marco para la gestión** del riesgo operativo aprobado por el CA.
- El marco deberá ser aplicado de forma consistente **en toda la organización.**
- Desarrollo de políticas, procesos y procedimientos destinados a la gestión de estos riesgos **para todos los productos, actividades, procesos y sistemas relevantes** de la Institución.

P3- Ambiente de desarrollo de riesgos

La Gerencia será responsable de:

- Establecer una **estructura** para medir la exposición al ROP e identificar la tolerancia de la institución al ROP.
- Identificar **personal** calificado para manejar el ROP y de los recursos técnicos para su manejo.
- Para monitorear y evaluar el perfil de riesgo, asegurarse de mantener prudentes niveles de **capital**.


Imágenes google

P4- Administración de riesgos

Las Entidades deberán:

- Identificar y evaluar el riesgo operativo inherente **a todos sus productos, actividades, procesos y sistemas relevantes.**
- Antes de implementar nuevas actividades, procesos o sistemas, evaluar el riesgo operativo inherente.
- Vigilar periódicamente los **perfiles de riesgo** operativo y las exposiciones sustanciales a pérdidas.

P5- Administración de riesgos

Las Entidades deberán:

- La Gerencia y el C.A deberán recibir **información pertinente** de forma periódica que complemente la gestión activa del riesgo operativo.
- Dar señales de alertas temprana de potenciales futuras pérdidas de ROP.
- Reportes deben reflejar totalmente problemas en las áreas y las acciones correctivas.

Imágenes google

P6 - Administración de riesgos

Las Entidades deberán:

- Contar con políticas, procesos y procedimientos **para controlar** y cubrir los riesgos operativos más relevantes.

Las prácticas de un adecuado control incluyen:

- Monitoreo continuo y **definición de límites**
- Asegurar un continuo monitoreo de las transacciones
- Administrar el **riesgo asociado** con las actividades de **outsorurcing**.

P7 - Administración de riesgos

Las Entidades deberán

- Contar con **planes de contingencia y de continuidad** de la actividad del negocio, que aseguren su capacidad operativa continua y que reduzcan las pérdidas en caso de interrupción grave de la actividad.

Que significa para las Instituciones

- Identificar los **procesos críticos**
- Identificar **mecanismos alternativos** de servicios para continuar operaciones
- El **plan** de continuidad de negocio debe ser **testeado** regularmente.

P8 - Supervisores

- Exigir a **todas las entidades**, sea cual sea su tamaño que mantengan un marco eficaz para identificar, evaluar, seguir y controlar o **mitigar sus riesgos operativos más relevantes**, como parte de su aproximación general a la gestión de riesgos.

P9 - Supervisores

- Establecer **procedimientos y mecanismos de control**
- **Evaluar los métodos de monitoreo**
- Evaluar la **integridad del procedimiento** de ROP
- Determinar la **efectividad de las medidas de mitigación**
- Evaluar los procesos para determinar las necesidades de capital
- Evaluar la calidad de los **reportes internos** y si estos son revisados

P10 - Divulgación

Las Entidades deben:

- Hacer divulgación pública suficiente para permitir a los participantes del mercado evaluar su enfoque a la administración del riesgo operacional.

ISO 31000/2018 (Organización Internacional de Normalización)

Marco de Referencia

Principios

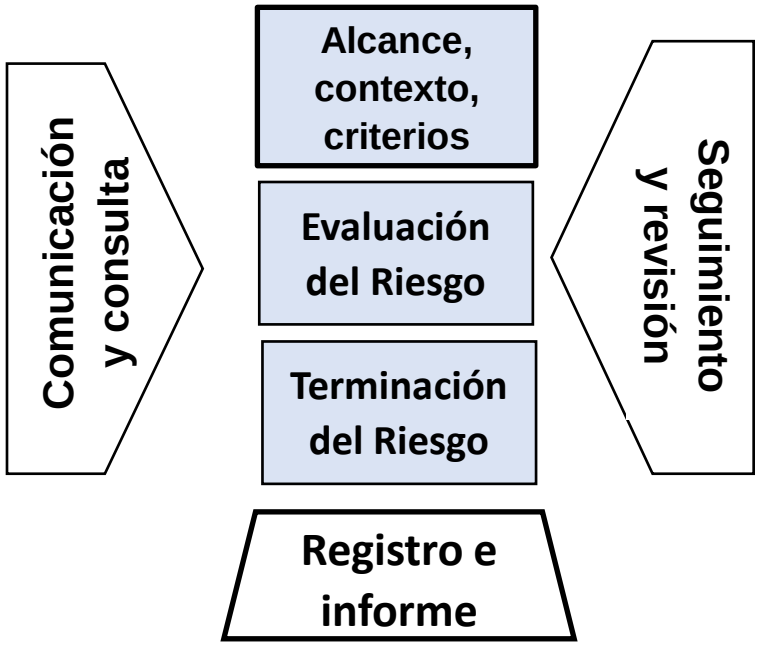
Creación

y

protección

del valor

Proceso



Principios: Creación y protección del valor:

- Los principios son el fundamento de la gestión del riesgo.
- Orienta sobre las características de una gestión del riesgo eficaz y eficiente.

Integrada

Estructurada y exhaustiva

Adaptada

Inclusiva

Dinámica Mejorar información disponible

Factores humanos y culturales

Mejora continua

Creación y Protección del valor:

Integrada

Todas las actividades de la organización.

Estructurada y exhaustiva

Contribuye a resultados coherentes y comparables.

Adaptada

Marco de referencia y proceso de la gestión son adaptables al contexto interno y externo de la organización.

Creación y Protección del valor:

Inclusiva

Participación de las partes interesadas.

Dinámica Mejorar información disponible

Los riesgos son cambiantes, anticipar y responder a los eventos de manera oportuna.

Factores humanos y culturales

La información debe ser oportuna, clara y alcanzable para las partes interesadas.

Creación y Protección del valor:

Factores humanos y culturales

La cultura de la organización y el comportamiento humano influyen en la gestión de riesgo.

Mejora continua

La gestión de riesgo mejora continuamente mediante aprendizaje y experiencia.

Marco de referencia

- Asiste a la organización para integrar la gestión del riesgo en todas sus actividades y funciones significativas.

- Para ser efectiva requiere apoyo de las partes interesadas y especialmente de la alta dirección.

Proceso de la gestión de riesgos

- Debe ser una parte integral de la gestión toma de decisiones.
- Puede aplicarse a nivel estratégico, operacional o de proyecto.
- Es importante considerar la naturaleza dinámica y cambiante del comportamiento humano y de la cultura.

Riesgo = f (Amenaza, Exposición, Vulnerabilidad, Capacidad)

COSO
(Committee of Sponsoring Organizations of the Treadway)

Comisión de organizaciones del sector privado en EEUU, para dar atención a tres temas:

- Gestión del riesgo empresarial (ERM)
- Control interno
- Disuasión del fraude.

Las organizaciones son:

- La Asociación Americana de Contabilidad
- El Instituto Americano de Contadores Públicos Certificados
- Ejecutivos de Finanzas Internacional
- Instituto de Auditores Internos
- Asociación Nacional de Contadores

Objetivos y Componentes del COSO

COSO

COSO II

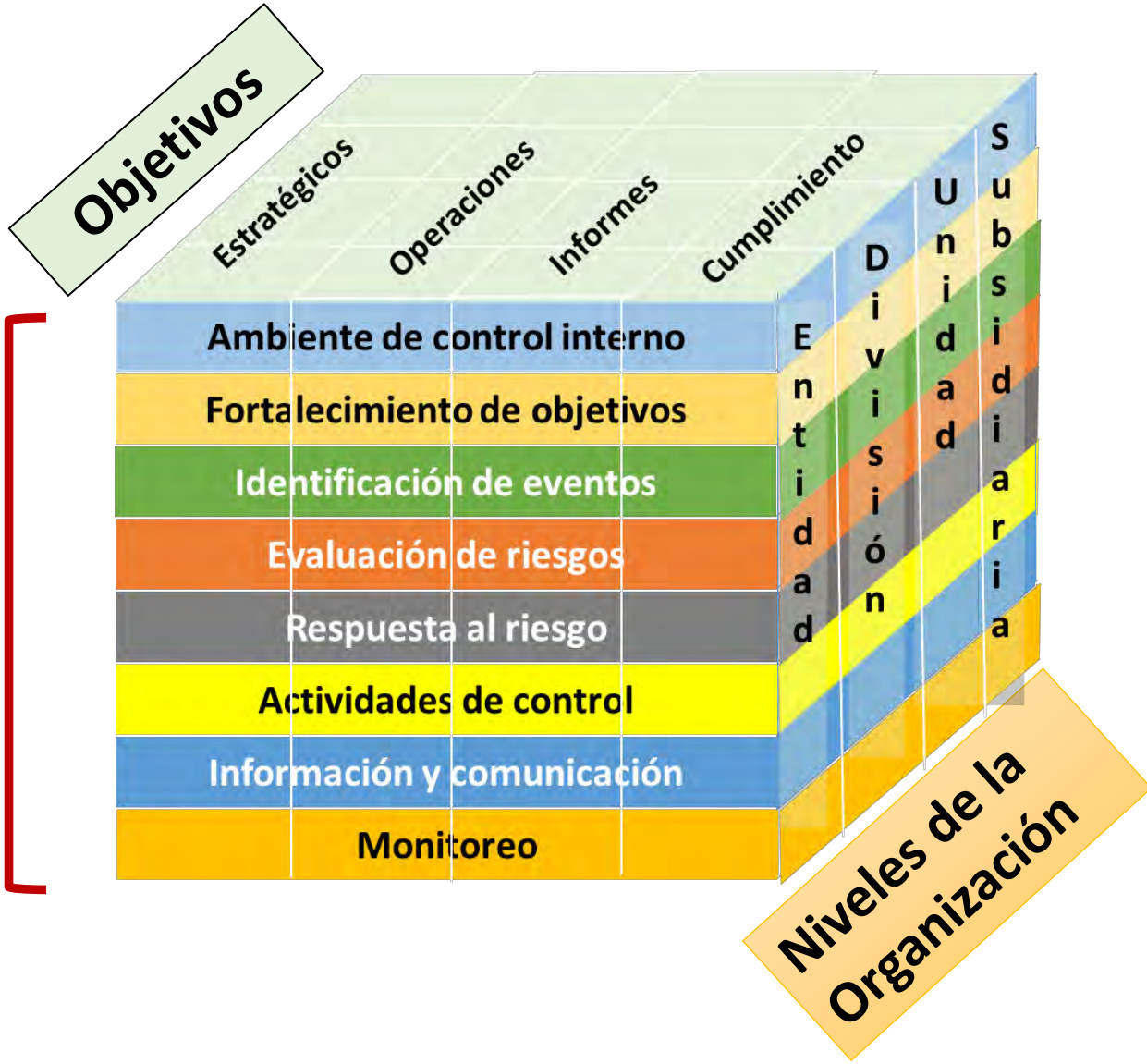
Riesgos

COSO III

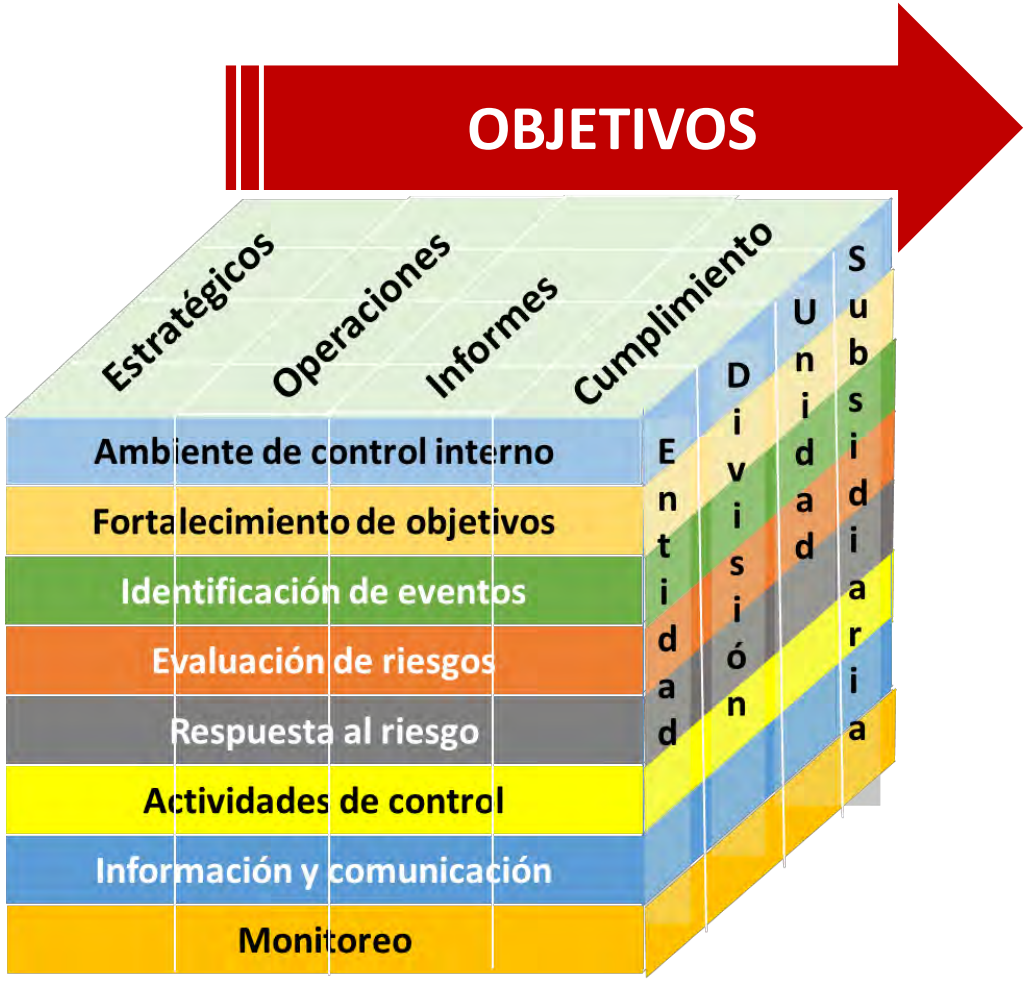
Integridad

Valores Éticos

Componentes



Objetivos del COSO - ERM



Estratégicos

- Misión y Visión de la entidad

Operaciones

- **U**so eficiente de los recursos de la entidad

Información

- Transparencia de información interna y externa

Cumplimiento

- Leyes y regulaciones aplicables.

Norma Australiana

Establecer el contexto	• Organizacional • Externo	• Gestión de riesgos • Plan de trabajo
Identificar el riesgo	• Que puede suceder • Como puede suceder	
Análisis del riesgo	• Existencia de controles • Probabilidad e impacto	• Determinar nivel de riesgo
Evaluar el riesgo	• Comparar criterios • Establecer prioridades	
Tratamiento del riesgo	• Opciones de tratamiento • Evaluar opciones	• Selección de opción • Implementar acciones

CONTENIDO

1. Introducción al riesgo operativo
2. Metodologías y recomendaciones internacionales
3. **Técnicas de identificación y medición del riesgo operativo**
4. Técnicas control y seguimiento del riesgo operativo
5. Gestión tecnología de la información
6. Plan de contingencia y continuidad de negocios
7. Riego Legal

Contexto Organizacional

Aspectos a tener en cuenta

- Establecer metas y objetivos
- Costos, beneficios, oportunidades
- Extensión del proyecto
- Recursos requeridos
- Roles y responsabilidades

Manual de ROP

- Políticas, procesos y procedimientos
- Roles y responsabilidades
- Medidas para asegurar cumplimiento de políticas y objetivos
- Metodologías para identificar, medir, controlar y monitorear
- Procedimientos para priorizar y gestionar los eventos de riesgo
- Estrategias de capacitación en gestión de ROP
- Reporte de la administración de riesgo operativo

Proceso de gestión de riesgo operativo

Identificar los riesgos

- Qué puede suceder ?
- Cómo puede suceder ?
- Efectos

Analizar los riesgos

- Determinar probabilidad
- Determinar impacto

Medir los riesgos

Estimar nivel de riesgo

Controlar los riesgos

- Identificar opciones de control
- Evaluar y seleccionar opciones
- Implementar planes de control

Seguimiento

Continúo

Identificación de Riesgo Operativo

Metodología para Identificar Procesos

MACROPROCESO

- Agrupación de procesos

PROCESO

- Conjunto de actividades que transforman insumos en productos o servicios

SUBPROCESO

- Es la desagregación de un proceso

ACTIVIDAD

- Conjunto de Tareas

TAREA

- Procedimientos que conducen a un resultado

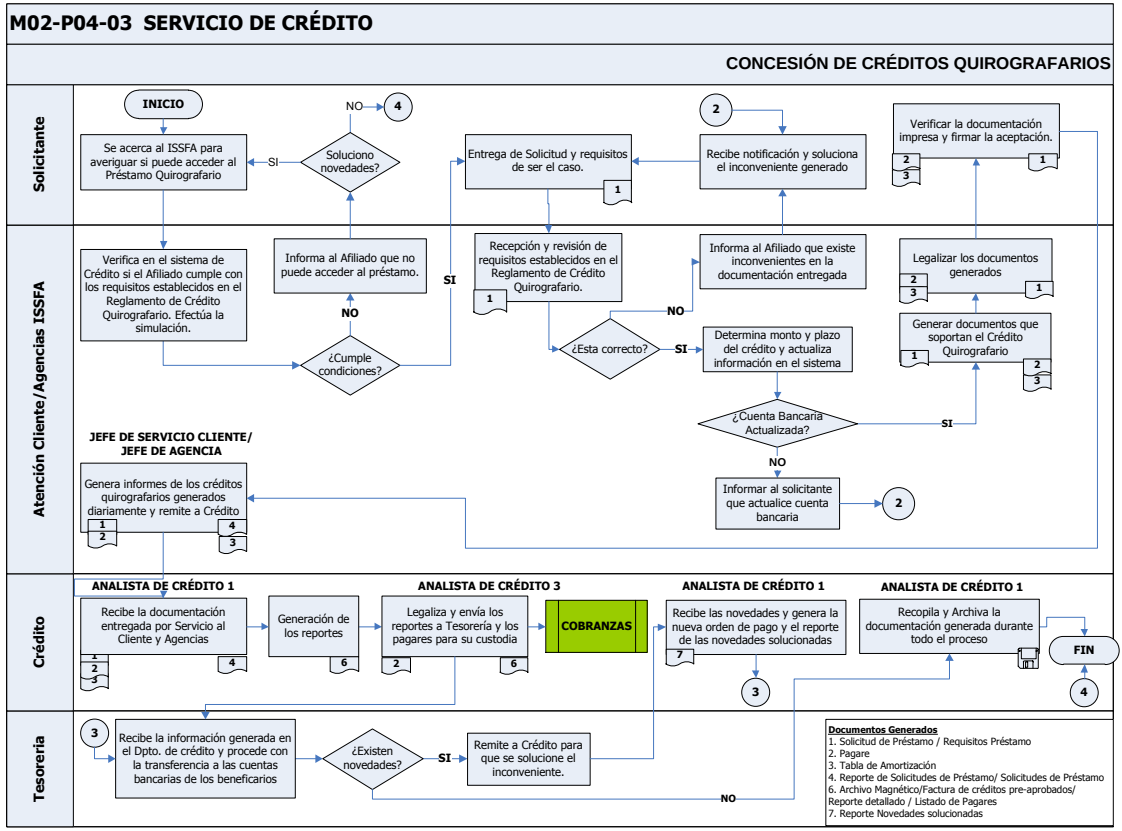
Clasificación Procesos

Gobernantes o estratégicos

Productivos, fundamentales u operativos

Habilitantes, de soporte o apoyo

Mapear los Procesos



Líneas de Negocio

Basilea	
Minorista	• Recepción de depósitos • Otorgamiento de créditos consumo y vivienda. • Negociación de letras de cambio, pagarés, facturas, que representen obligación de pago creados por ventas a crédito.
Microfinanzas	• Préstamos de microcrédito • Ahorro o transferencias a personas naturales que provenga de actividades económicas de menor escala
Tarjetas	• Actividades y servicios de tarjetas de crédito, débito, pago y prepago
Comercial	• Crédito comercial de primer piso, operaciones financieras de segundo piso del sector popular y solidario
Inmobiliaria	• Planificación, construcción y comercialización de proyectos de vivienda
Compensación de pagos	• Gestión de pagos, transferencias y compensación
Tesorería tradicional	• Gestión de liquidez y administración de flujo de fondos.

Identificación de Riesgo Operativo

Base de datos los distintos procesos, que permita:

La rápida identificación, clasificación, jerarquización con un enfoque de administración de riesgos.

FACTORES | **EVENTOS**

- Tipo
  - Gobernante
  - Productivo
  - Apoyo
- Nivel
  - Macro
  - Proceso
  - Subproceso
- Frecuenci
  - Diario
  - Semanal
  - Mensual
- Crítico
  - SI
  - NO

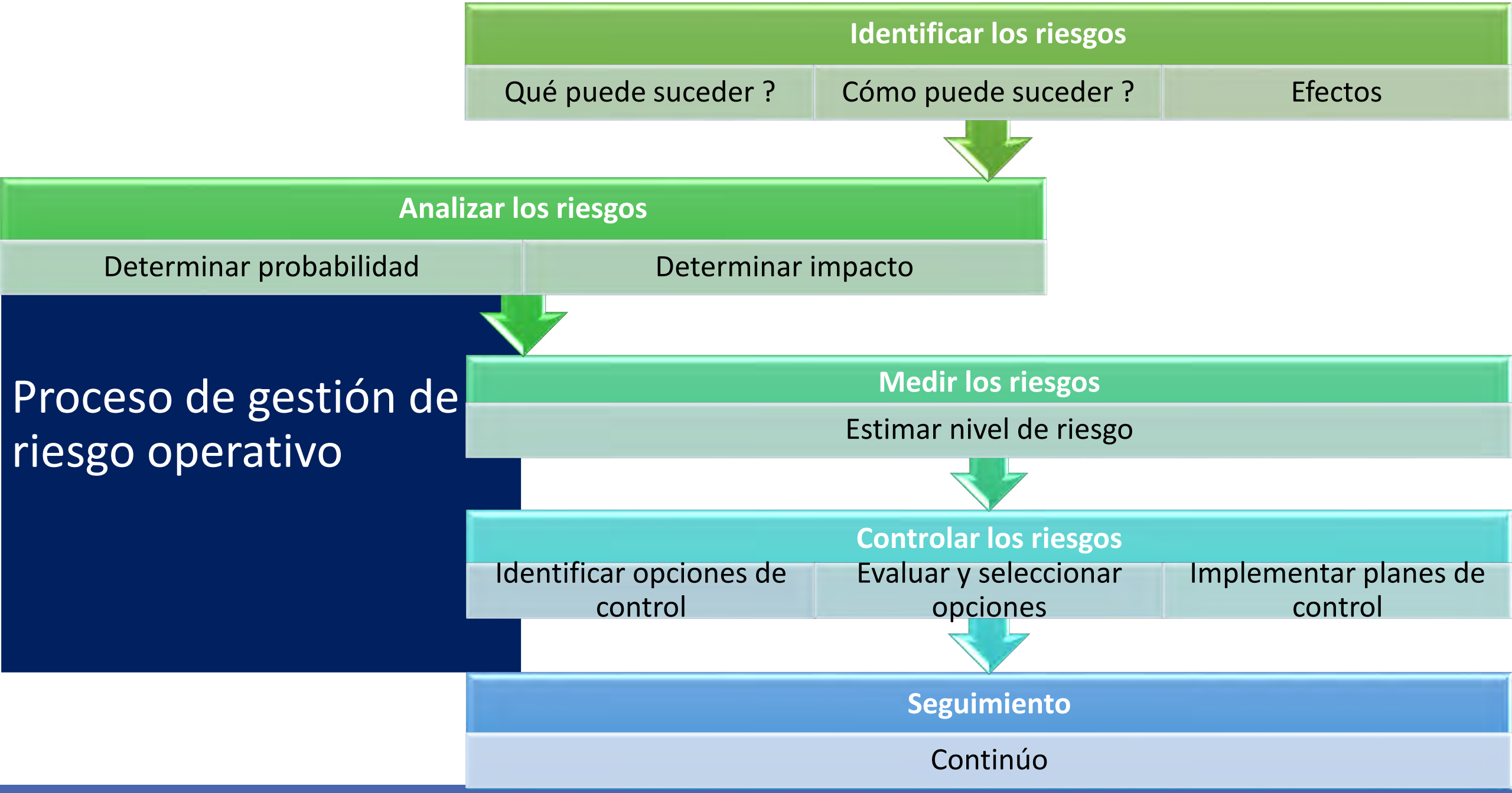
BASE DE DATOS – CUBO DE INFORMACION

- Nivel de Ejecución
  - Asistente
  - Técnico
  - Director
- Nivel de Supervisión
  - Director
  - Subgerente
  - Gerente
- Áreas Ejecutoras
  - Tesorería
  - Crédito
  - Contabilidad
- Manual Supervisión
  - SI
  - NO

Identificación de Riesgo Operativo

- **La identificación** de fuentes de riesgo se realiza teniendo en cuenta la cantidad potencial de fuentes e impactos.

- Lista genérica que focalice las actividades de **TODOS los riesgos**.


Identificar los riesgos
Qué puede suceder ?
Cómo puede suceder ?
Efectos
Analizar los riesgos
Determinar probabilidad
Determinar impacto
Proceso de gestión de riesgo operativo
Medir los riesgos
Estimar nivel de riesgo
Controlar los riesgos
Identificar opciones de control
Evaluar y seleccionar opciones
Implementar planes de control
Seguimiento
Continúo

Costos de las fallas en la Identificación de Riesgos

CONSECUENCIAS

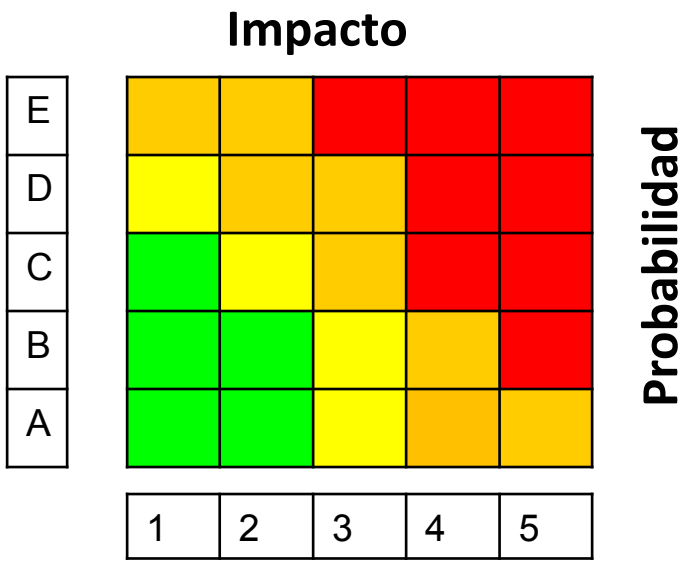
CAUSAS, FUENTES

Analizar el Riesgo Operativo

Identificar

Pérdidas y Amenazas al cumplimiento de objetivos, estratégicos y de negocio

Metodología: **Matriz de Riesgos (mapa de calor)**



1. Insignificante		A. Mu Baja
2. Menor		B. Baja
3. Moderado	✖	C. Moderada
4. Alto		D. Alta
5. Catastrófico		E. Muy Alta

Riesgo

Bajo
Moderado
Alto
Crítico

Analizar el Riesgo Operativo

Probabilidad	Nivel	Descripción
A	Muy baja	
B	Baja	
C	Moderada	
D	Alta	
E	Muy Alta	

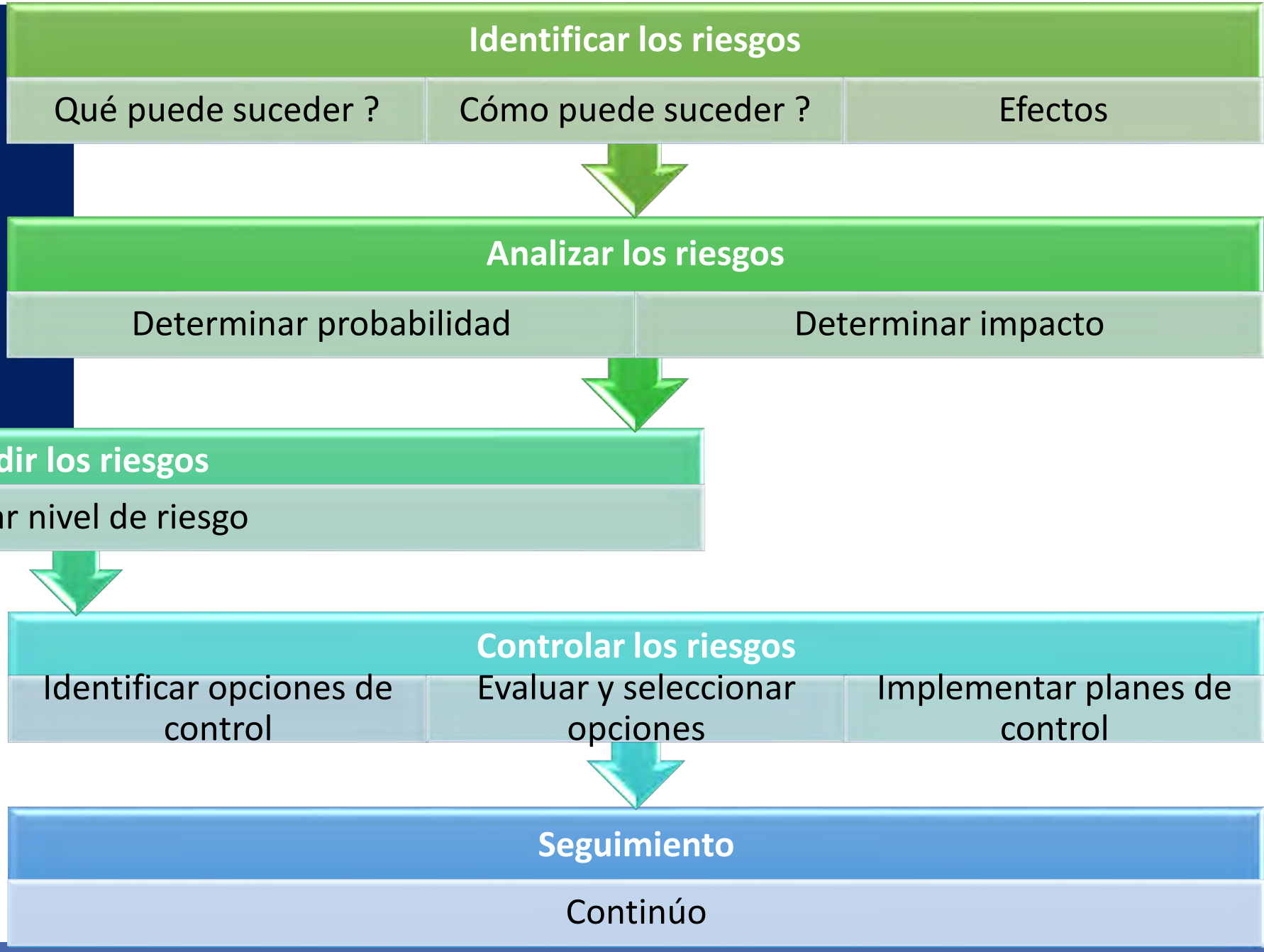
Impacto	Nivel	Descripción
1	Insignificante	
2	Menor	
3	Moderada	
4	Alto	
5	Catastrófico	

Riesgo	Nivel	Descripción
1	Bajo	
2	Moderado	
3	Alto	
4	Crítico	

Los eventos de riesgo se caracterizan por generar:

a) Pérdidas que afecten al estado de resultados;
b) Pérdidas que no afecten el estado de resultados; y,
c) Potenciales pérdidas que aún no se hayan materializado.

Proceso de gestión de riesgo operativo



Medición del Riesgo Operativo

Métodos de Valorización de los riesgos:

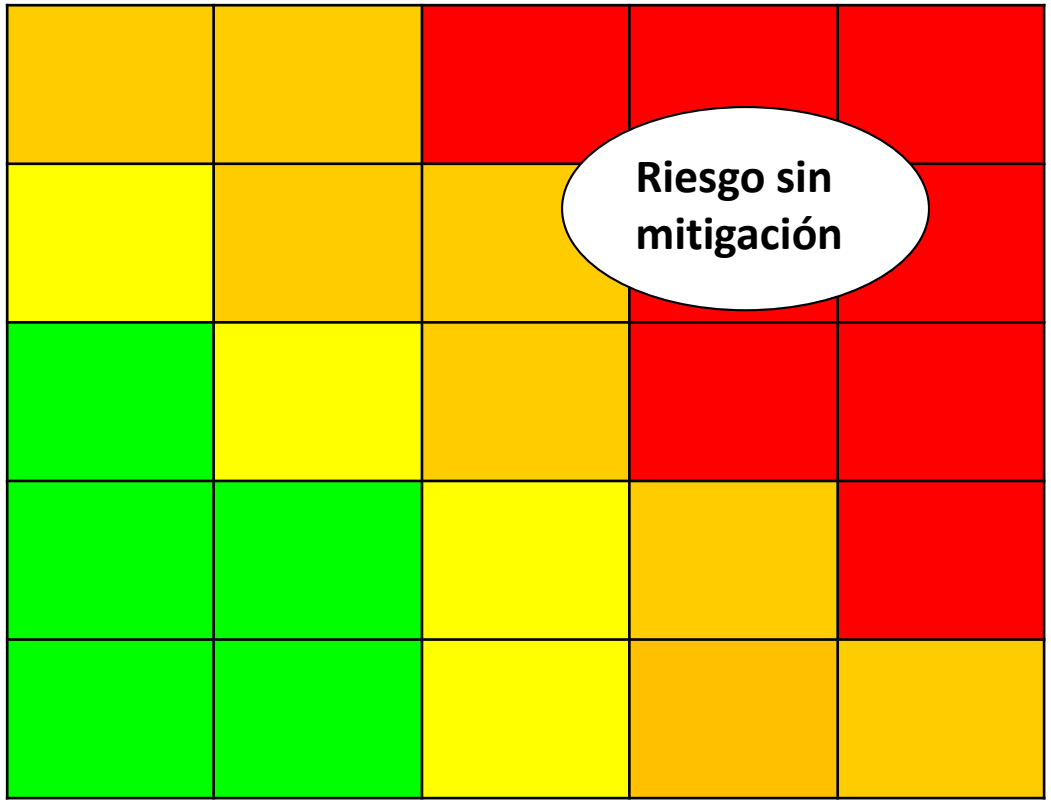
- **Cualitativos**
- **Semi-cuantitativos**
- **Cuantitativos**

Teniendo en cuenta la calidad y la disponibilidad de información.

Evaluaciones cuantitativas y semi-cuantitativas son las más prácticas.

La información cualitativa se utiliza cuando los datos numéricos son incompletos para llevar un análisis cuantitativo.

Matriz de Riesgos Inherente



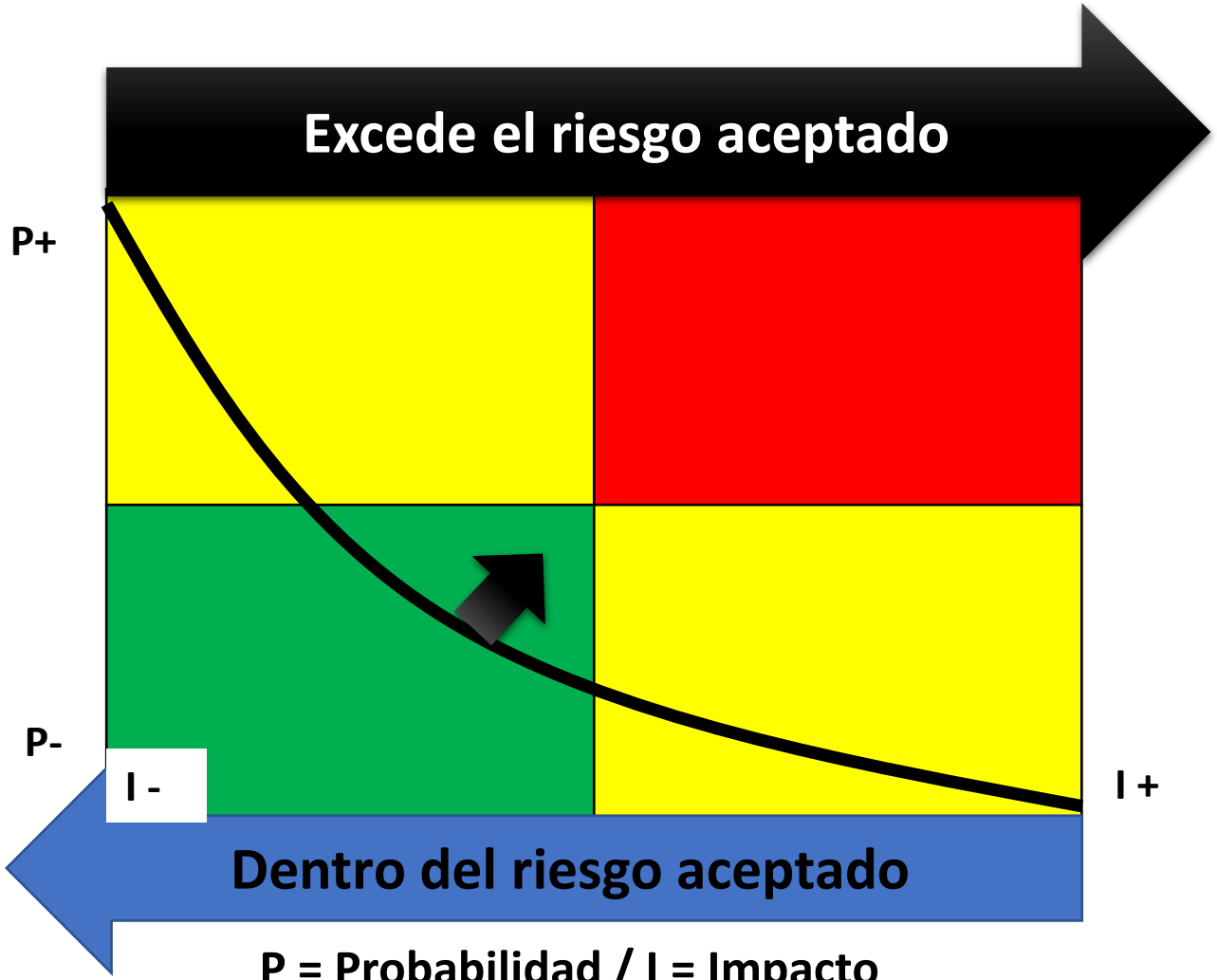
Medición del Riesgo Operativo

La Metodología de la Matriz de Riesgos que deberá estar contenida en un Manual.

Aprobado por el Comité Integral de Riesgos.

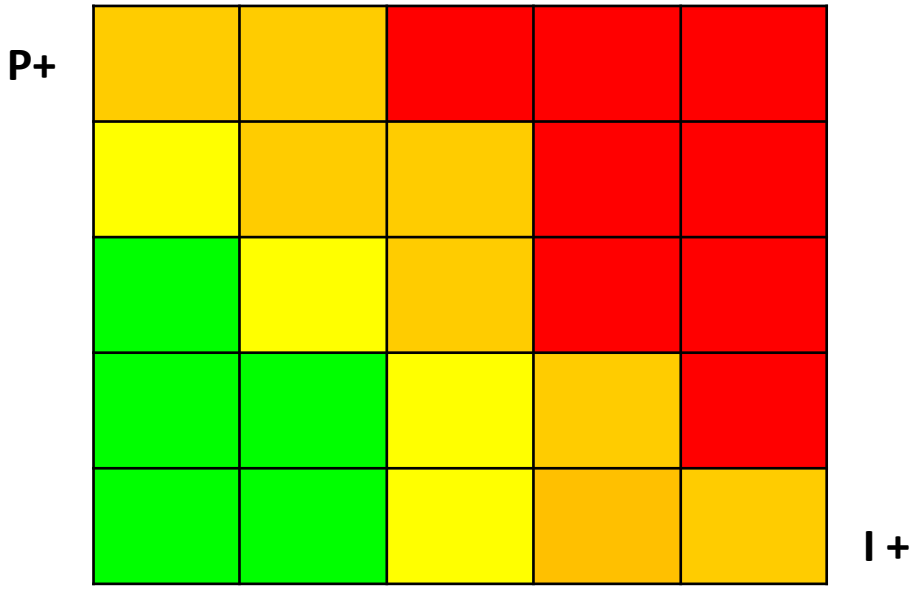
Las Gerencias deberán implementar la construcción de la matriz de riesgo con la coordinación del área de Riesgos.

Medición del Riesgo Operativo



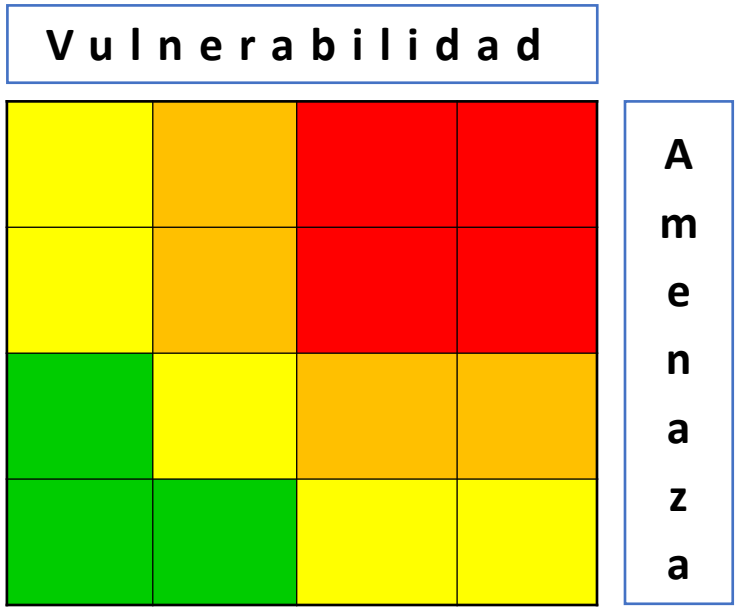
Limitaciones uso de la matriz

El análisis del riesgo en función de dos variables Probabilidad / Impacto, pudiera generar desviaciones en la percepción de algunos riesgos



Calculo de la Probabilidad:

Análisis de las Vulnerabilidades y Amenazas de un determinado evento de riesgo



Medición del Riesgo Operativo **– Método Cuantitativo**

OBJETIVO:

Medir la máxima perdida posible en un intervalo de tiempo y bajo un intervalo de confianza determinado.

REQUERIMIENTOS NECESARIOS GENERALES

- Participación activa de la Alta Dirección .
- Modelo integrado en los sistemas de medición y gestión de riesgos de la entidad.
- Comprobación por parte de los supervisores, de que el modelo de medición sirve para la gestión activa del riesgo, y es utilizado por la organización.
- Existencia de recursos suficientes en las líneas de negocio, áreas de control y auditoría.

Medición del Riesgo Operativo **– Método Cuantitativo**

- Método Básico
- Método Estándar
- Metodología Estandarizada
- Métodos Avanzados

Medición del Riesgo Operativo – **Método Cuantitativo**

Elementos necesarios para la medición del Riesgo Operativo **–AMA-**

Data histórica interna

Data de otras IFIS

Escenarios de análisis

Controles internos

Los sistemas de medida deben considerar

- Mitigación del riesgos
- Correlación de los eventos

CONTENIDO

1. Introducción al riesgo operativo
2. Metodologías y recomendaciones internacionales
3. Técnicas de identificación y medición del riesgo operativo
4. **Técnicas control y seguimiento del riesgo operativo**
5. Gestión de la tecnología e información
6. Plan de contingencia y continuidad de negocios
7. Riego Legal

Proceso de gestión de riesgo operativo

Identificar los riesgos

- Qué puede suceder ?
- Cómo puede suceder ?
- Efectos

Analizar los riesgos

- Determinar probabilidad
- Determinar impacto

Medir los riesgos

- Estimar nivel de riesgo

Controlar los riesgos

- Identificar opciones de control
- Evaluar y seleccionar opciones
- Implementar planes de control

Seguimiento

- Continúo

Gestión de Riesgo Operativo

Identificar controles asociados a cada uno de los riesgos, con el objetivo de determinar la efectividad de éstos, y de esta manera obtener el nivel de severidad residual.

Control	Efectividad	Confianza del Control
Insignificante	1	
Bajo	2	
Medio	3	
Alto	4	

Mitigación del Riesgo

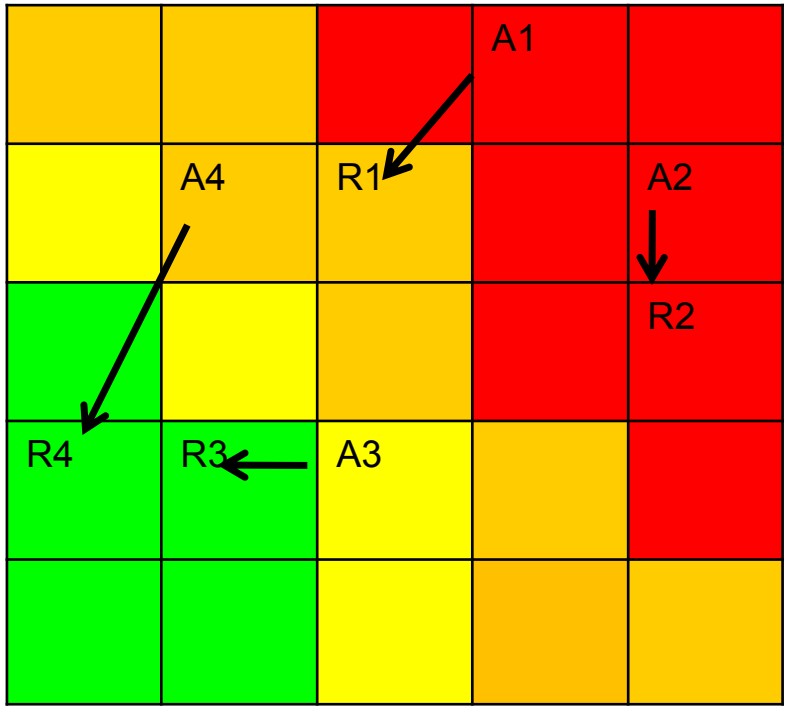
Gestión de Riesgo Operativo

Matriz de Riesgos Residual

Registra la posición final de los eventos de riesgo, evaluado por la probabilidad e impacto.

Algunos eventos han reducido:

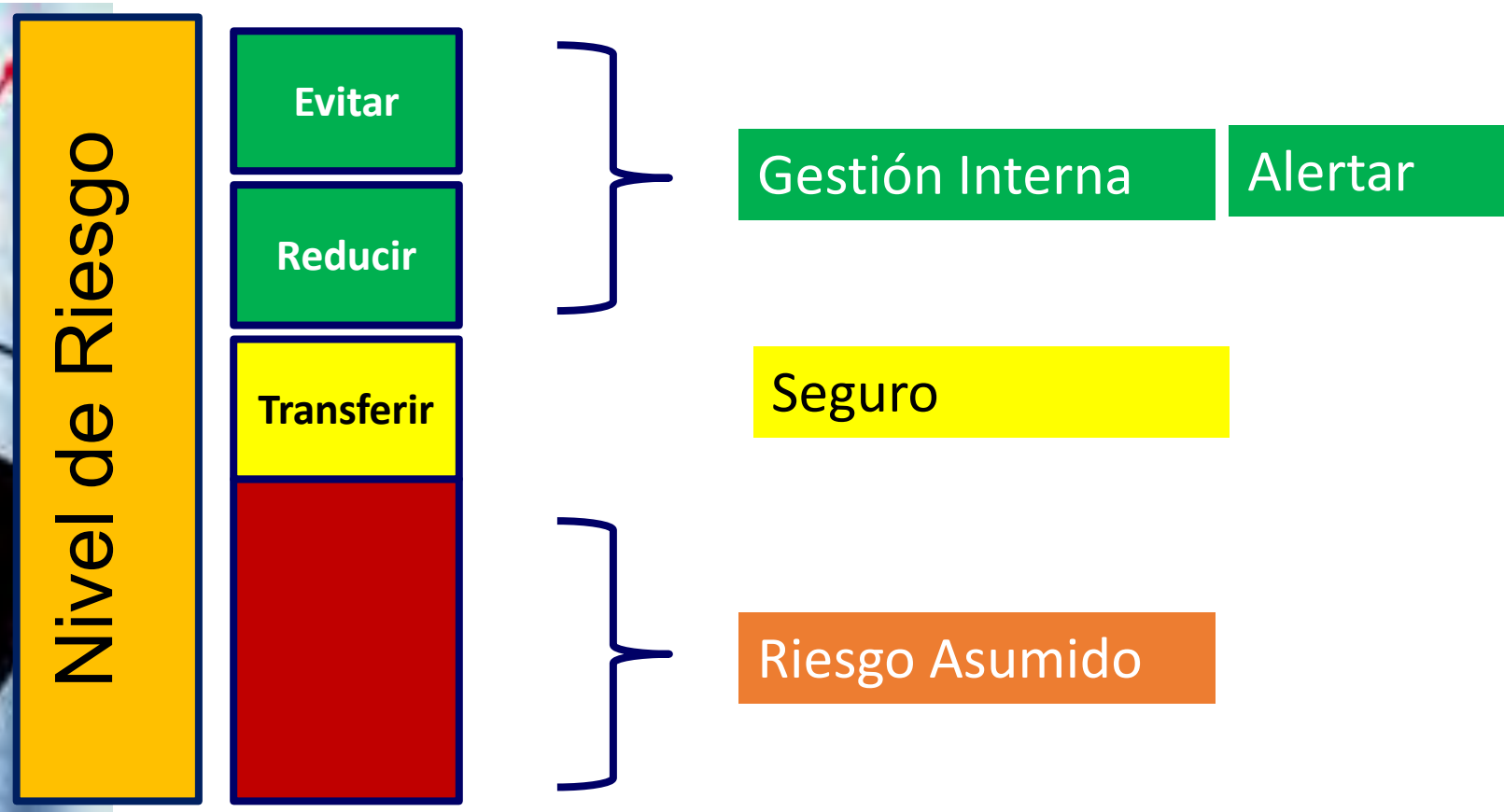
- solo el nivel de impacto,
- solo la probabilidad de ocurrencia
- Ambos, probabilidad e impacto.



Gestión de Riesgo Operativo

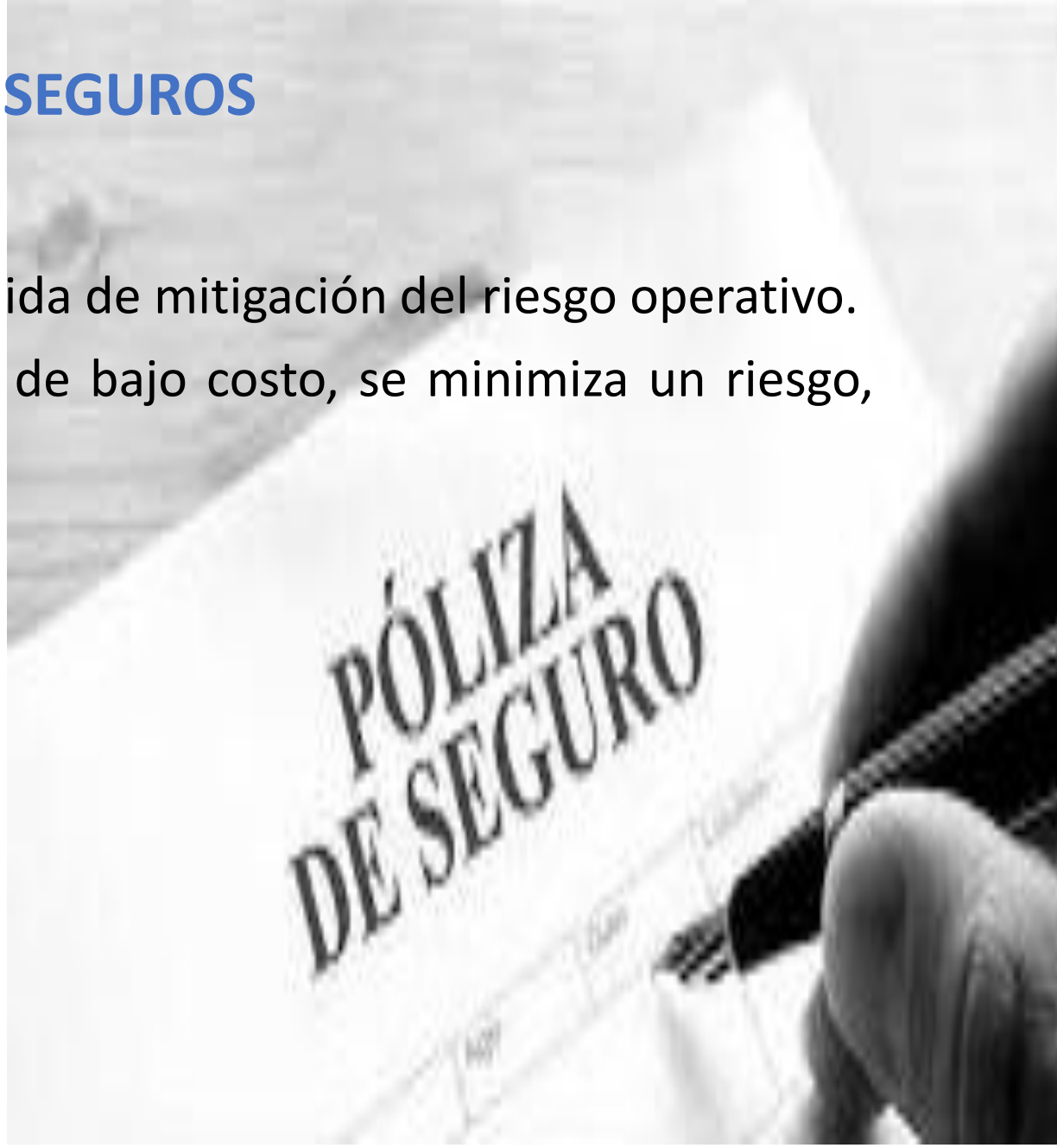
Resultado de multiplicar la Severidad del riesgo inherente por el porcentaje de mitigación del control

Transferencia del riesgo - Póliza de seguros



POLIZA DE SEGUROS

- La contratación de seguros es una medida de mitigación del riesgo operativo.
- A través de una prima, relativamente de bajo costo, se minimiza un riesgo, relativamente alto.
- El Comité de Basilea, permite que a través de una política de seguros mitiguen los ROP, teniendo en cuenta:
  - Tipo de coberturas y pagos
  - Niveles de cobertura
  - Activadores del seguro
  - Resolución de controversias.



TIPOS DE POLIZAS

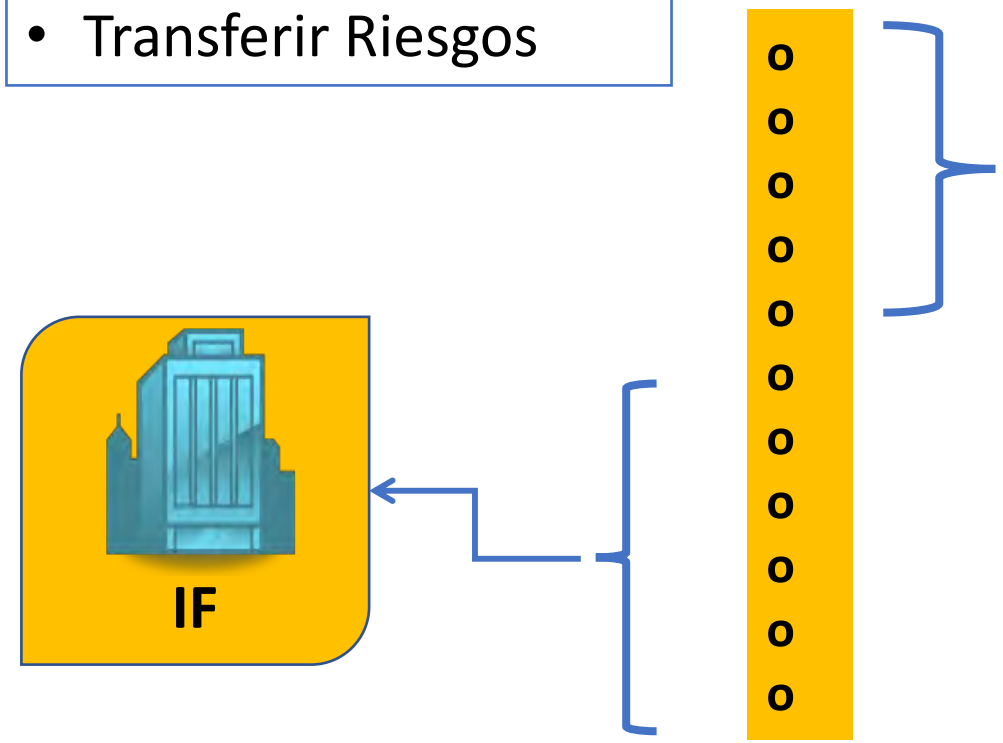
De Riesgo Específico	• Las más contratadas, concentradas en determinados eventos.
Multiproductos	• Agrupación de pólizas específicas en carteras multiproductos.
Cobertura Agregada	• Que afecte a la totalidad del espectro del riesgo operacional.

Riesgo de Tercerización

Tercerización de Servicios Financieros

Objetivos:

- Reduce Costos
- Transferir Riesgos



Pueden ser empresas donde la administración y el cumplimiento del proveedor no esta regulado.

Tercerización de Servicios Financieros

Principios en la tercerización de servicios financieros de IFIS:

- Evaluación de actividades que pueden ser tercerizadas
- Establecimiento de programas de administración de riesgo de actividades tercerizadas
- Evaluación exhaustiva de proveedores
- Regulación mediante contratos de los servicios tercerizados
- Mantenimiento de planes de contingencia por parte de la IFI y el proveedor
- Protección de información
- No reduce la capacidad de las IFIs de cumplir con sus obligaciones con clientes y supervisores. **NO SE TRANSFIEREN**

Tercerización de Servicios Financieros

Desventajas

- Afectar la confidencialidad.
- Perder el control sobre el producto final y afectar la calidad.

Áreas que no deben tercerizarse

- Administración de Planeación Estratégica
- Tesorería
- Administración de calidad
- Evaluación de servicio al cliente
- Estrategia de distribución y ventas

CONTENIDO

1. Introducción al riesgo operativo
2. Metodologías y recomendaciones internacionales
3. Técnicas de identificación y medición del riesgo operativo
4. Técnicas control y seguimiento del riesgo operativo
5. **Gestión de la tecnología e información**
6. Plan de contingencia y continuidad de negocios
7. Riego Legal

Definición

C ***Control***

OB ***Objectives***

I ***for Information***

T ***and Related Technology***

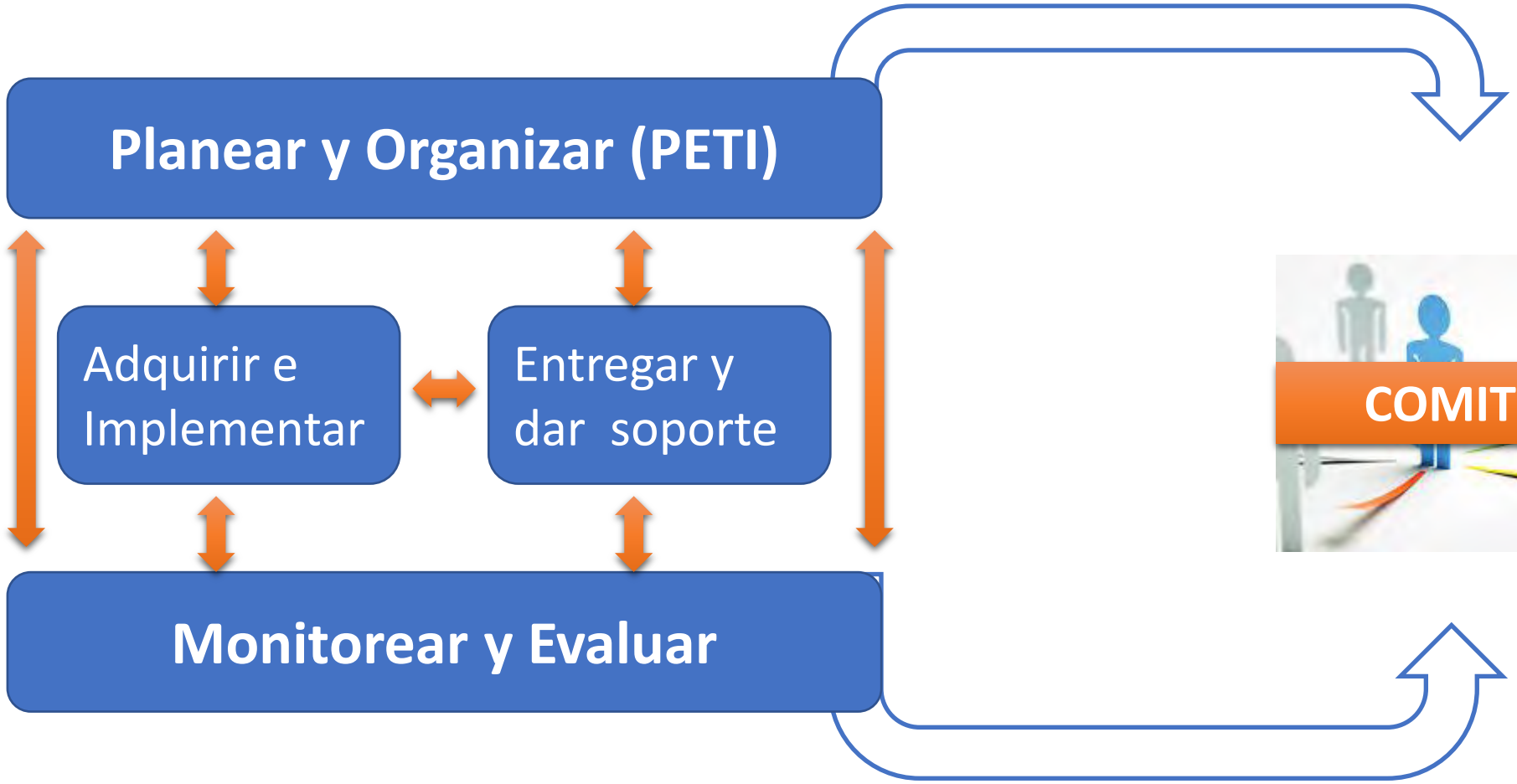
COBIT 5 - GEIT

- No es una disciplina aislada, sino una parte integral del gobierno corporativo.
- Aprovechar al máximo las ventajas de TI, maximizar los beneficios, capitalizando las oportunidades y ganando ventaja competitiva.
- Está relacionado con la entrega de valor de TI al negocio y la mitigación del riesgo relacionado con TI.

Objetivos del GEIT		
Realización de beneficios	Optimización del riesgo	Optimización de recursos

COBIT 5

Orientado a Procesos - Organizado en cuatro dominios:

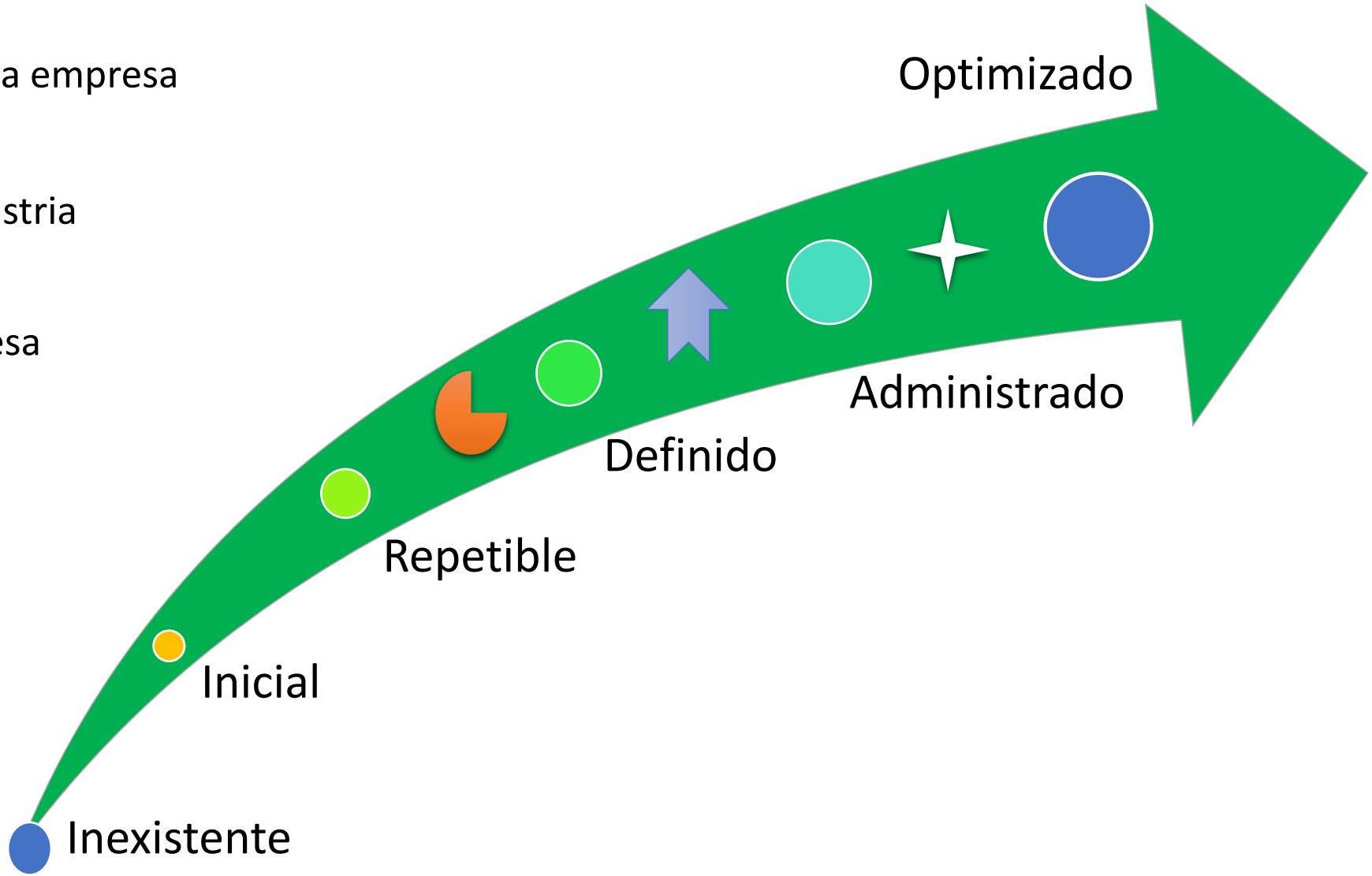


Modelo de Madurez

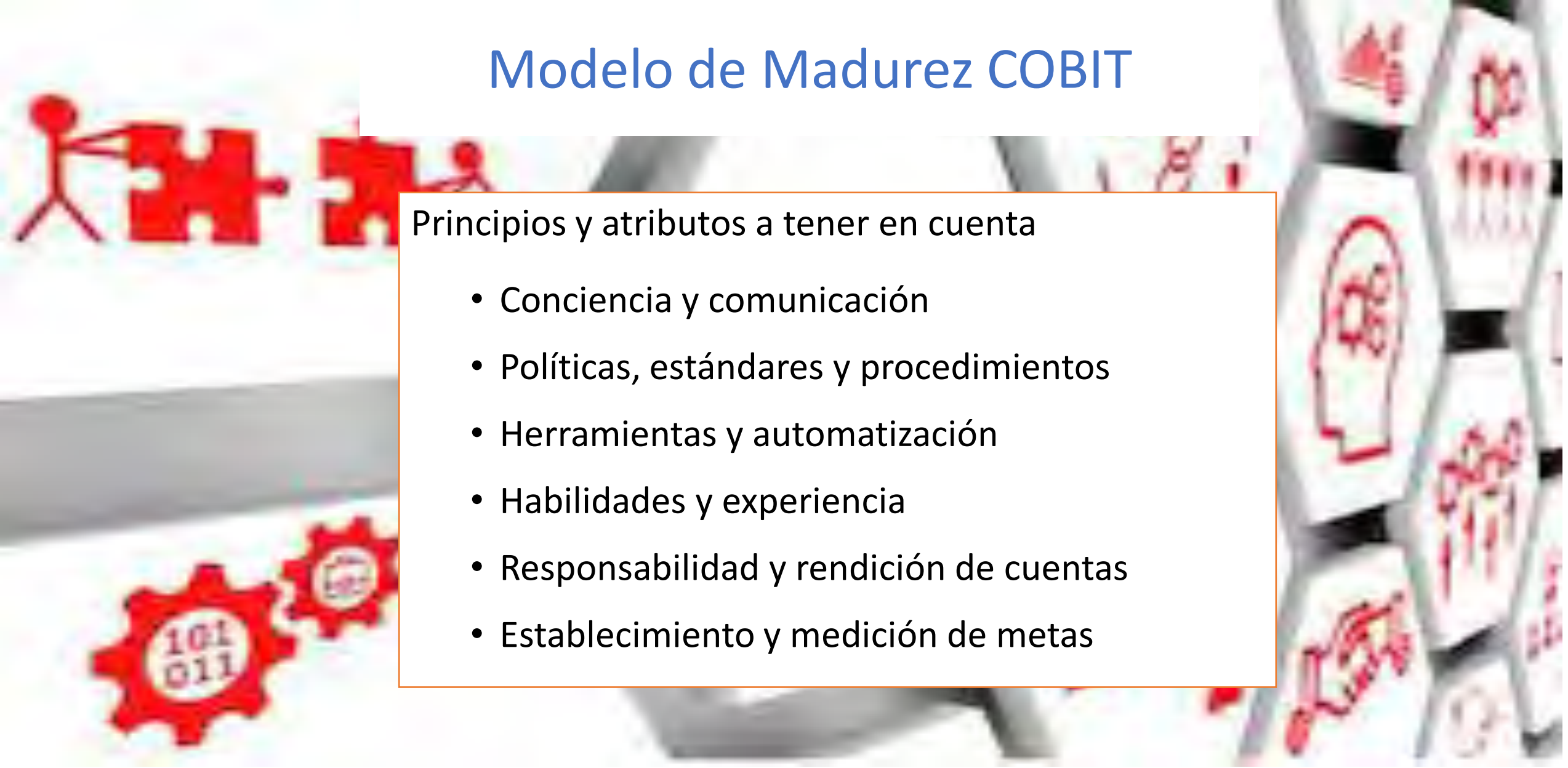
Situación actual de la empresa

Promedio de la Industria

Objetivo de la empresa



Modelo de Madurez COBIT



Principios y atributos a tener en cuenta

- Conciencia y comunicación
- Políticas, estándares y procedimientos
- Herramientas y automatización
- Habilidades y experiencia
- Responsabilidad y rendición de cuentas
- Establecimiento y medición de metas

Seguridad de la información - SGSI

Adecuada interrelación de normas, procedimientos, mecanismos y recursos en una ADECUADA estructura de la Organización.

Adecuada interrelación de normas, procedimientos, mecanismos y recursos informáticos en una ADECUADA estructura de la Organización.

Un Plan de Seguridad de Información debe incluir:

- Los activos de tecnología que deben ser protegidos
- Metodología usada
- Objetivos de control y controles
- Grado de seguridad requerido.

Seguridad física

Ciberseguridad

Principios de confidencialidad, disponibilidad e integridad

Vulnerabilidades - Cyberseguridad

Técnicas	Del Proceso	Organizacional	Emergente
• Errores de diseño / configuración	• Errores en la operación	• Errores en la gestión, decisiones, planificación	• Interacciones o cambios de ambiente

Seguridad de la información - SGSI

CONFIDENCIALIDAD

- La información no pueda estar disponible para personas, entidades o procesos **NO** autorizados.

INTEGRIDAD

- La información podrá ser modificada, sólo por el personal autorizado.
- Garantizar que la información no sea modificada mientras está en comunicación.

DISPONIBILIDAD

- La información está disponible en el lugar, momento y forma en que es requerido por el usuario autorizado.

Sensibilidad de la información

Criterios de sensibilidad de la información

Secreta

Información muy sensible para la entidad
Su divulgación puede ser perjudicial

Sensible

Información sensible para la entidad
El acceso debe ser controlado y autorizado

Uso interno

Información a utilizar dentro de la entidad
Su acceso puede ser controlado y autorizado

Pública

Información que puede ser conocida
Libremente por el personal y externos

Actores de la información

PROPIETARIO

- Responsable de identificar, clasificar y establecer las medidas de protección adecuadas a cada categoría.

CUSTODIO

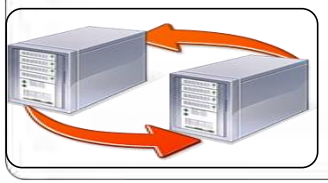
- Responsable de guardar, mantener y proteger adecuadamente los activos de información según su clasificación.

USUARIO

- Empleados a quienes les ha asignado licencias de uso de software o Sistemas de Información para el desempeño de sus funciones.
- Son responsables de conocer el nivel de protección designado y cumplir con los controles establecidos para su protección.

Respaldo de la información

Estrategia de respaldo de información:



Datos de aplicaciones centralizadas

Datos almacenados en estaciones de trabajo de los usuarios

Sistemas Operativos, software de escritorio y aplicaciones centralizadas

Servicios de Correo electrónico y Web

Matriz de clasificación de la información

CATEGORIAS					Propietario	Custodio			
	Secreta	Sensible	Uso Interno	Pública			Múltiples	Grupos	Individuales

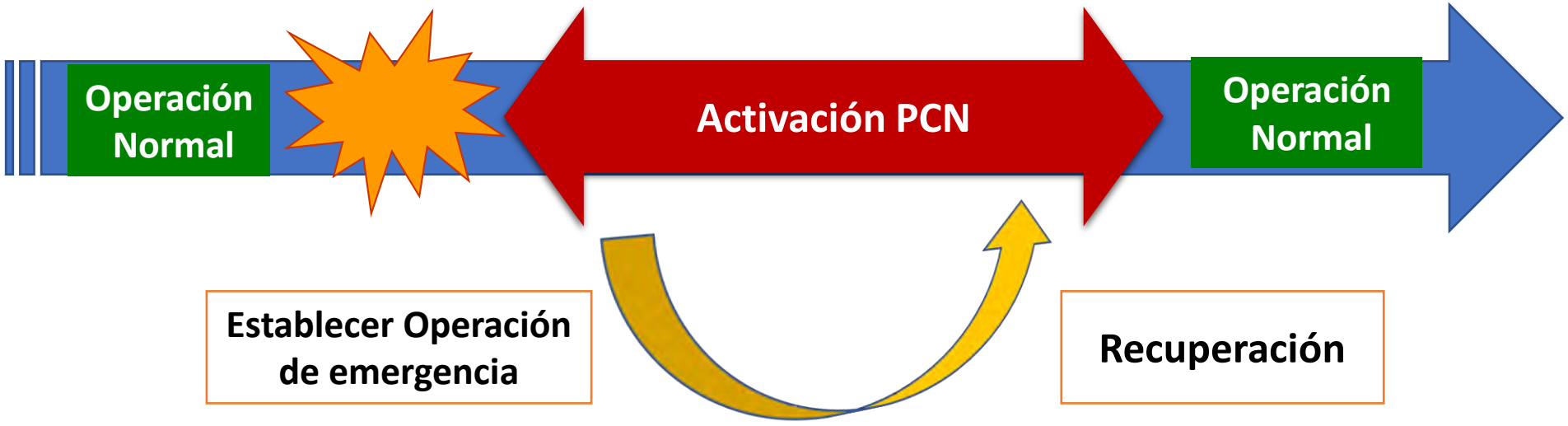
CONTENIDO

1. Introducción al riesgo operativo
2. Metodologías y recomendaciones internacionales
3. Técnicas de identificación y medición del riesgo operativo
4. Técnicas control y seguimiento del riesgo operativo
5. Gestión de la tecnología e información
6. **Plan de contingencia y continuidad de negocios**
7. Riego Legal

Aspectos Generales : Plan Continuidad del Negocio

Concepto

Un plan que mantiene la continuidad de los procesos críticos del negocio requeridos a un nivel aceptable de operación desde el momento de ocurrencia de un evento de interrupción de los mismos y/o de los recursos que los soportan hasta la recuperación de la normalidad.



Lecciones Aprendidas

Aspectos Generales : Plan Continuidad del Negocio

Objetivos:

- Garantizar la capacidad para operar en forma continua.
- Minimizar las pérdidas
- Minimizar el impacto cuantitativo y cualitativo
- Superar eficientemente la pérdida total o parcial de la capacidad operativa
- Salvaguardar los intereses de la institución, reputación, marca y actividades críticas.
- Adoptar medidas preventivas para minimizar la probabilidad de ocurrencia de contingencias que afecten a los procesos críticos de la Organización.

Minimizar el número de decisiones a ser tomadas durante la duración de un desastre, garantizando la **correcta** recuperación de los sistemas y procesos.

Recomendaciones Basilea (BIS)

1.- **Obligaciones y responsabilidades del Consejo y alta administración**:

Promover la creación de una cultura organizativa que otorgue la necesaria importancia a asegurar la continuidad del negocio.

Establecer quiénes entre los ejecutivos formarían parte de un equipo de “gestión de crisis”, sus funciones, responsabilidades y autoridad, así como por quiénes deberían ser sustituidos en caso necesario.

Recomendaciones BIS

2.- Riesgo de que se produzcan perturbaciones operativas graves:

Contemplar cómo responderán ante una gran perturbación operativa que afecte a las entidades financieras o al sistema financiero.

A través de un “análisis de impacto” del negocio, establecer un orden de prioridades para el restablecimiento de sus funciones y operaciones.

Recomendaciones BIS

3.- Objetivos de recuperación y restablecimiento de la actividad:

Desarrollar objetivos de recuperación que reflejen y sean proporcionales al riesgo.

Considerar en su gestión de la continuidad de su negocio el riesgo que una perturbación que les ocurra pueda afectar también a la capacidad de otras entidades financieras – o incluso del conjunto del sistema financiero.

Recomendaciones BIS

4.- Comunicaciones internas y externas:

Entidades y autoridades deben incluir en sus planes de continuidad de negocio procedimientos de comunicación tanto dentro de sus organizaciones como con terceras partes en caso de que se produzca un problema operativo importante.

5.- Comunicaciones transfronterizas:

Comunicación con autoridades financieras de otras jurisdicciones en caso de que se pueda producir un fallo operativo de importancia que tenga implicaciones transfronterizas.

Recomendaciones BIS

6.- Comprobación de la eficacia y actualización de los planes:

Comprobar periódicamente la capacidad de restablecimiento de las operaciones críticas según los objetivos marcados.

Auditoría interna y externa valoren la efectividad y resultados de los programas de comprobación que realice la entidad e informar de sus resultados al Directorio de la entidad.

Los programas de comprobación en centros alternativos o de respaldo tienen especial relevancia en el caso de entidades con una mayor importancia relativa en el sistema financiero.

Fases del plan de continuidad

Identificar procesos críticos

- Indispensable para la continuidad del negocio y las operaciones
- Falta de identificación y aplicación puede generarle un impacto financiero negativo

https://www.youtube.com/watch?v=xsFYbkY3aeI&t=216s

3. Definición del Plan de Continuidad

Identificación de riesgos potenciales y amenazas

Eventos Naturales	Eventos Provocados	Pérdida de Servicios	Falla en equipos y sistemas:
Inundación Temblor Incendio Terremoto	Sabotaje Vandalismo Robo	Falla eléctrica Falla en comunicaciones	Energía interna Aire acondicionado

Incidentes de Seguridad de la Información:	Otras situaciones de emergencia
Ataque cibernético Pérdida de registro de datos Revelación de información sensible Falla en los sistemas	Ubicación Moral de los empleados Publicidad Negativa Problemas legales

3. Definición del Plan de Continuidad

Valoración de Riesgos:

- **Limitaciones**:
  - Identificar todas las amenazas y estimaciones de probabilidad para riesgos operacionales catastróficos.
  - Determinar la formula para priorizar las amenazas y tabular un sistema scoring:

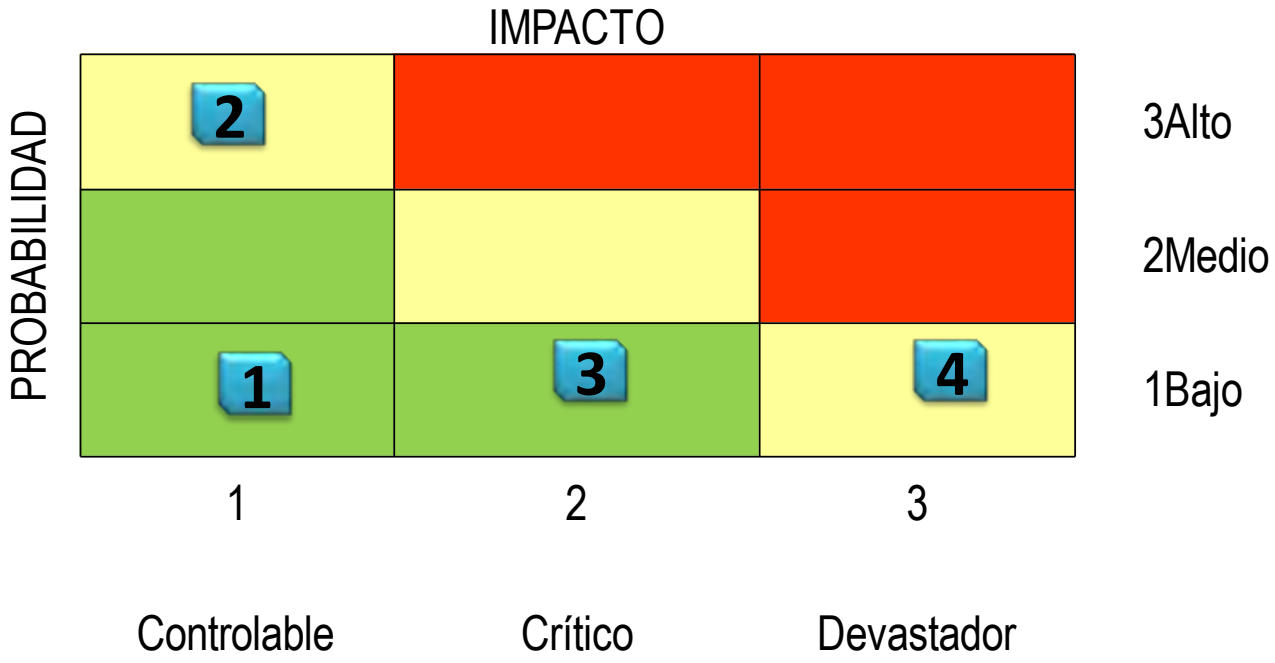
    - **Riesgo = amenaza de impacto x probabilidad**
    - **Prioridad= riesgo x habilidad para controlar el riesgo**

- **Enfoque**: Analiza y valora el riesgo en las funciones más criticas determinadas

- **Control del riesgo**: Aceptación, reducción, transferencia o remover la causa.

3. Definición del Plan de Continuidad

Matriz de Eventos de Riesgo



Evento		Definición	Probabilidad	Impacto
NATURALES	1	Inundación	Baja	Controlable
	2	Temblor	Alta	Controlable
	3	Incendio	Baja	Crítico
	4	Terremoto	Baja	Devastador

3. Definición del Plan de Continuidad

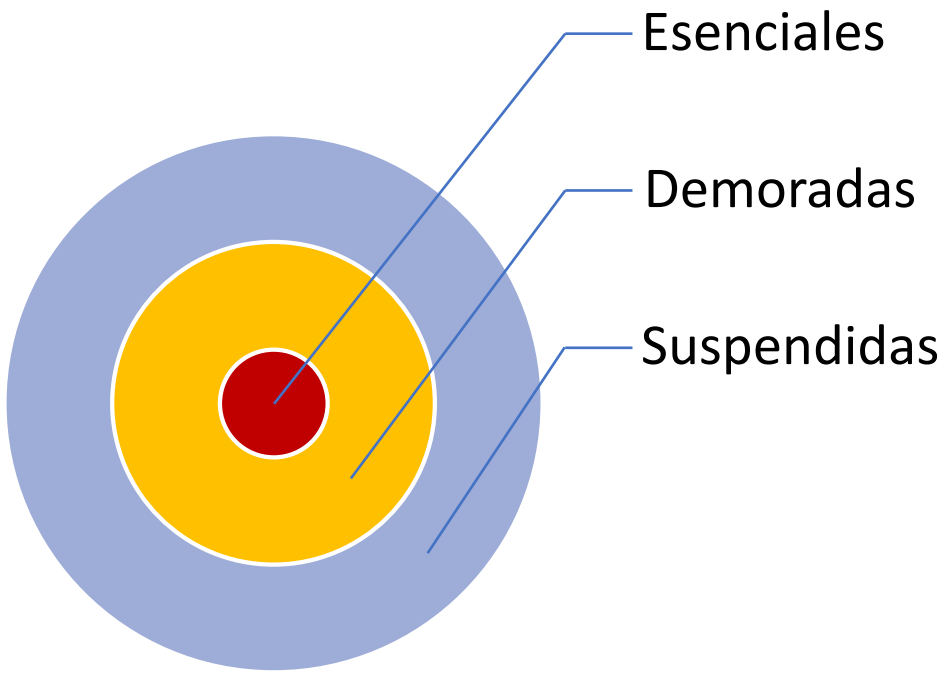
Valoración del impacto de los eventos de riesgo en los procesos

ANALISIS DE CRITICIDAD		
Descripción		Tiempo de interrupción
Críticos:		Menos de 1 día
Vitales:		
Sensitivos:		
No críticos:		Más de x días

3. Definición del Plan de Continuidad

Valoración de Impacto de los Eventos de Riesgo en TI

Es necesario comprender los procesos críticos de la organización, y la dependencia que tienen de las aplicaciones tecnológicas. Se pueden clasificar las aplicaciones en categorías, ejemplo:



3. Definición del Plan de Continuidad

Desarrollo de una respuesta

1.- Punto de Recuperación Objetivo:
Que tan actualizados necesitan estar los datos?

2.- Máximo tiempo de interrupción tolerable

3.- Tiempo de Recuperación Real

3. Definición del Plan de Continuidad

- Estrategias genéricas para mitigar el impacto de una interrupción o reducir la probabilidad de un evento de amenaza.
- Cada estrategia tiene parámetros de velocidad de recuperación, confiabilidad, capacidad y costos que son apropiados para diferentes segmentos del negocio
- Análisis costo/beneficio para cada alternativa a fin de alcanzar los tiempos objetivos de recuperación y asegurar costos adecuados.
- Estrategia acordada: datos para el proyecto de implementación y plan de acción.

Estrategia de recuperación

3. Definición del Plan de Continuidad

Desarrollo de una respuesta - Definir Situación de Riesgo

- Aplicaciones
- Responsable
- Personas que usan
- Criticidad
- Tiempo Tolerable de Interrupción
- Controles funcionales e informáticos
- Posibilidad procesar en diferido
- T sin procesar datos
- Efecto inmediato de no disponer de información
- Efecto de largo plazo

- Volumen de transacciones
- Horario programado de interrupción
- Tiempo programado de interrupción
- La aplicación ha tenido problemas de procesamiento
- Tiempo promedio mensual de interrupción
- Las pérdidas de datos afectan el desarrollo de los negocios

3. Definición del Plan de Continuidad

Desarrollo de una respuesta: Recursos requeridos por proceso

PROCESO

- Depósitos
- Cartera
- Inversiones
- Contable
- Fideicomisos

Día 1 / Día 2 / Día 3

RECURSOS

- Personal
- Cubículos, Escritorios, Sillas, Teléfonos, Pc's, Impresoras, Copidaoras.

3. Definición del Plan de Continuidad

Matriz de Roles y Funciones del Equipo de Continuidad

Identifica las acciones que deben realizarse para poner en marcha el Plan de Continuidad en base a las estrategias definidas.

Las acciones especificadas en el plan de continuidad definen los ámbitos de gestión que le competen, tomando en cuenta que por su naturaleza cada incidente es diferente.

3. Definición del Plan de Continuidad

Procedimientos de emergencia

Los objetivos de los procedimientos de emergencia son:

- Minimizar el daño a los equipos
- Obtener un reporte de valoración de daños dentro de las **XXXXX** primeras horas de la interrupción
- Recuperar los sistemas y capacidades de procesamiento, almacenamiento y comunicación dentro del tiempo de recuperación objetivo establecido.

La seguridad de los empleados, es la primera prioridad en un evento de contingencia.

CONTENIDO

1. Introducción al riesgo operativo
2. Metodologías y recomendaciones internacionales
3. Técnicas de identificación y medición del riesgo operativo
4. Técnicas control y seguimiento del riesgo operativo
5. Gestión de la tecnología e información
6. Plan de contingencia y continuidad de negocios
7. Riego Legal

RIESGO LEGAL

Definición BIS, la posibilidad de ser sancionado, multado u obligado a pagar daños punitivos como resultado de acciones supervisoras o de acuerdos privados entre las partes.

Definición SEPS, Es la probabilidad de que una entidad incurra en pérdidas debido a la inobservancia e incorrecta aplicación de disposiciones legales, normativas e instrucciones emanadas por organismos de control; aplicación de sentencias o resoluciones judiciales o administrativas adversas; deficiente redacción de textos, formalización o ejecución de actos, contratos o transacciones o porque los derechos de las partes contratantes no han sido debidamente estipuladas.

- El Riesgo Legal, desde la perspectiva del ROP debe ser identificado, valorado mediante escalas cualitativas y cuantitativas.
- Debe ser comunicado y monitoreado periódicamente por los niveles administrativos.

RIESGO LEGAL

OBJETIVOS

Identificar de forma oportuna el Riesgo Legal a través del análisis de la información de la organización en lo que tiene relación con asuntos legales que implican riesgo

ALCANCE

Contratos, resoluciones y procedimientos, cuya inobservancia o falta de aplicación puede causar daños a la organización

RIESGO LEGAL – Clasificación

- **Riesgo de documentación:** Documentos incorrectos o extraviados, o la inexistencia de ellos, que incida negativamente en las actividades de negocio.

- **Riesgo de legislación:** Operaciones que no puedan ser ejecutadas por prohibición, limitación o incertidumbre acerca de la legislación del país de residencia de alguna de las partes, o por errores en la interpretación.

- **Riesgo de capacidad:** Se refiere a dos conceptos: riesgo de que la contraparte no tenga capacidad legal para operar en un sector, producto o moneda determinada y el riesgo de que las personas que actúan en nombre de la contraparte no cuenten con poder legal suficiente para comprometerla.

RIESGO LEGAL – Categorización

Actos societarios	Decisiones de los órganos de gobierno, necesarios para el desenvolvimiento societario de las entidades
Gestión de crédito	Documentación relacionada con la instrumentación y gestión de las operaciones de crédito.
Operaciones del giro financiero	Documentación relacionada con la instrumentación y gestión de otras operaciones no relacionadas al crédito.
Actividades complementarias de las operaciones del giro financiero	Las que sin ser propias del giro financiero, son necesarias para el cumplimiento y desarrollo de su objeto social.
Estipulaciones contractuales	Cláusulas mínimas
Proveedores extranjeros	Deberán estar domiciliadas en el país o contar con un representante legal en el Ecuador, para responder por las obligaciones contraídas.
Cumplimiento legal y normativo	Procesos de verificación el cumplimiento legal y normativo

Aspectos del Riesgo Legal

- Leyes
- Decretos
- Normas

1

Variables internas de cumplimientos permanente. Políticas relacionadas con: el negocio, recursos humanos, clientes, terceros, etc.

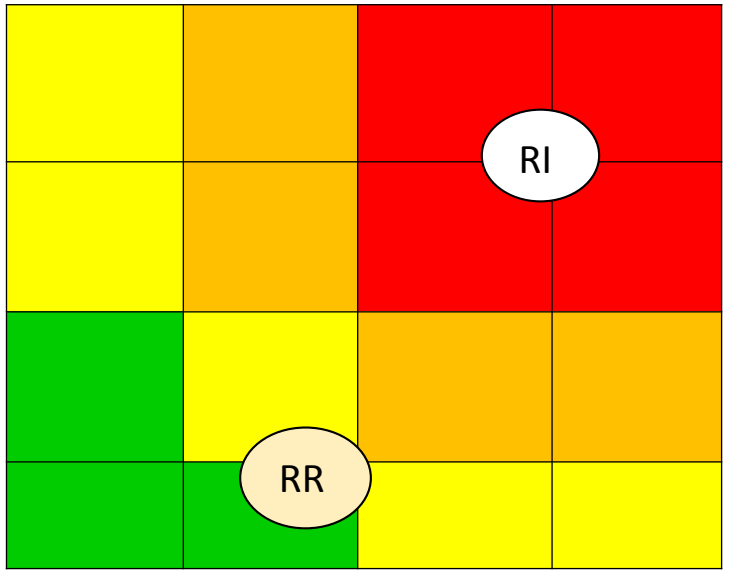
2

Elemento esencial en el sistema financiero a fin de evitar problemas relacionados a lavado de activos y adicionalmente con el riesgo reputacional.

3

Matriz de riego legal

- Ley, Regulación o Política Corporativa
- Descripción del Requerimiento
- Penalización o consecuencia de no cumplir con el requerimiento
- Riesgo Inherente
- Evaluación del Riesgo Inherente (A - M - B)
- Controles clave para el cumplimiento del requerimiento
- Frecuencia del aseguramiento del control
- Acciones por realizar
- Responsables
- Comprensión de las disposiciones legales
- Estimar la probabilidad que se emitan resoluciones adversas y estimar las pérdidas correspondientes.



Control del riego legal

- Operaciones estén de conformidad con las disposiciones legales
- Incursión de nuevos productos o mercados deben contar con un análisis de riesgo legal
- Políticas para que previo a la celebración de actos jurídicos se analice su validez
- Manual de políticas legal
- Reportes de riesgo legal: estado de los juicios, pérdida esperada
- Cumplimiento de políticas, verificado por las áreas de control, riesgo y auditoria, al menos una vez al año.
- Valoración de Demandas, Multas

PREGUNTAS

GRACIAS

ivanv@iv-consultores.com