Riesgo Operativo

Roger Augusto Chamba González

DGRV – Confederación Alemana de Cooperativas

Agosto 2022

cooperación alemana
DEUTSCHE ZUSAMMENARBEIT

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

EIN GEWINN FÜR ALLE
Die Genossenschaften

DGRV
DIE GENOSSENSCHAFTEN

Agenda

- Introducción al Riesgo Operativo
- Factores de riesgo
- Gestión de eventos de riesgos
- Tecnología de la información
- Seguridad de Información
- Inventario de infraestructura tecnológica
- Respaldos y custodia de información (backups externos)

DGRV
DIE GENOSSENSCHAFTEN

“No es la especie más fuerte la que sobrevive ni la más inteligente, sino la más receptiva al cambio”

Leon C. Megginson

¿Que es lo que se busca con esta capacitación?

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

EIN GEWINN FÜR ALLE
Die Genossenschaften

DGRV
DIE GENOSSENSCHAFTEN

Conciencia del riesgo

"…con toda mi experiencia, nunca he visto un accidente de ninguna clase que merezca mencionarse. Ni siquiera he visto un sólo barco con problemas en alta mar… Nunca he visto un hundimiento ni estuve en ninguna situación que me amenace de ningún tipo…"

Edward J. Smith, Capitán del TITANIC, entrevistado por la prensa de Nueva York, 1907

Interrogantes a responder

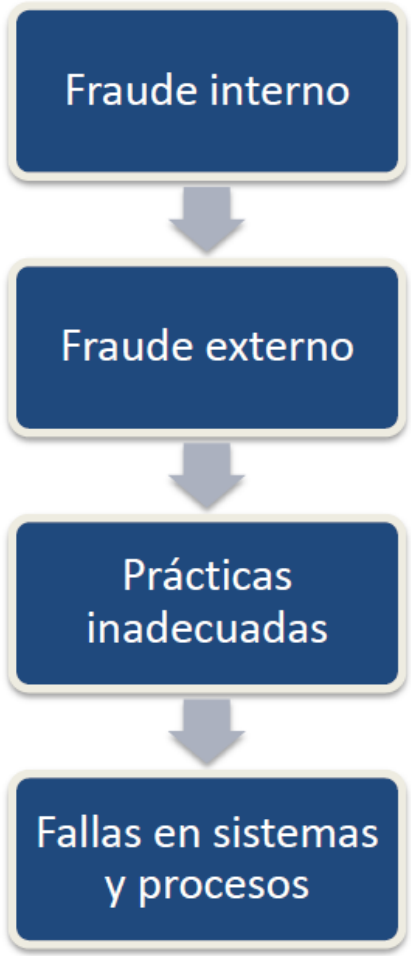
- Tenemos conciencia de nuestros riesgos?
- Tenemos apropiados procesos y controles?
- Tenemos estrategias de mitigación del riesgo?
- Estamos trabajando en un Plan de Continuidad de Negocio (BCP) ante un evento de desastre?
- Es nuestra infraestructura de tecnología segura?
- La estrategia de seguridad soporta nuestro crecimiento?
- En Nuestra institución están cumpliendo con nuestras reglas y regulaciones?
- Estamos manejando nuestra imagen?
- Está siendo efectiva nuestra función de Auditoría Interna?

Introducción al Riesgo Operativo

Riesgo operativo no solo lo que por que lo pide la normativa!

El riesgo operacional no es un riesgo reciente, de hecho ha sido uno de los primeros riesgos por el que se preocupaban las entidades financieras en ese entonces. Por lo tanto cabe preguntarse: ¿qué ha cambiado para que en los últimos años haya adquirido tanta popularidad entre los entes reguladores, las entidades financieras, los consultores y la academia?

Riesgo operativo no solo lo que por que lo pide la normativa!



CAUSAS

AÑO	ENTIDAD	IMPORTE PÉRDIDAS
1995	BARINGS BANK	USD$ 1,300
1996	SUMITOMO BANK	USD$ 2,600
1997	NATWEST BANK	USD$ 127
2001	ALLIANZ, LLOYD´S, AXA,BERKSHIRE-HATHAWAY, ETC.	USD$ 44,000
2002	ALLIED IRISH BANK	USD$ 691
2002	CITIGROUP (CASO WORLDCOM)	USD$ 9,000
2005	CASO WINDSOR	¿?

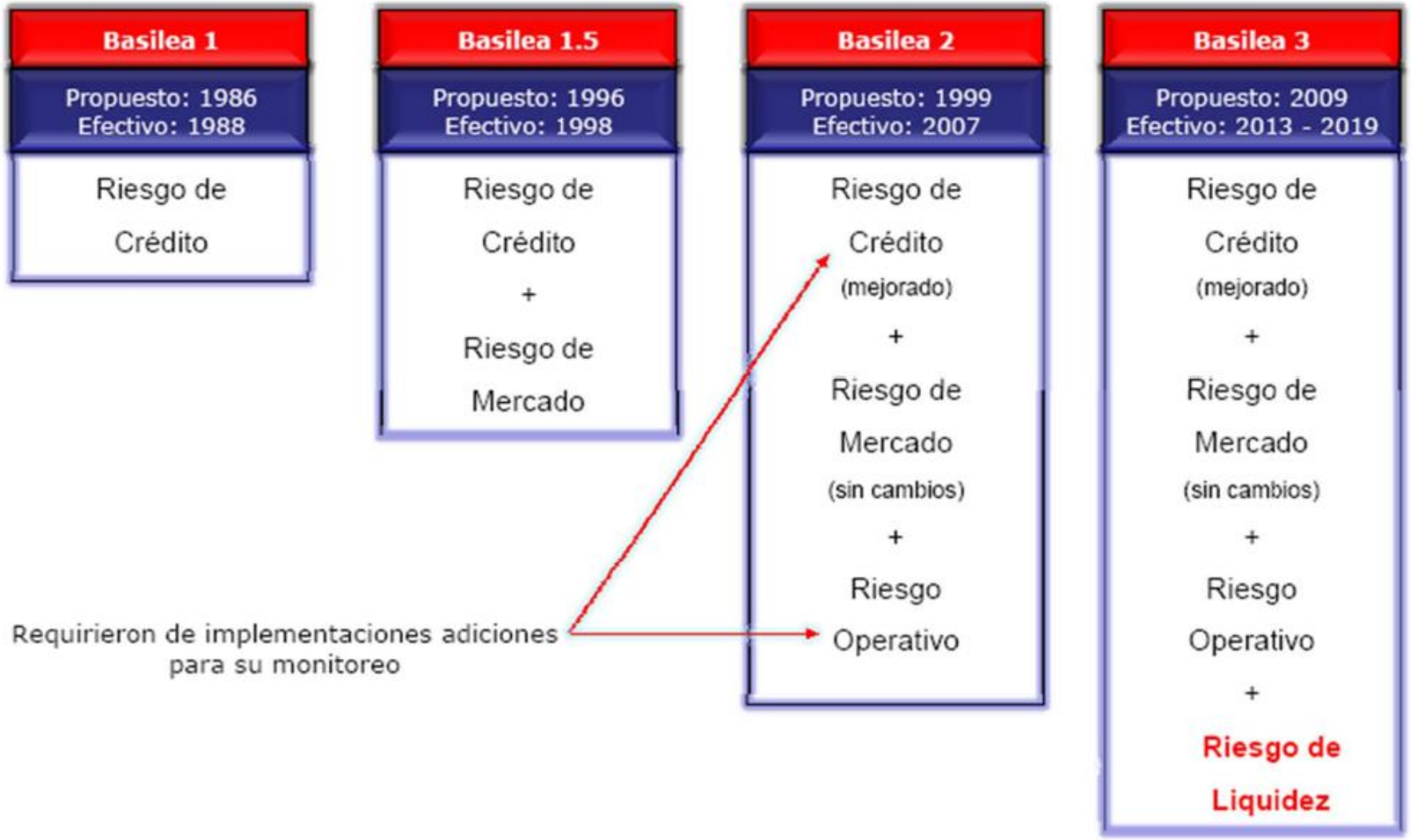
SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

FÜR ALLE Die Genossenschaften

DGRV DIE GENOSSENSCHAFTEN

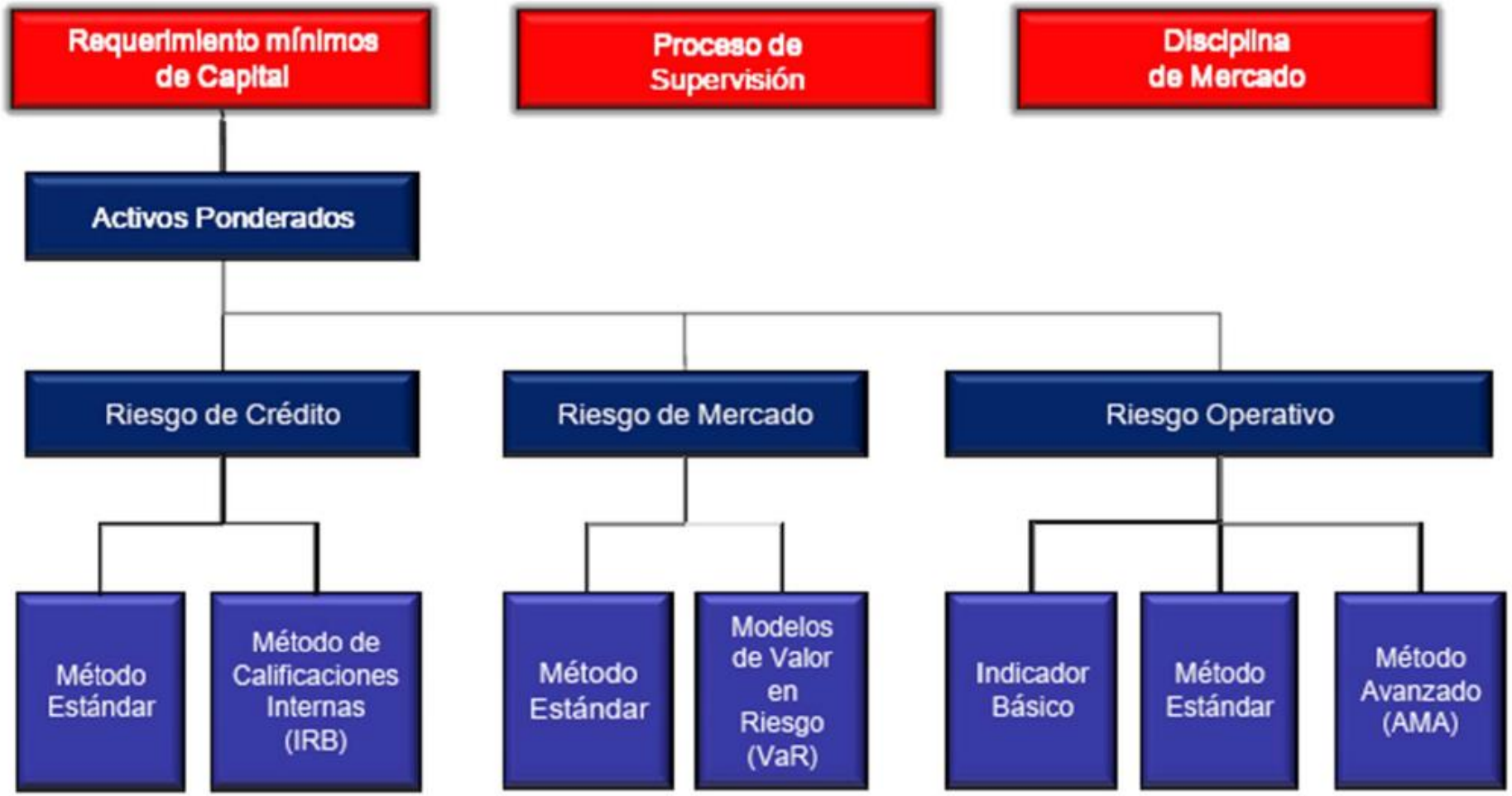
Normativa de Basilea

Evolución Acuerdos de Basilea



Normativa de Basilea

Pilares Basilea II



RECOMENDACIONES DEL COMITÉ DE BASILEA

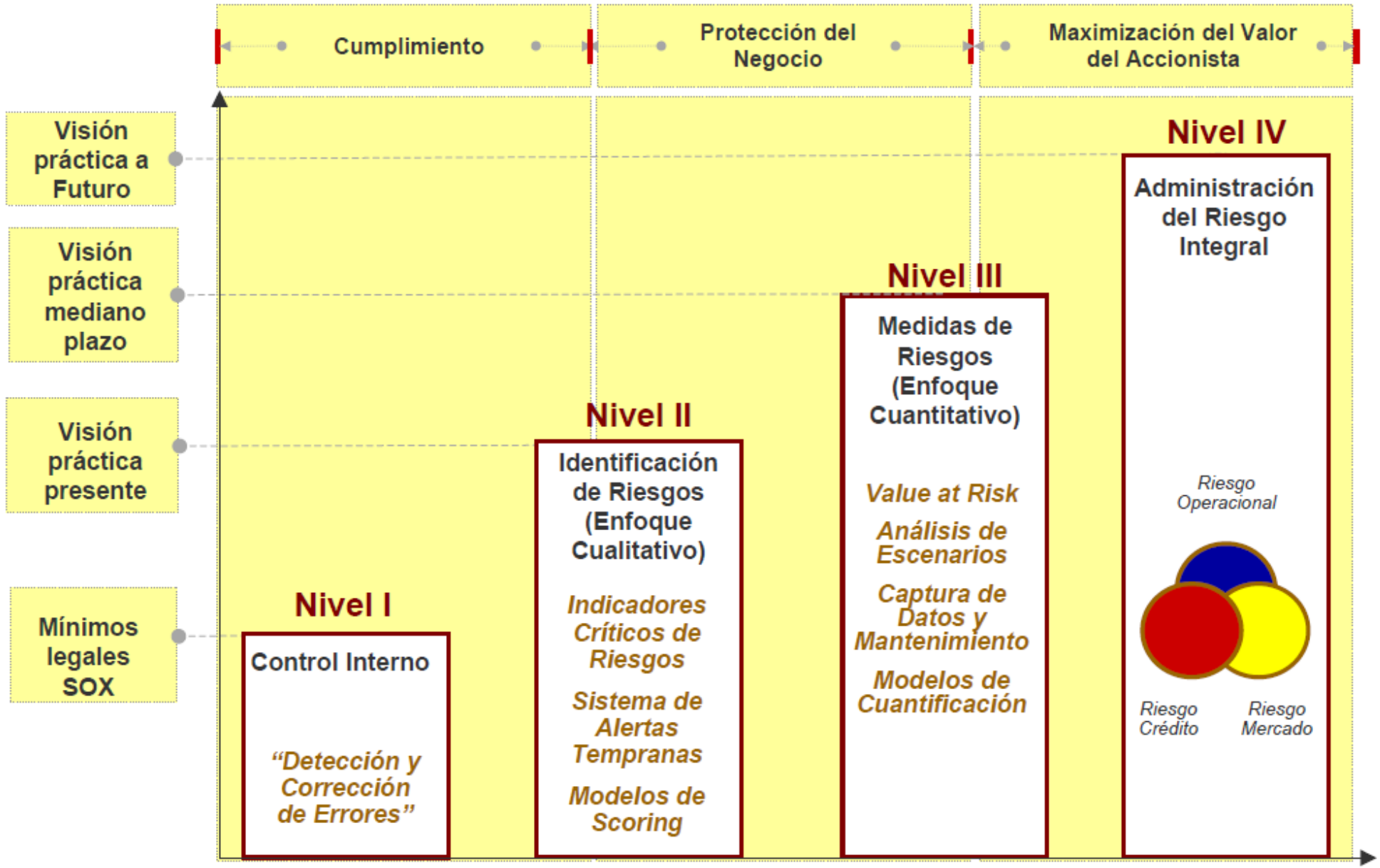
El Comité de Supervisión Bancaria de Basilea recomienda:

- **A las Instituciones:** La adopción de prácticas adecuadas para la gestión de los riesgos.

- **A los Supervisores:** La necesidad de exigir y vigilar su cumplimiento.

Para fortalecer la solidez y estabilidad de las Entidades Financieras.

Evolución de la Administración de Riesgo Operacional



Evolución de la Administración de Riesgo Operacional

Enfoque de Riesgo Operacional:

Etapa 1

Cultura

- Fase A. Concientización Importancia Del Riesgo Operacional

Etapa 2

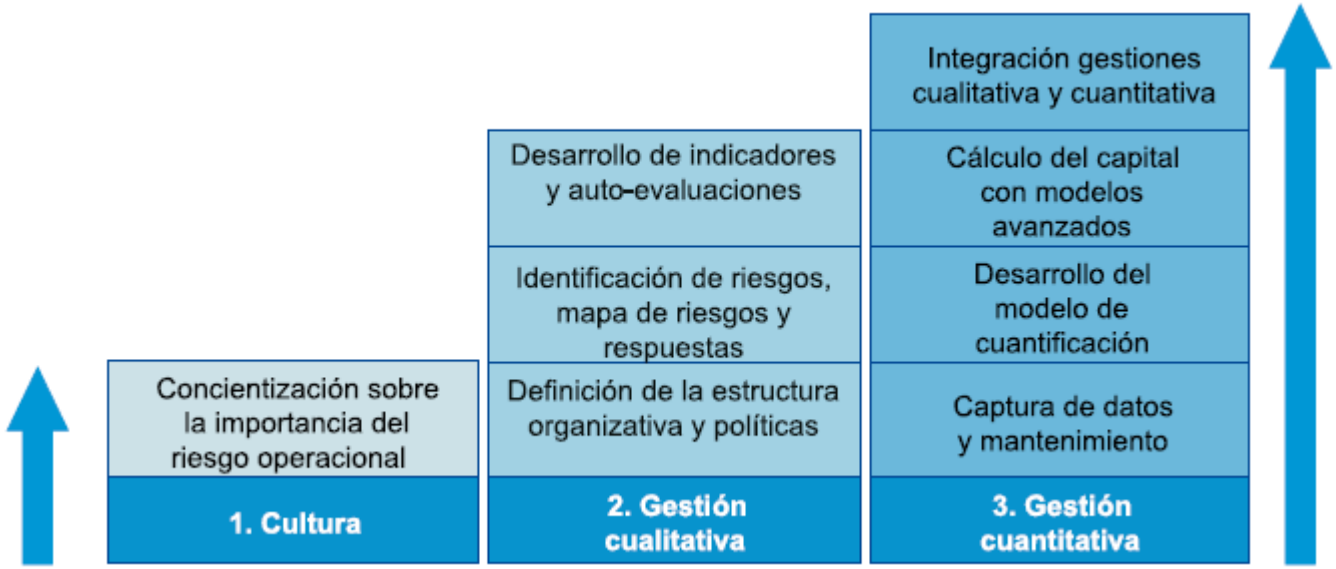
Gestión Cualitativa

- Fase B. Definición de la Estructura Organizacional, Políticas Lineamientos
- Fase C. Identificación de Riesgos, Mapa de Riesgos Controles
- Fase D. Desarrollo de Indicadores Auto-Evaluaciones

Etapa 3

Gestión Cuantitativa

- Fase E. Captura de Datos Mantenimiento
- Fase F. Desarrollo del Modelo de Cuantificación
- Fase G. Cálculo del Capital con Modelos Avanzados
- Fase H. Integración Gestiones Cualitativa Cuantitativa



Ejemplificación de un caso de riesgo operativo

- En 1988, Celia Reyes invierte en Banco Bital Usd. 27.000,oo a tasas de interés del 124% y del 149%.
- El contrato de inversión establecía que si el cliente no se acercaba al banco a cobrar su inversión, ésta se renovaba automáticamente … en las mismas condiciones.
- En 1989, la señora Celia acude al banco y cobra la totalidad de su inversión. Sin embargo, el cajero olvida retirarle los documentos.
- En 1997, la señora Celia pide al banco un pago de 42 millones de dólares!
- En 2000, una corte federal falla a favor de la señora Celia Reyes y ordena al banco que realice el pago.
- El banco nunca logró probar que efectivamente pagó en su momento a la señora Celia, pero apela ante el juez para que se revisen las condiciones de mercado en cuanto a las tasas de interés.
- El juez acepta la apelación y Banco Bital únicamente debió pagar a la señora Celia Reyes USD. 5,6 millones.

Ejemplificación de un caso de riesgo operativo…

- **Riesgo:** Pérdida por incobrabilidad de un crédito, debido a que se desembolsan operaciones con documentos habilitantes con inconsistencias (incompletos, desactualizados, con errores, tachones, enmendaduras, etc.)
- **Debilidad:** Falta de capacitación del personal del área comercial en el manejo de documentos de crédito.
- **Evento:** El 6 de agosto no se pudo recuperar la operación # 001 por $15.000 debido a que el pagaré se encontraba con tachones y enmendaduras.

Normativa en Ecuador para Cooperativas de Ahorro y Crédito

- Resolución No. SEPS-IGT-IR-IGJ-2018-0279, de 26 de noviembre de 2018: Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del Sector Financiero Popular y Solidario, bajo el control de la Superintendencia de Economía Popular y Solidaria.
- Reformada por las resoluciones Nos. SEPS-IGT-IR-IGJ-2018-0284, de 13 de diciembre de 2018; y, SEPS-IGT-IGS-INR-INGINT-2020-0221, de 2 de junio de 2020.
- El 7 de julio de 2022 se expide la Norma reformatoria a la resolución No. SEPS-IGT-IR-IGJ-2018- 0279 de 26 de noviembre de 2018, que contiene la "Norma de control para la administración del riesgo operativo y riesgo legal en las entidades del sector financiero popular y solidario bajo el control de la Superintendencia de Economía Popular y Solidaria"

Generalidades

- **Riesgo:** Es la posibilidad de que se produzca el evento que genere pérdidas con un determinado nivel de impacto para la entidad.

- **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.

  El riesgo operativo no incluye los originados por el entorno político, económico y social, los riesgos sistémico, estratégico y de reputación.

Generalidades

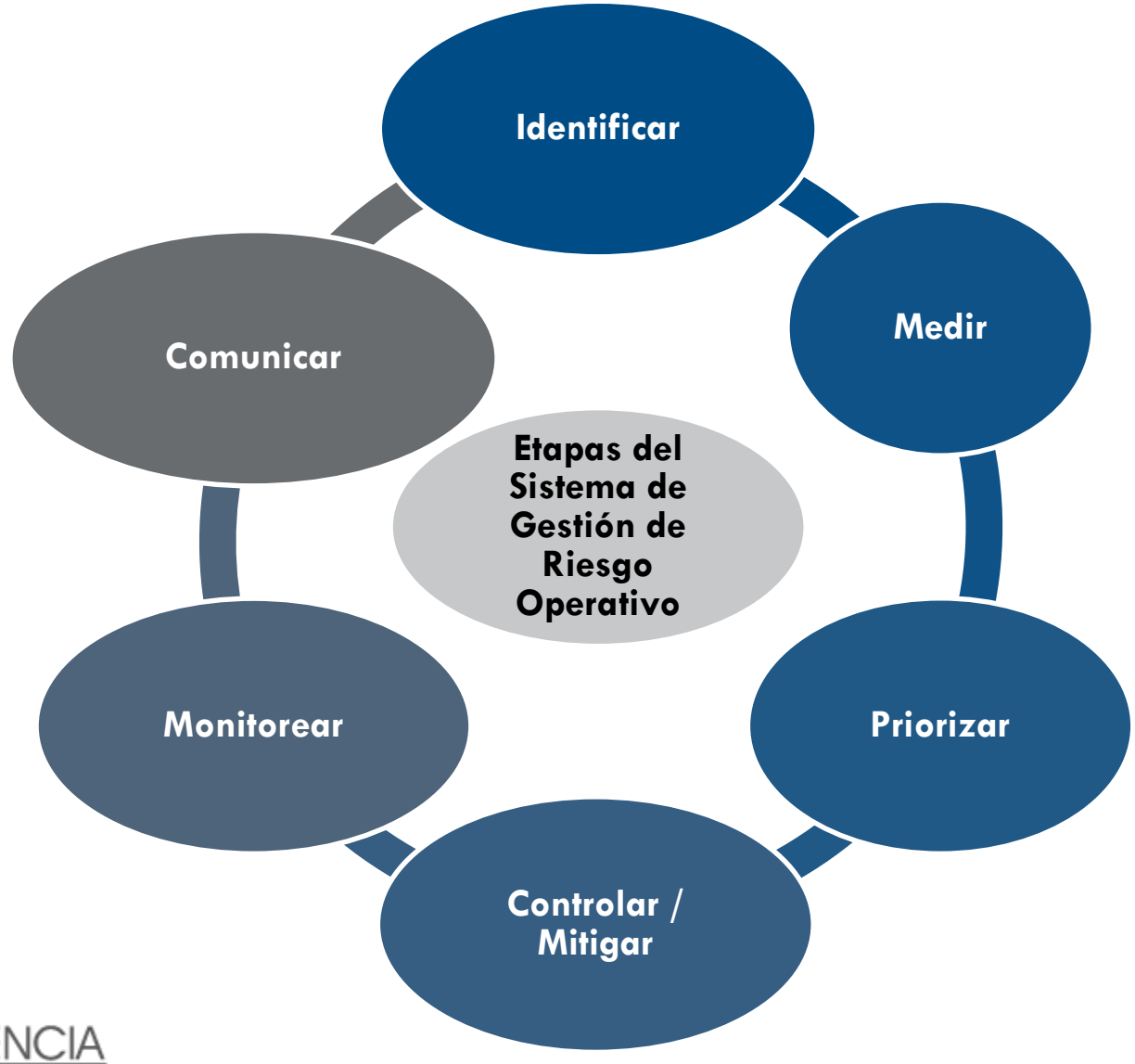
- **Debilidad**: Es la falencia evidenciada en el proceso y que esta asociada a la causa u origen de riesgo (factores: personas, procesos, TI, Eventos Externos).

- **Evento de riesgo.-** Es un hecho que podría generar pérdidas para la entidad.

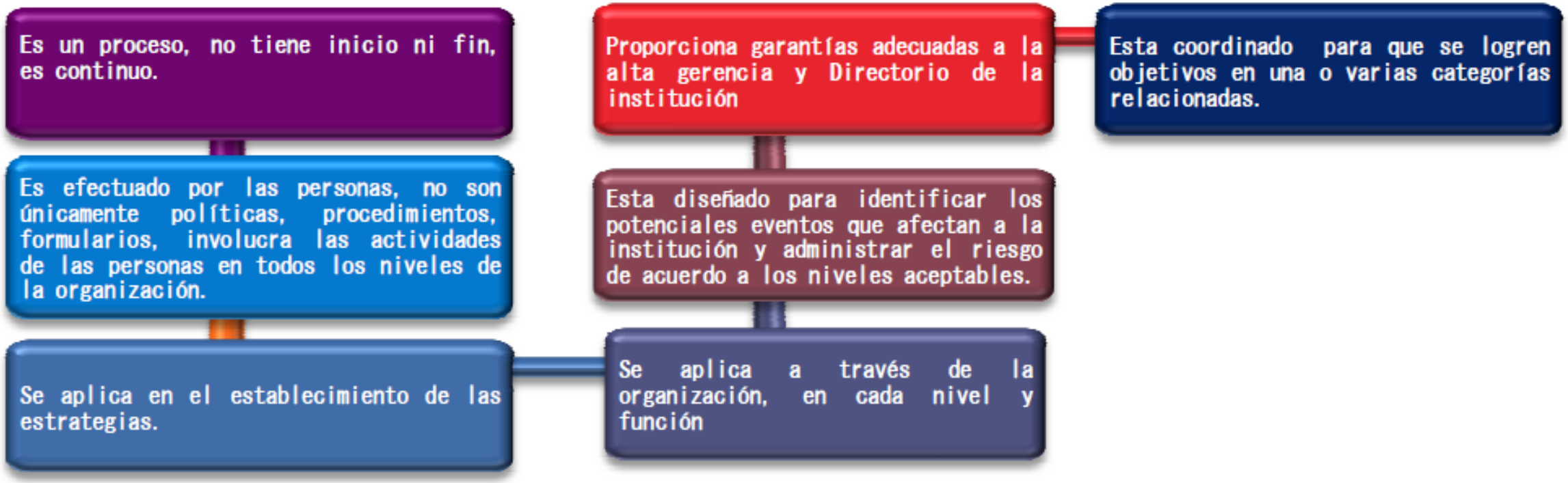
Sistema de Gestión de Riesgo Operativo

- **Sistema de Gestión de Riesgo Operativo**: Para una adecuada administración de riesgo operativo y legal, las entidades y la Corporación deberán implementar un Sistema de Gestión del Riesgo Operativo (SIGRO) que corresponde al conjunto de etapas y elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las entidades identifican, miden, priorizan, controlan/mitigan, monitorean y comunican dicho riesgo.

Etapas del Sistema de Gestión de Riesgo Operativo

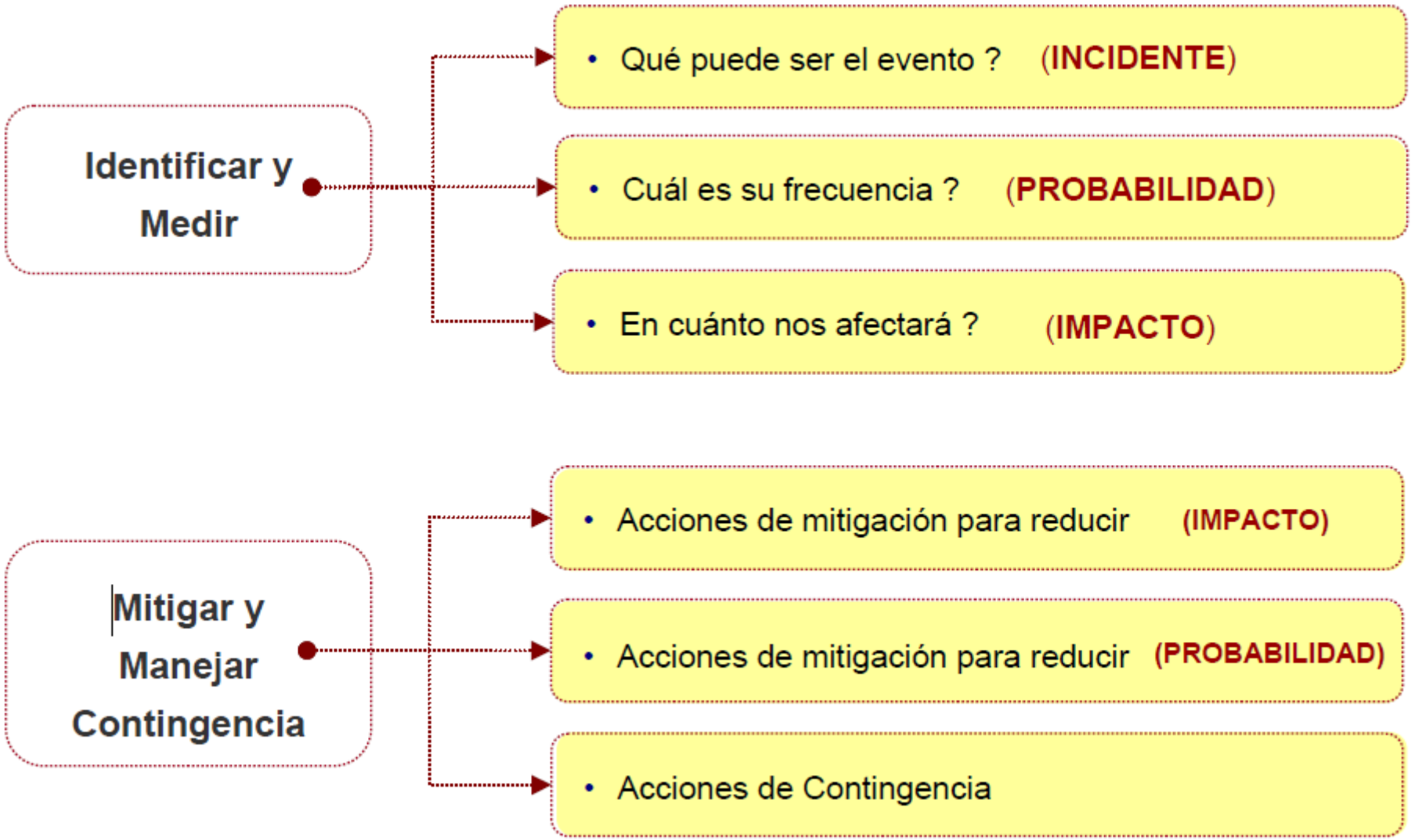


Etapas del Sistema de Gestión de Riesgo Operativo



Fuente: Enterprise Risk Management Framework - Executive Summary
Committee of Sponsoring Organizations of the Treadway Commission

Identificar, Medir y Administrar el Riesgo Operacional



Etapas del Sistema de Gestión de Riesgo Operativo

Etapas del Sistema de Gestión de Riesgo Operativo

- **Identificar**: Debe realizarse con anterioridad a la ejecución de cualquier proceso, con el fin de determinar los riesgos operativos que han ocurrido, así como aquellos riesgos operativos en potencia que van a suponer una serie de obstáculos al logro de los objetivos definidos.
- En esta etapa de identificación pueden a su vez diferenciarse dos sub-etapas:
  - Inventario de procedimientos
  - Recolección de información

Etapas del Sistema de Gestión de Riesgo Operativo

- **Medir:** Una vez que los riesgos operativos de los diferentes procesos han sido identificados, el siguiente paso es evaluar la posibilidad de materialización de los mismos (en función de la frecuencia con la que los mismos suceden) así como, definir el impacto que los mismos podrían generar en caso de ocurrencia.
- Como resultado de esta segunda etapa, establecemos el llamado riesgo inherente, que no es más que el nivel de riesgos que presenta una actividad concreta, sin aplicarle ningún tipo de control.

Etapas del Sistema de Gestión de Riesgo Operativo

- **Priorizar:** Los resultados de la matriz de probabilidad e impacto, permiten identificar aquellos riesgos que representan una mayor amenaza, a los cuales se les puede dar mayor prioridad o gestión de respuesta, con los recursos de los que dispone la entidad

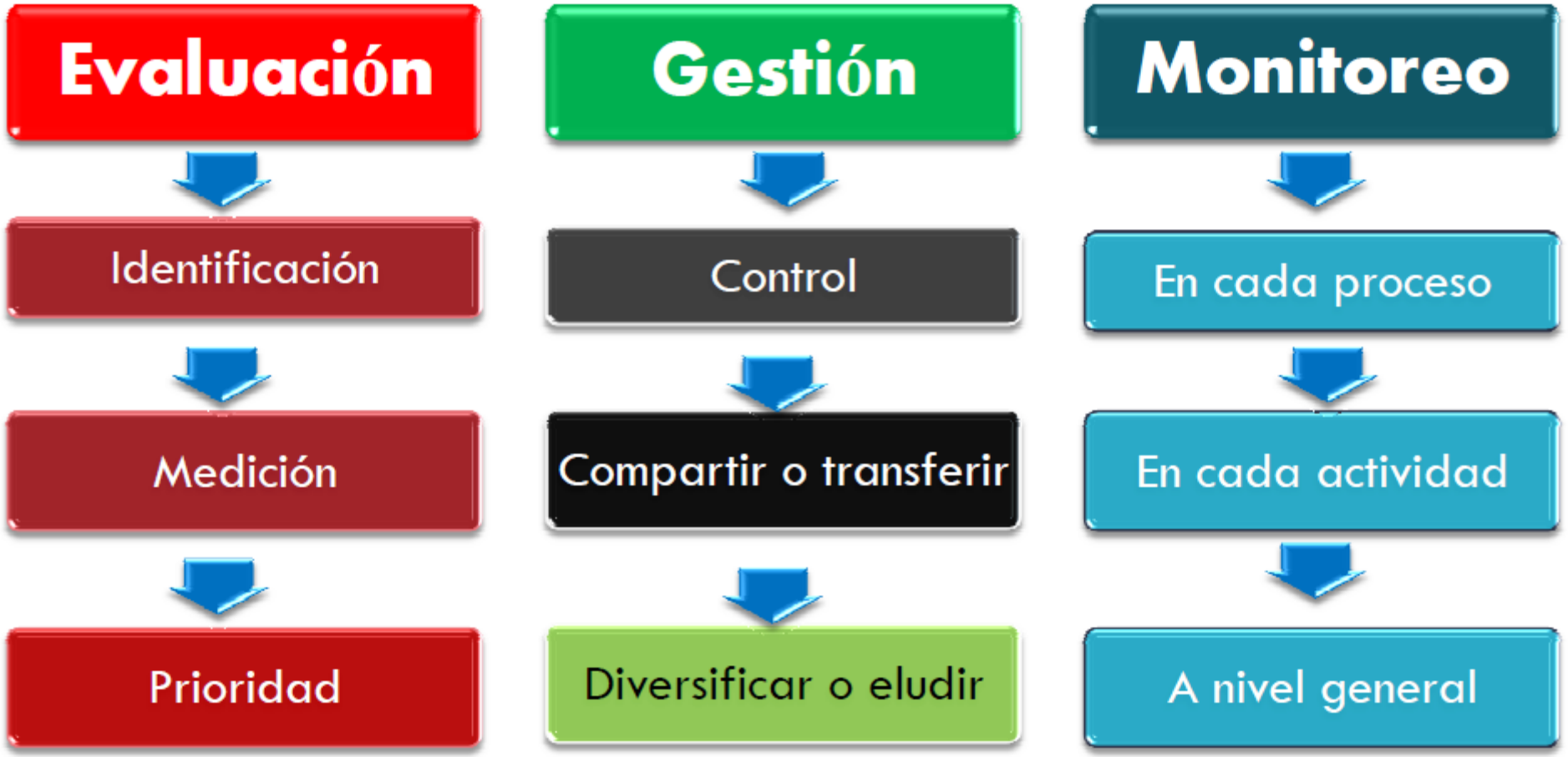
Etapas del Sistema de Gestión de Riesgo Operativo

- **Controlar/mitigar:** En esta etapa se busca definir las medidas de control que permitan reducir la probabilidad de ocurrencia y/o impactos ocasionados por los riesgos inherentes detectados.
- Tras esta etapa, la entidad obtiene el conocido riesgo residual, que es el riesgo que resulta tras la aplicación de los oportunos controles que hayan sido considerados por la entidad.

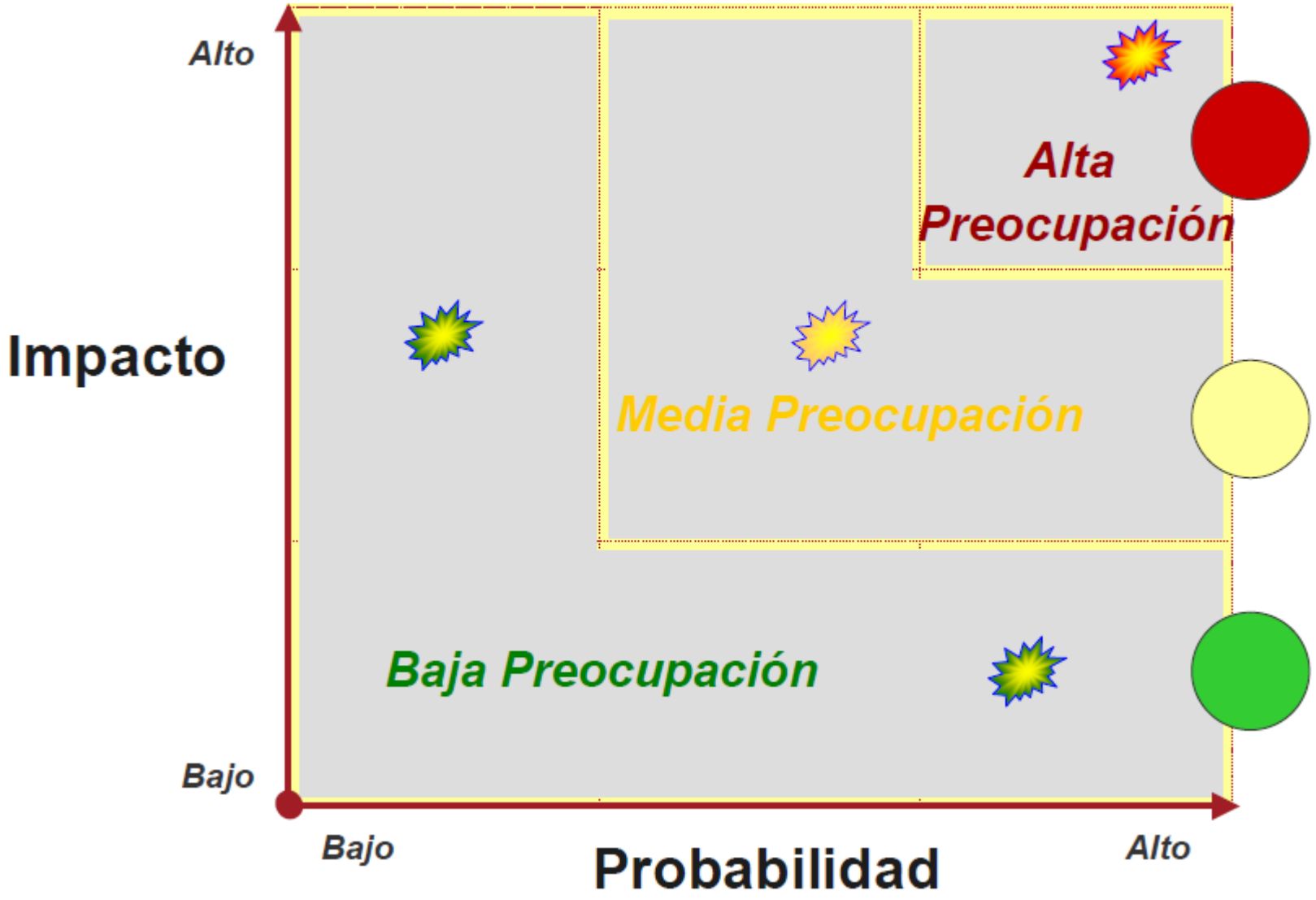
Etapas del Sistema de Gestión de Riesgo Operativo

- **Monitorear:** En esta etapa se debe llevar a cabo el seguimiento adecuado a los riesgos con el fin de ir analizando su evolución.
- **Comunicar:** Las entidades deben definir una política sobre los eventos de riesgo operativo que deban informar interna o externamente y que esté sujeta a revisión periódica, en función de las estrategias organizacionales. Además, deben implementar un proceso para evaluar el impacto de la información a comunicar en función a su gestión de riesgos.

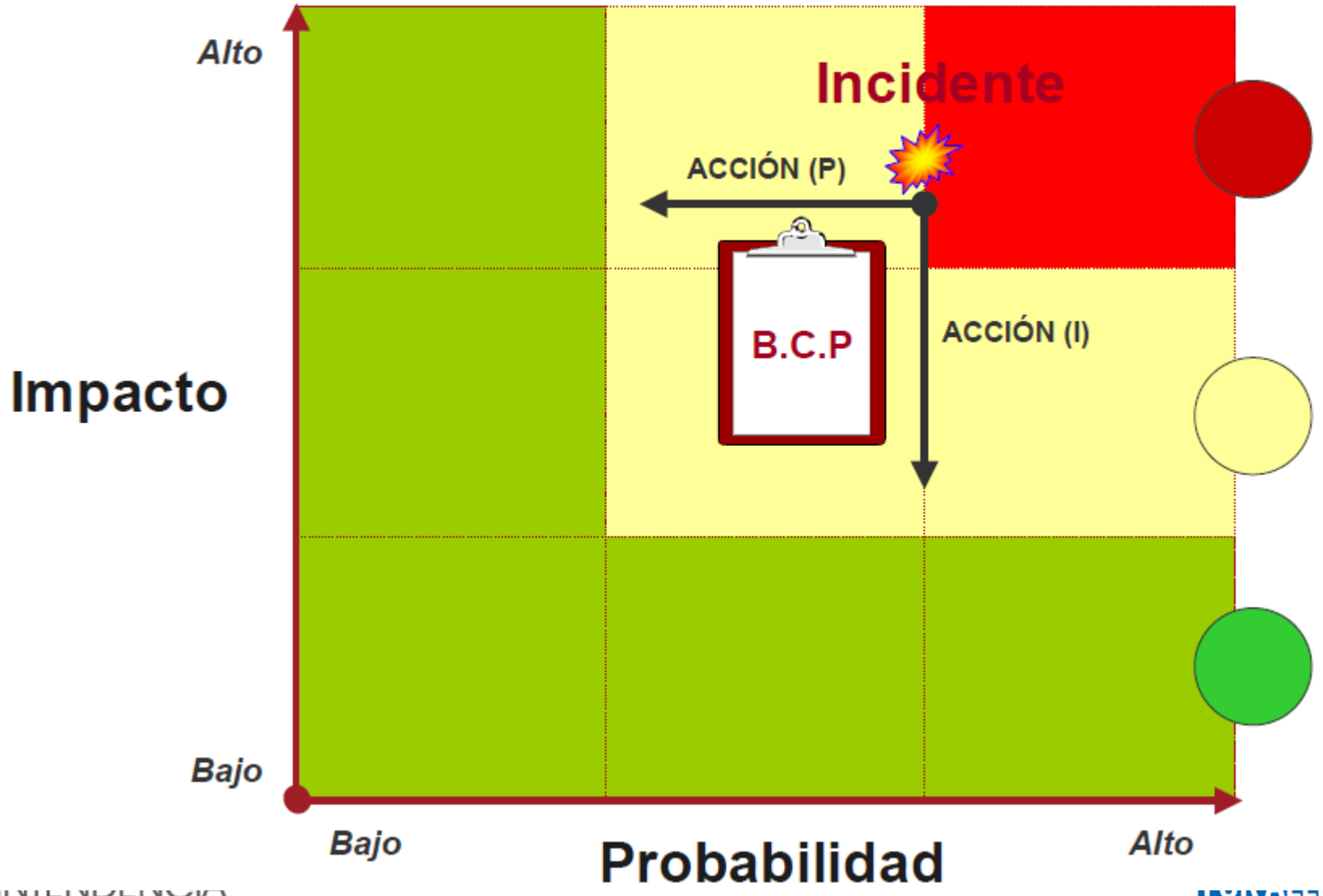
Etapas del Sistema de Gestión de Riesgo Operativo



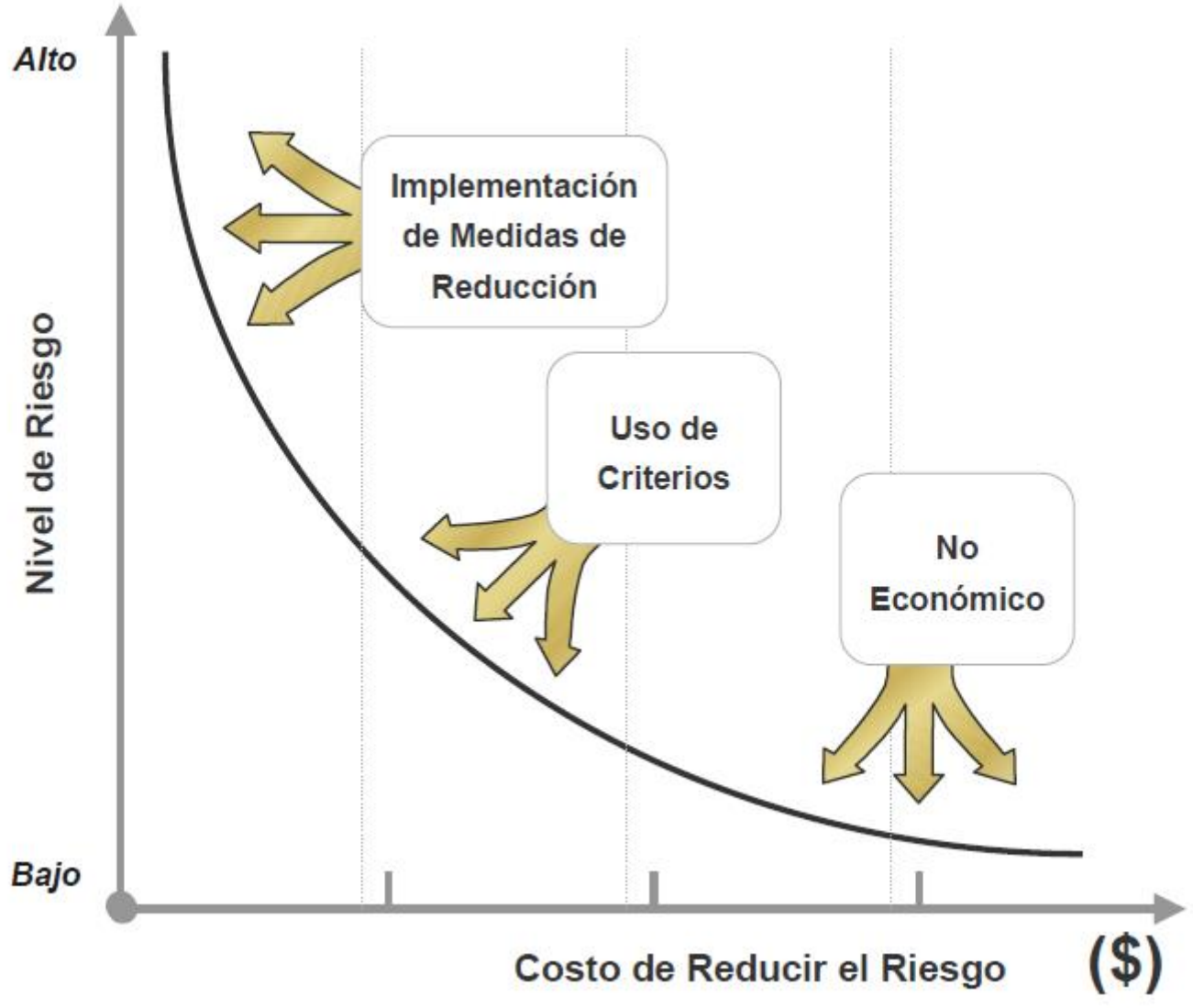
Mapa de Riesgo Operacional - Identificación y Medida de los Eventos



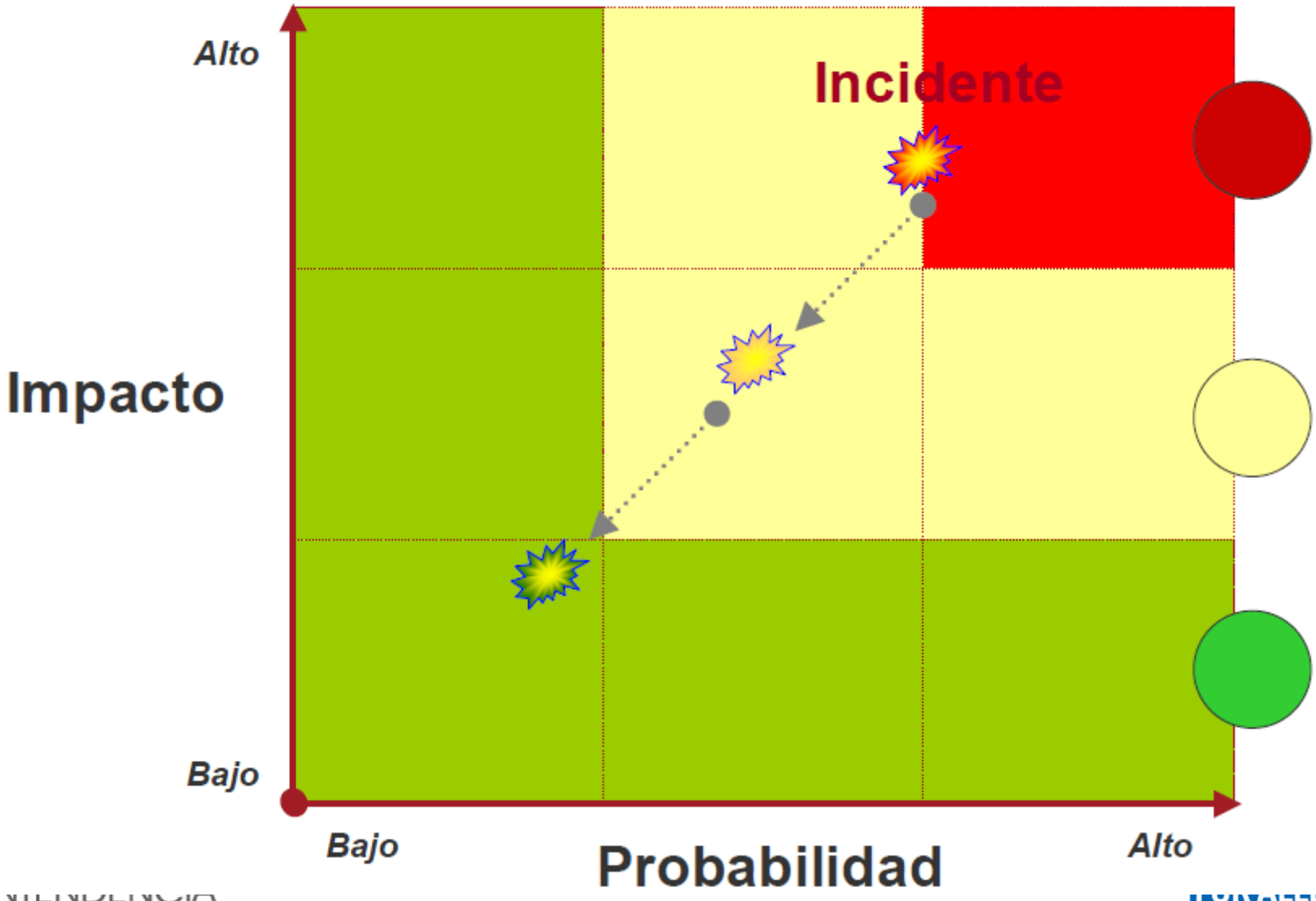
Mapa de Riesgo Operacional – Estrategia de Respuesta al Riesgo



Mapa de Riesgo Operacional - Análisis Costo versus Beneficio a los Riesgos



Mapa de Riesgo Operacional – Plan de Mitigación de los Riesgos



Etapas del Sistema de Gestión de Riesgo Operativo

Unidades Negocios/ Soporte

- (A) Evaluación periódica de riesgos
- (B) Estandarización de controles
- (C) Aplicación de controles
- (D) Análisis operacional de nuevos productos o procesos de negocios
- (E) Relaciones con clientes

Unidad de Riesgos y Riesgo Operacional

- (A) Desarrollo de la Gestión de Riesgos
- (B) Generación de Reportes de Riesgos
- (C) Facilitador
- (D) Coordinación y trabajo en conjunto con Auditoría Interna

Etapas del Sistema de Gestión de Riesgo Operativo

INFORME ANÁLISIS DE RIESGOS

FECHA ELABORACIÓN	08 octubre de 2020
VERSIÓN	1.0

ELABORADO		Administrador de Riesgos	
REVISADO		Comité de Administración Integral de Riesgos	

APROBACIÓN	El documento fue aprobado por los integrantes del Consejo de Administración en sesión del _____ según consta en acta #	PRESIDENTE SECRETARIA

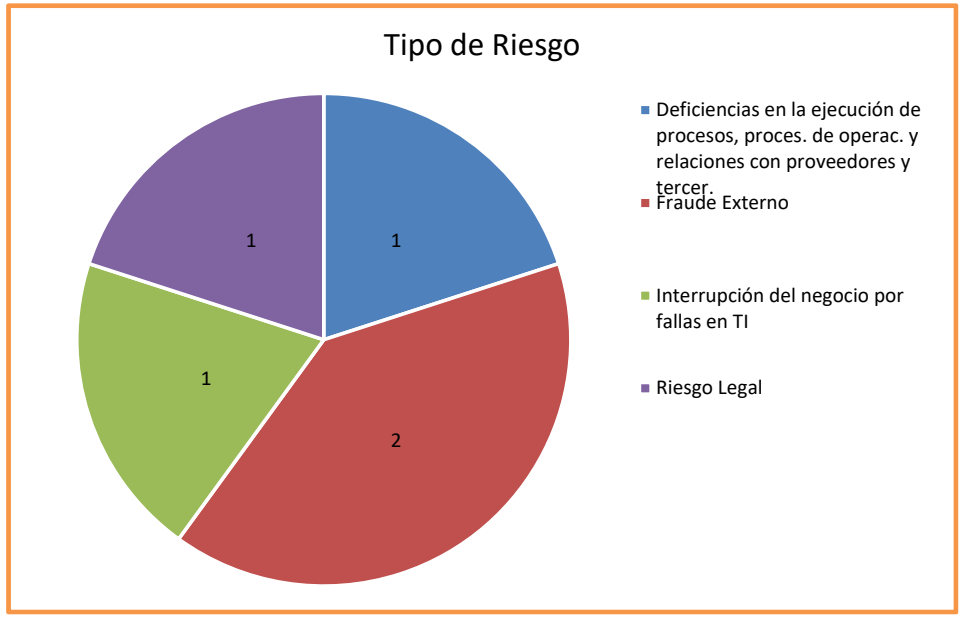
La información contenida en este documento es confidencial y de propiedad de la Cooperativa.

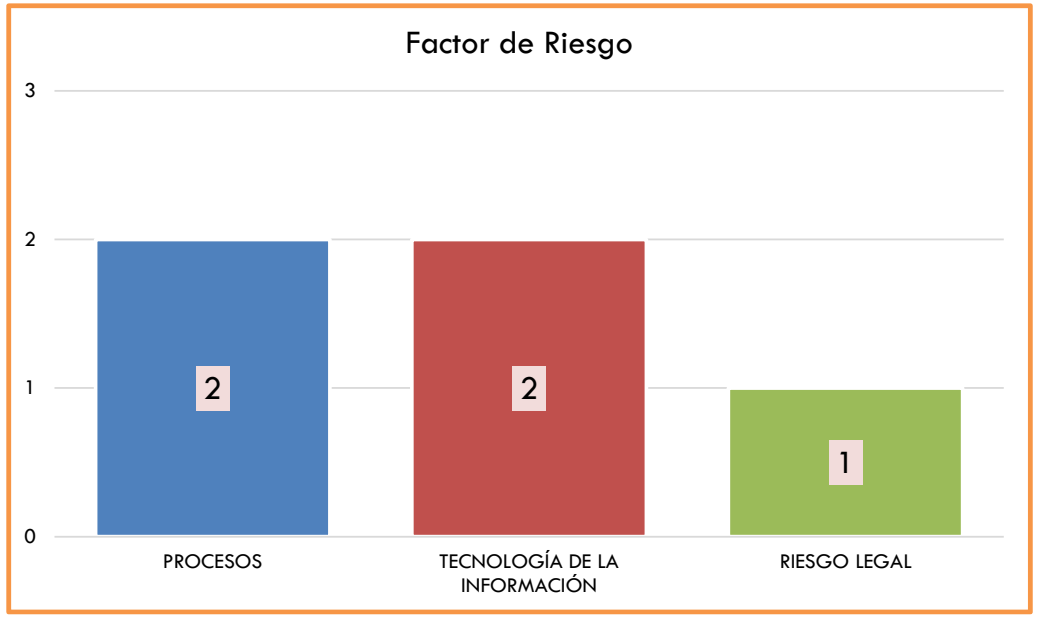
SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

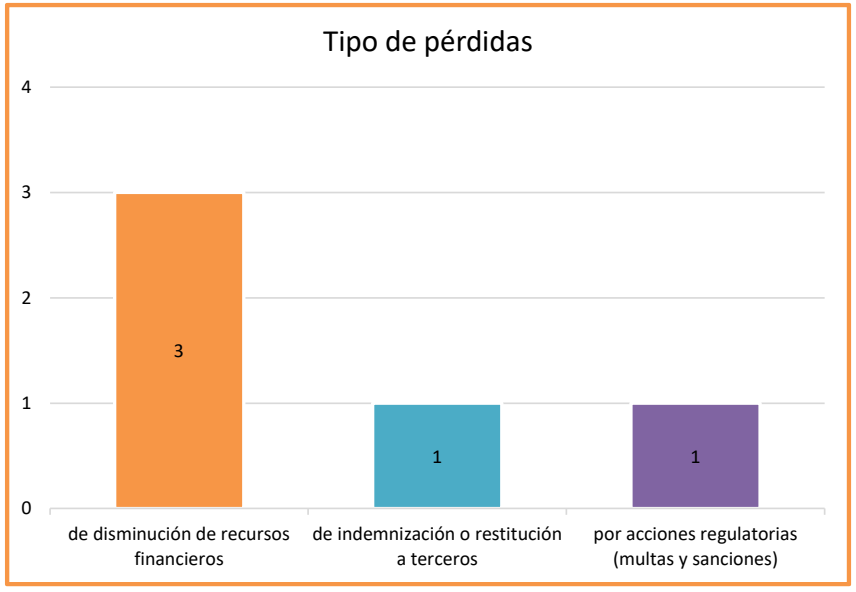
EIN GEWINN FÜR ALLE Die Genossenschaften

DGRV DIE GENOSSENSCHAFTEN

Etapas del Sistema de Gestión de Riesgo Operativo







SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

EIN GEWINN FÜR ALLE Die Genossenschaften

DGRV DIE GENOSSENSCHAFTEN

Factores Críticos de Éxitos ...

1. Ser lo más simple posible
2. Soporte claro desde arriba hacia abajo
3. Establecer un lenguaje común
4. Operar con el concepto de dueño de riesgo.
5. Convencimiento del nivel gerencial del esquema de Administración de Riesgo Operacional
6. Creación de cultura que permita la identificación, reportes y corrección de aspectos de Riesgo Operacional.
7. Mantener una visión de Administración de Riesgo Operacional
8. Establecer Roles en la Administración de Riesgo Operacional
9. Establecer un proceso uniforme de Administración de Riesgo Operacional
10. Establecer un proceso de reportes de Riesgo Operacional

Líneas de Negocio

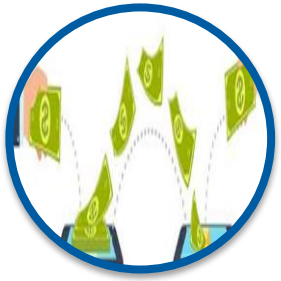
Línea minorista

Línea de microfinanzas

Línea de tarjetas

Línea comercial

Línea inmobiliaria



Línea de compensación de pago

Línea de tesorería tradicional

Líneas de Negocio

Para una adecuada administración del riesgo operativo las entidades y la Corporación, deberán agrupar justificada y documentadamente sus procesos por líneas de negocio de acuerdo a la siguiente clasificación:

Línea minorista.- Contempla las actividades de intermediación financiera tales como: recepción de depósitos en cualquier modalidad; asesoramiento de inversiones; otorgamiento de créditos en las modalidades de consumo y vivienda.

Este grupo incluye, servicios financieros, negociación de letras de cambio, libranzas, pagarés, facturas y otros documentos que representen obligación de pago creados por ventas a crédito, así como el anticipo de fondos con respaldo de los documentos referidos.

No incluye las operaciones y servicios relacionados con tarjetas de crédito, débito, pago y prepago.

Líneas de Negocio

Línea de microfinanzas.- Incluye operaciones financieras como préstamos en el segmento de microcrédito, ahorro o transferencias a personas naturales cuyo sustento provenga de actividades económicas de menor escala.

Línea de tarjetas.- Contempla las actividades y servicios relacionados con tarjetas de crédito, débito, pago y prepago.

Línea Comercial.- Incluye las operaciones de crédito comercial de primer piso, operaciones financieras de segundo piso con cooperativas de ahorro y crédito y asociaciones mutualistas de ahorro y crédito para la vivienda.

Líneas de Negocio

Línea de compensación de pagos.- Contempla todas las actividades relacionadas con la gestión de pagos, transferencias y compensación de acuerdo a lo establecido en el artículo 470 del Código Orgánico Monetario y Financiero.

Línea de tesorería tradicional.- Representan actividades cotidianas de la gestión de liquidez y administración de flujo de fondos.

Líneas de Negocio

Los procesos productivos deberán asignarse a las líneas de negocio de acuerdo con los productos y servicios que generan, de forma que a cada uno de los procesos les corresponda una sola línea de negocio y que ningún proceso permanezca sin asignar.

Las líneas de negocio también deberán agrupar los procesos gobernantes y los procesos habilitantes que intervienen en las mismas. Si algún proceso gobernante o proceso habilitante interviene en más de una línea de negocio, la entidad deberá utilizar un criterio de asignación objetivo, considerando su línea de negocio principal

Mapc

Tabla 5-A: Líneas de Negocios, definición y mapeo, según Basilea II.

Nivel 1	Definición General	Nivel 2	Grupos de Actividades (Nivel 3)
Finanzas empresariales o corporativas	acuerdos bancarios que se proporcionan a las grandes compañías comerciales, compañías multinacionales, instituciones financieras no bancarias, departamentos del gobiemos, entre otras.	Finanzas Corporativas	Fusiones y adquisiciones, suscripción de emisiones, privatizaciones, titulización, servicio de estudios, deuda (pública, alto rendimiento), acciones, sindicaciones, Ofertas Públicas Iniciales, colocaciones privadas en mercados secundarios.
		Finanzas Municipales y de Gobiemo	
		Banca de inversión	
		Servicios de asesoramiento	
Negociación y ventas	operaciones de tesorería, compra y venta de valores, divisas y materias primas por cuenta propia y de clientes.	Ventas	Renta fija, renta variable, divisas, productos básicos, crédito, financiación, posiciones propias en valores, préstamo y operaciones con pacto de recompra, intermediación, deuda, intermediación unificada (prime brokerage)
		Generación de Mercado	
		Posiciones Propietarias	
		Tesorería	
Pagos y liquidación	actividades relacionadas con pagos y cobros, transferencias interbancarias de fondos, compensación y liquidación.	Clientes Externos	Pagos y recaudaciones, transferencia de fondos, compensación y liquidación (Las pérdidas derivadas de las operaciones de pago y liquidación relacionadas con las actividades propias del banco se incorporarán al historial de pérdidas de la línea de negocios afectada.)
Servicios de agencia	funcionando como agentes de emisión y pago a empresas clientes, proporcionando servicios de custodia, entre otros.	Custodia	Contratos de plica, certificados de depósito, operaciones de sociedades (clientes) para préstamo de valores
		Agencia a Empresas	Agentes de emisiones y pagos
		Fideicomisos a Empresas	-
Administración de activos	administración de fondos de clientes de manera conjunta, separada, minorista, institucional, abierta o cerrada según el mandatario.	Administración discrecional de fondos	Agrupados, segregados, minoristas, institucionales, cerrados, abiertos, participaciones accionariales
		Administración no discrecional de fondos	Agrupados, segregados, minoristas, institucionales, de capital fijo, de capital variable
Intermediación minorista	servicios de intermediación que se ofrecen a clientes que son inversores minoristas, más que inversionistas institucionales.	Intermediación minorista	Ejecución y servicio completo
Banca minorista	acuerdos de financiación para clientes particulares, clientes minoristas y pequeñas compañías (tales como prestamos, tarjetas de crédito, etc.), así como de otras facilidades, como fidecomisos y patrimonios, y asesoramiento sobre inversiones.	Banca Minorista	Préstamos y depósitos de clientes minoristas, servicios bancarios, fideicomisos y testamentarías
		Banca Privada	Préstamos y depósitos de particulares, servicios bancarios, fideicomisos y testamentarías, y asesoramiento de inversión
		Servicios de Tarjetas	Tarjetas de empresa / comerciales, de marca privada y minoristas
Banca comercial	acuerdos de financiación para compañías comerciales, incluida la financiación de proyectos, propiedades inmobiliarias, comercio exterior, factoring, leasing, garantías, letras de cambio, etc.	Banca Comercial	Financiación de proyectos, bienes raíces, financiación de exportaciones, financiación comercial, factoring, arrendamiento financiero, préstamo, garantías, letras de cambio

Fuente: BCBS (2006a) y "Basel II - Operational Risk - BIA & SA", FSI, (http://www.fsiconnect.org).

Factores de Riesgo Operativo

RIESGO OPERATIVO

El riesgo operativo es la **posibilidad** de que se produzcan **pérdidas económicas** para la Cooperativa, **debido a fallas o debilidades** originadas por factores en: procesos, personas, tecnología de información o eventos externos.

PROCESOS

PERSONAS

TECNOLOGÍA DE INFORMACIÓN

EVENTOS EXTERNOS

No incluye entorno político, económico y social, riesgo sistémico, estratégico y de reputación

EIN GEWINN FÜR ALLE Die Genossenschaften

DGRV DIE GENOSSENSCHAFTEN

PROCESOS

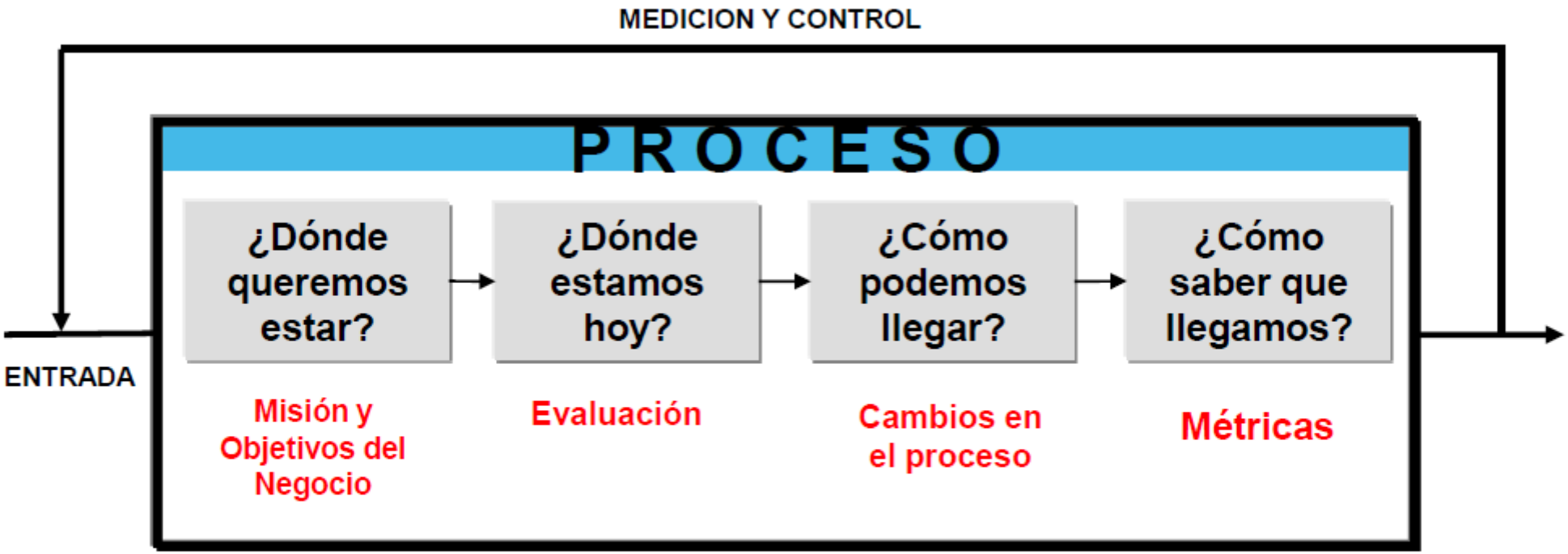
- **Procesos gobernantes o estratégicos. -** Se considerarán a aquellos que proporcionan directrices a los demás procesos y son realizados por el directorio u organismo que haga sus veces y por la alta gerencia para poder cumplir con los objetivos y políticas institucionales. Se refieren a la planificación estratégica, los lineamientos de acción básicos, la estructura organizacional, la administración integral de riesgos, entre otros;

- **Procesos productivos, fundamentales u operativos. -** Son los procesos esenciales de la entidad destinados a llevar a cabo las actividades que permitan ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus socios, clientes o usuarios.

- **Procesos habilitantes, de soporte o apoyo. -** Son aquellos que apoyan a los procesos gobernantes y productivos, se encargan de proporcionar personal competente, reducir los riesgos del trabajo, preservar la calidad de los materiales,

PROCESOS

Serie de actividades relacionadas lógicamente para definir un objetivo



Actividad					
Procedimientos					
Rol					

PROCESOS

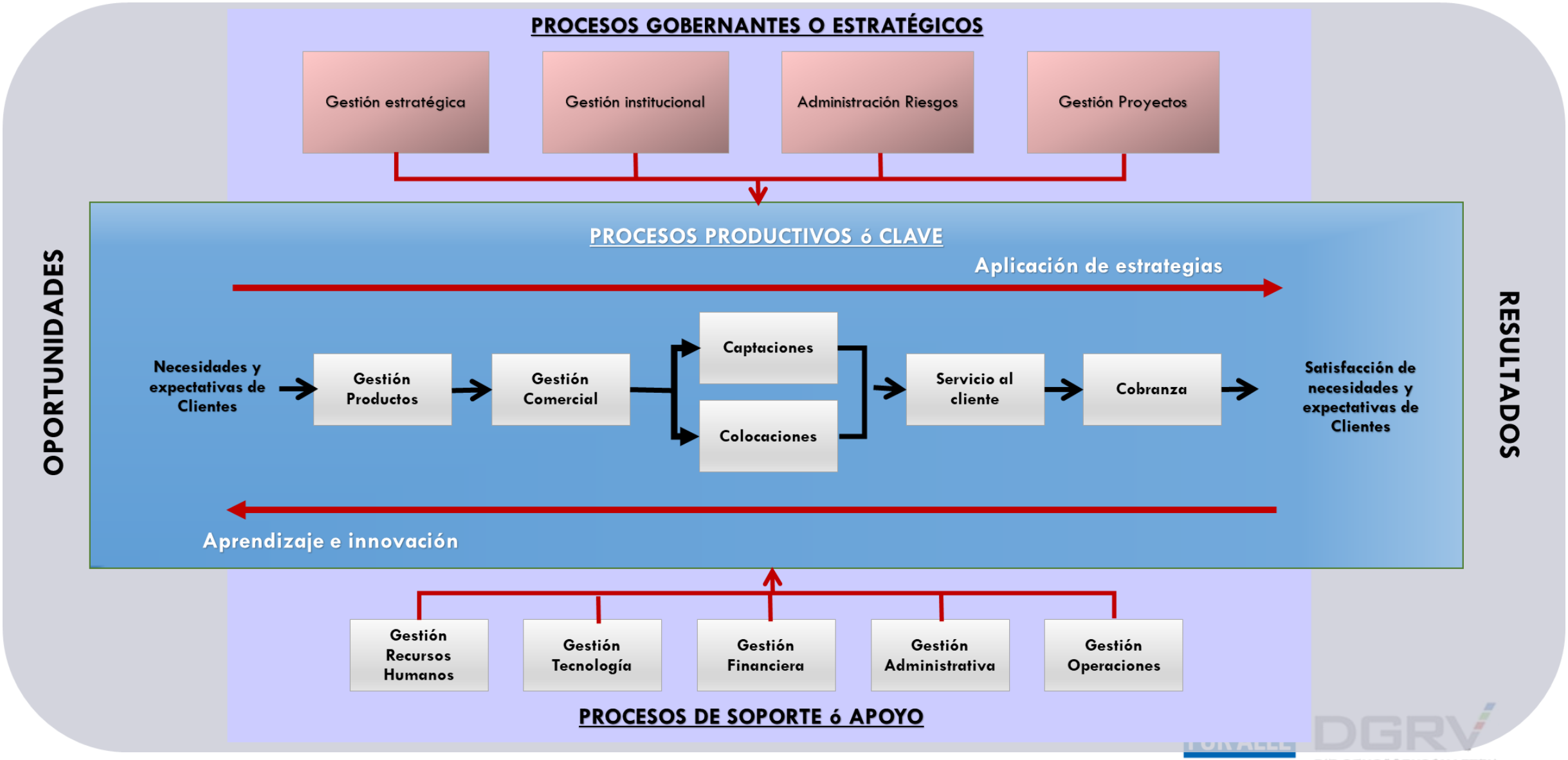
IMPORTANCIA

- Una organización es una cadena de procesos.
- Todos estamos involucrados en algún proceso.
- Permiten mejorar la productividad.

RESPONSABLE DEL PROCESO

- Es el responsable último de mejorar un proceso.
- Debe distribuir y evaluar periódicamente el trabajo entre los participantes del proceso y establecer puntos de control, productos y servicios, clientes internos y externos.
- Identifica y ejecuta los cambios requeridos para satisfacer las necesidades tanto de la organización como de los clientes.
- Comunica el proceso entre los participantes y lo debe difundir en la institución.

PROCESOS



PERSONAS

INCORPORACIÓN

- Planificación de necesidades.
- Reclutamiento.
- Selección de personal.
- Contratación.
- Inducción.

PERMANENCIA

- Condiciones laborales idóneas.
- Capacitación y formación.
- Sistemas de evaluación del desempeño.
- Planes de carrera.
- Rendición de cuentas e incentivos.
- Personal de reemplazo

DESVINCULACIÓN

- Planificación de la salida del personal.
- Preparación de aspectos jurídicos para llegar al finiquito y finalización de la relación laboral.

PERSONAS

Acuerdo de confidencialidad: Las entidades y la Corporación deben asegurar que se mantengan actualizados los acuerdos de confidencialidad relacionados con los procesos que ejecuta el empleado y los riesgos asociados a las funciones que desempeña, así mismo, debe determinar responsabilidades y deberes de seguridad de la información que permanezcan vigentes después del cambio de funciones o de la terminación de la relación laboral, conforme lo establecido en dicho acuerdo

TECNOLOGÍA DE INFORMACIÓN (TI)

TECNOLOGÍA DE INFORMACIÓN (TI)

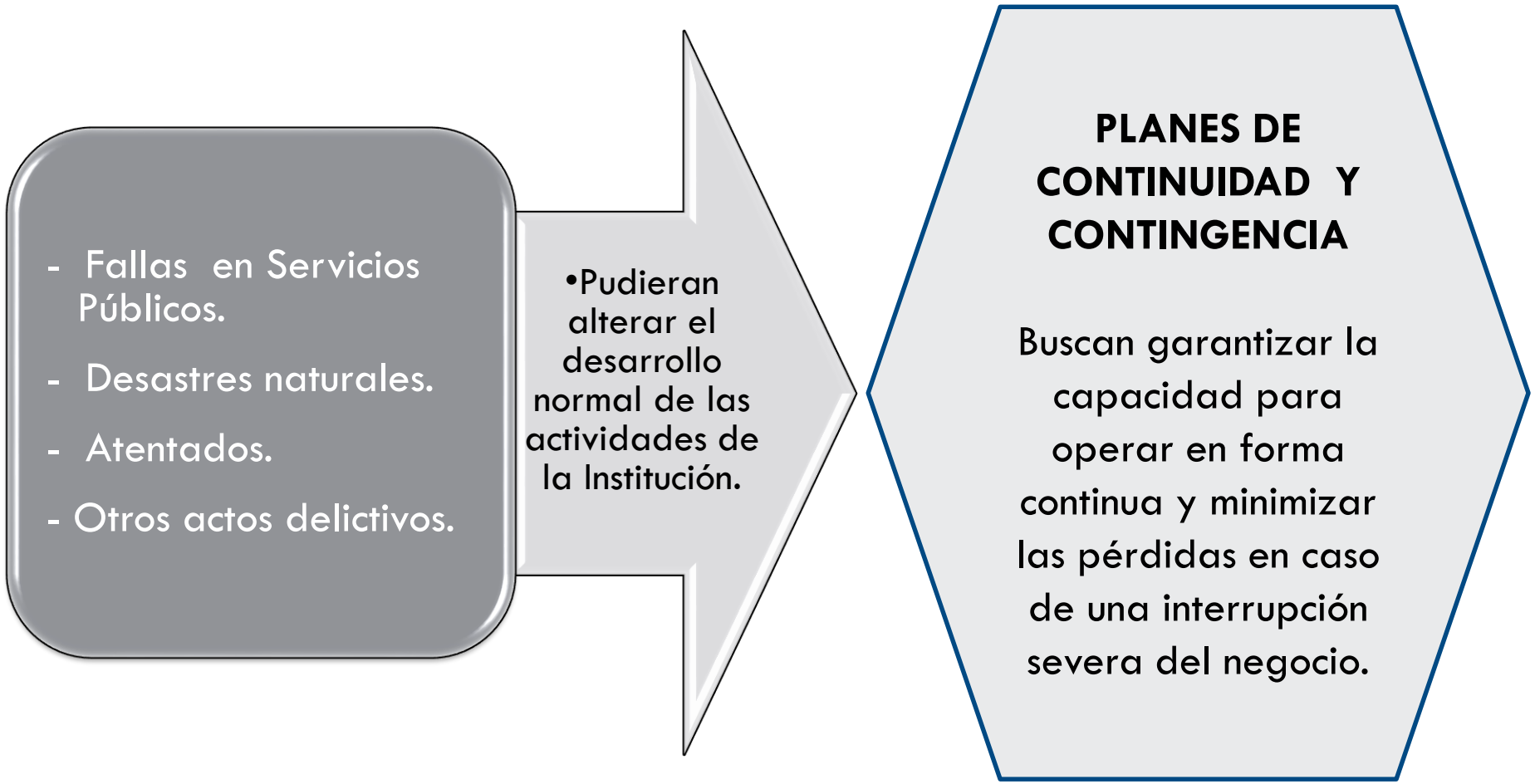
- ❑ Área de tecnología de la información
- ❑ Estructura de gestión de tecnología
  - ✓ Conformación del Comité de Tecnología de la Información
  - ✓ Funciones del Comité de Tecnología de la Información
- ❑ Políticas, procesos, procedimientos y metodologías para la administración de la tecnología de información
  - ✓ Cumplan estándares
  - ✓ Plan estratégico de tecnología de la información (PETI) alineado con el plan estratégico institucional
  - ✓ Proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio
  - ✓ Manual de gestión de la infraestructura
  - ✓ Proveedor servicios de infraestructura, plataforma y/o software en la nube

TECNOLOGÍA DE INFORMACIÓN (TI)

Las entidades de los segmentos 4 y 5 deberán incluir dentro de su gestión, la administración de la tecnología de información; para lo cual deben contar al menos con:

a) Un presupuesto aprobado para el funcionamiento de la operación de tecnología de información;
b) Respaldos de los movimientos de operaciones activas, pasivas, contingentes y de servicios, ubicados fuera del área de procesamiento; y,
c) Normas básicas de operación y un inventario de los principales elementos tecnológicos con los que cuenta.

Eventos Externos



Eventos Externos

NIVEL	ALCANCE	CONTROL
B	PRO	**Determinar el alcance del PCN** Analizas para que activos y procesos debes garantizar la continuidad.
B	PRO	**Concretar el flujo de responsabilidades** Determinas las responsabilidades de las personas que deben llevar a cabo el plan de continuidad en caso de aparición de desastres.
A	PRO/TEC	**Realización del BIA (Análisis del Impacto en el Negocio)** Elaboras detalladamente el BIA de tu empresa.
B	PRO	**Definir la política de comunicación y aviso a entidades externas** Defines que tipo de mensajes debe transmitir tu empresa en caso de desastre.
B	PRO	**Caducidad del PCN** Actualizas el plan de continuidad de negocio de tu empresa cada _____.
A	PRO/TEC	**Elegir la estrategia de continuidad** Eliges la estrategia de continuidad óptima para tu empresa. Teniendo en cuenta si fuera preciso la implantación de un centro de respaldo.
A	PRO/TEC	**Detallar la respuesta a la contingencia** Detallas los procedimientos y controles específicos a ejecutar ante la aparición de un desastre.
A	PRO/TEC	**Desarrollar actividades para verificar, revisar y evaluar el plan de continuidad del negocio** Pruebas y evalúas cada _____ el plan de continuidad de negocio de tu empresa.

EIN GEWINN FÜR ALLE
Die Genossenschaften

DGRV
DIE GENOSSENSCHAFTEN

Eventos Externos

- Definición de una estrategia de continuidad de los negocios en línea con los objetivos Institucionales;
- Identificación de los procesos críticos del negocio, aún en los provistos por terceros;
- Análisis de los principales escenarios de contingencia considerando el impacto y la probabilidad de que sucedan
- Determinar el impacto en términos de magnitud de daños, período de recuperación y tiempos máximos de interrupción que puedan ocasionar los siniestros;
- Elaboración del Plan de Continuidad del Negocio, y aprobado por del Directorio
- Comprobación de la aplicabilidad del PCN mediante pruebas periódicas y los procesos implantados para realizar los ajustes necesarios
- Incorporación del proceso de administración del plan de continuidad del negocio al proceso de administración integral de riesgos

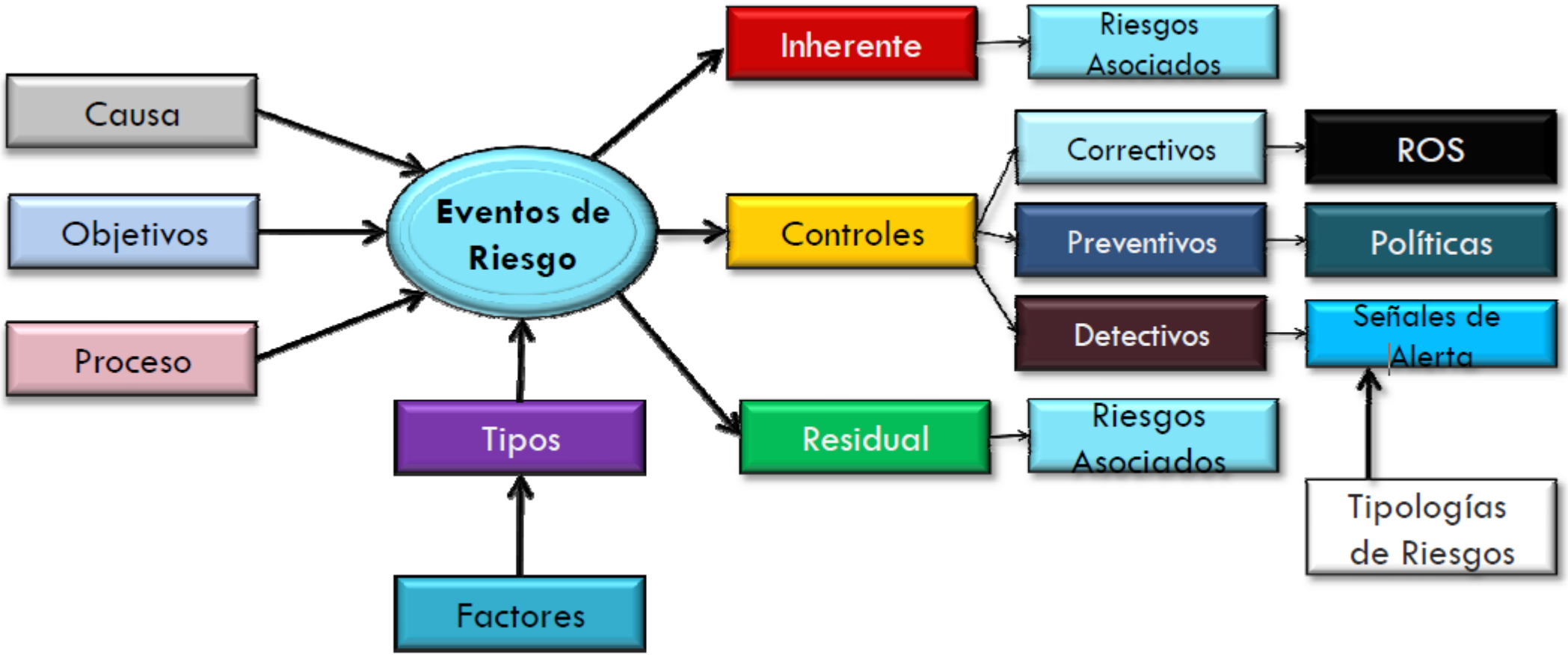
Gestión de eventos de Riesgo Operativo

Gestión de eventos de riesgo operativo

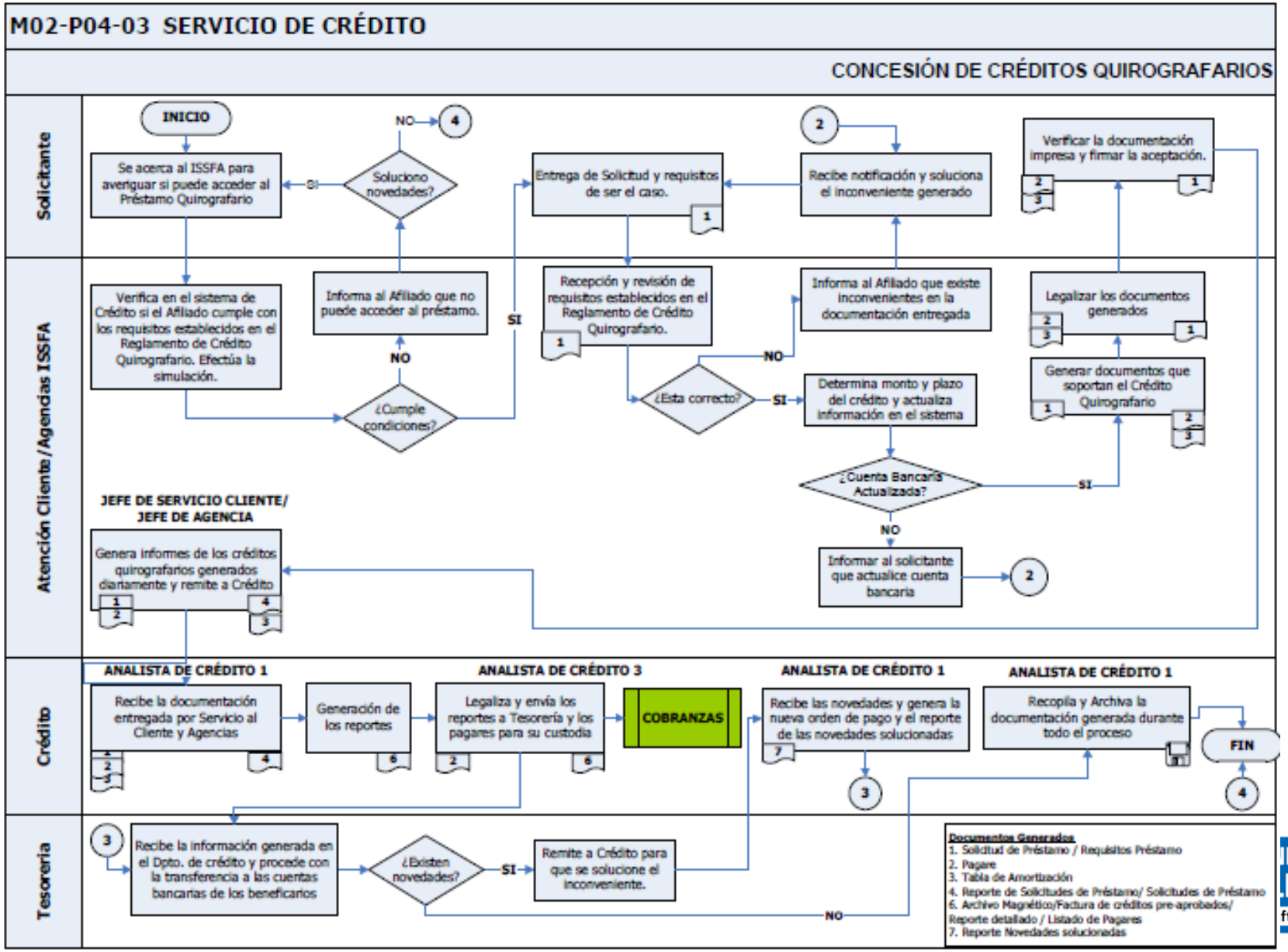
EVENTO DE RIESGO OPERATIVO, es el **riesgo materializado** que deriva en pérdidas financieras para la Cooperativa.

Gestión de eventos de riesgo operativo

Identificar por línea de negocio, los riesgos operativos, agrupados por tipo de evento y las fallas o insuficiencias en los factores de riesgo relacionados con personas, procesos, tecnología de la información y eventos externos



Mapeo de procesos



Proceso de reporte de eventos de riesgo operativo

Funcionario

Identifico el riesgo

Elaboro notificación

Remito al Responsable de Riesgos

Unidad de Riesgos

Evalúa Evento

Levantamiento de información

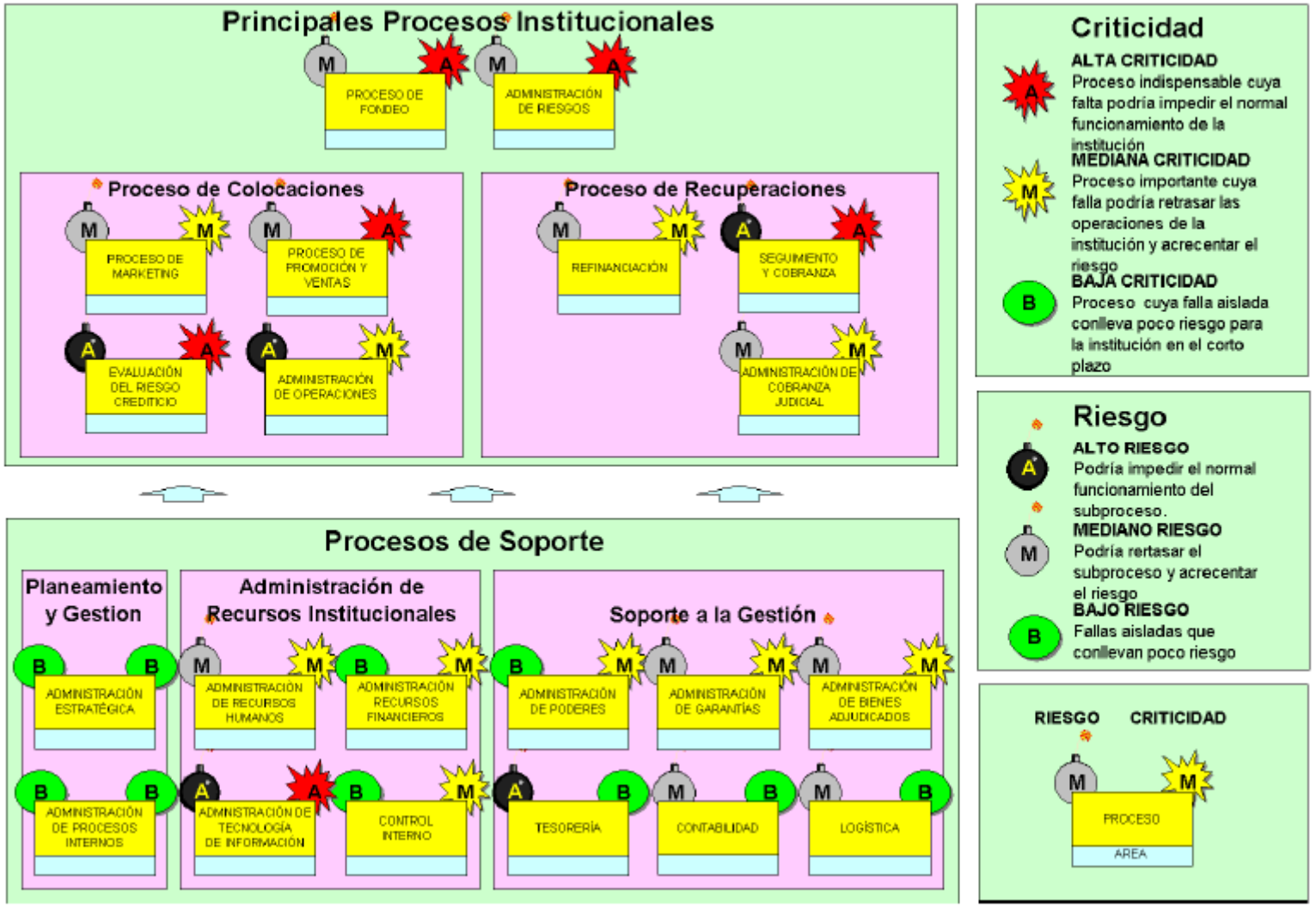
Detalla Formulario

Analiza y clasifica riesgo por proceso

Registra evento de riesgo operativo

DGRV
DIE GENOSSENSCHAFTEN

Mapeo de procesos



EIN GEWINN FÜR ALLE
Die Genossenschaften

DGRV
DIE GENOSSENSCHAFTEN

Etapas del Sistema de Gestión de Riesgo Operativo

Factores	Definición	Ejemplos
Procesos Internos	Pérdidas causadas por transacciones fallidas, cuentas de clientes, pagos y procesos diarios de negocios.	Error de ingreso de datos Acceso no autorizado Diferencia con vendedores Daño negligente/daño activos de clientes
Personas	Pérdidas causadas por falta del personal adecuado, negligencia, error humano nepotismo, inapropiadas relaciones interpersonales, ambiente laboral desfavorable	Negociación no autorizada Fraude interno Terminación equivocada Acoso / Discriminación
Tecnología de Información	Pérdidas originadas en la interrupción de negocios o fallas de los sistemas, o acceso a la información, aun la provista por terceros	Daño de Hardware o software Fallas de Telecomunicación Error de programación / virus informático Interrupción de servicios público
Legal	Pérdidas originadas en la vulnerabilidad de sus activos o que sus activos y contingentes se vean incrementados en niveles superiores a los esperados	Actos Societarios Gestión de Créditos Operaciones de Giro Financiero Actividades Complementarias Cumplimiento Legal y Normativo
Eventos Externos	Pérdidas por eventos fuera del control, por actividades de terceras personas, o cambios de regulaciones que impidan a la institución continuar sus negocios	Desastres naturales Terrorismo / Extorsión Fraude de tarjeta de crédito Crimen tecnológico

Prevención de Pérdidas

Riesgo Operacional Prevención de Pérdidas

- Reingeniería de procesos
- Reestructuración del trabajo
- Rediseño de Productos y Servicios
- Automatización
- Sistemas integrales

- Detección y prevención del fraude
  - Interno y Externo
  - Falsificación, fraude, robo, estafa
  - Utilización de propiedad empresarial
  - Separación de funciones
  - Redundancia de personal en funciones críticas
  - Vacaciones, rotación, entrenamiento cruzado
  - Reconciliaciones
  - Auditoría con clientes
  - Outsourcing

- Ingeniería del Factor Humano
  - Errores, edad, experiencia, stress,
  - Soporte, capacitación, factores ambientales
  - Prácticas gerenciales, contratación

Reporte a la SEPS

FORMULARIO DE REPORTE DE EVENTOS DE RIESGO OPERATIVO

INSTRUCCIONES PARA COMPLETAR ESTE FORMULARIO:

(1) En la columna FECHA DEL EVENTO, ingresar la fecha de registro del evento de riesgo en la matriz de riesgo correspondiente
(2) En la columna LÍNEA DE NEGOCIO, ingresar el nombre de la línea de negocio a la que fue asignado el Proceso en donde se produjo el evento reportado.
(3) En la columna PROCESO, ingresar el nombre del proceso en donde se produjo el evento reportado.
(4) En la columna TIPO DE PROCESO, indicar si el proceso es: Gobernante, Productivo, o de Apoyo.
(5) En la columna PROCESO CRÍTICO, identificar SI es o NO un proceso crítico.
(6) En la columna TIPO DE EVENTO, ingresar en función de la categoria del evento definido en el Articulo 8.
(7) En la columna DETALLE DEL EVENTO, ingresar el evento de riesgo operativo producido.
(8) En la columna FALLA O INSUFICIENCIA, especificar el problema que ocasionó el evento indicado en la columna anterior. En los que fuere el caso considerar las fallas o insuficiencias de orden legal.
(9) En la columna FACTOR DE RIESGO OPERATIVO, se debe indicar el factor de riesgo (Procesos, Personas, Tecnología de Información, ó Eventos Externos)
(10) En la columna PROBABILIDAD, ingresar el nivel de probabilidad o frecuencia de ocurrencia del evento
Con la finalidad de respetar sus propias metodologías favor ingresar en la columna **Nº** el número correspondiente al nivel de probabilidad dependiendo su escala, y en la columna **Nivel** el nombre del nivel de probabilidad
(11) En la columna IMPACTO,ingresar el nivel de impacto en la ocurrencia del evento
Con la finalidad de respetar sus propias metodologías favor ingresar en la columna **Nº** el número correspondiente al nivel de impacto dependiendo su escala, y en la columna **Nivel** el nombre del nivel de impacto
(12) En la columna EFECTO CUANTITATIVO, indicar el valor monetario de la pérdida producida por causa del evento presentado.
(13) En la columna RECUPERACIÓN MEDIANTE COBERTURA, indicar si la pérdida producida, se recuperó por una cobertura existente de forma previa al evento.
(14) En la columna VALOR RECUPERADO, ingresar el monto por valor recuperado por la cobertura
(15) En la columna ACCIÓN TOMADA, describir la(s) MEDIDA(S) DE MITIGACIÓN mas importante(s) que se ha(n) tomado para minimizar la posibilidad de que se vuelva a presentar el evento reportado, así como el NOMBRE y CARGO del Responsable, y las FECHAS DE INICIO y FIN de la implementación de la(s) medida(s) de acción tomada.

SE DEBEN INGRESAR LOS EVENTOS DE RIESGO OPERATIVO IDENTIFICADOS DESDE EL AÑO 2010 HASTA EL 15 DE JULIO DE 2014

POR FAVOR RESPETAR ESTE FORMATO: No modificar el formato, ni la estructura del archivo, y no dejar ninguna columna en blanco.

FECHA DEL EVENTO (1)	LÍNEA DE NEGOCIO (2)	PROCESO (3)	TIPO DE PROCESO (4)	PROCESO CRÍTICO (SI / NO) (5)	TIPO DE EVENTO (6)	DETALLE DEL EVENTO (7)	FALLA O INSUFICIENCIA (8)	FACTOR DE RIESGO OPERATIVO (9)	PROBABILIDAD (10)		IMPACTO (11)		EFECTO CUANTITATIVO (PÉRDIDA PRODUCIDA) (12)	RECUPERACIÓN MEDIANTE COBERTURA (Si / No) (13)	VALOR RECUPERADO (14)	ACCIÓN TOMADA (15)		
									Nº	Nivel	Nº	Nivel				MEDIDA(S) DE MITIGACIÓN	FECHA INICIO	FECHA FIN
08/17/2013	Segmento minorista	Apertura y cierre de oficinas	HABILITANTE	NO	Daños a activos materiales	PÉRDIDA DE LLAVES DE LAS PUERTAS PRINCIPALES (ACORDIONES) Y SECUNDARIAS (DE VIDRIO) DE LA OFICINA MATRIZ, POR PARTE DEL ENCARGADO DE LAS MISMAS (AUXILIAR DE SERVICIOS GENERALES)	Las únicas llaves se encontraban bajo custodio y administración del Auxiliar de Servicios	Personas	1	Improbable	1	Bajo	$ 65.00	NO	$ 65.00	Definición de procedimiento de contingencia para la administración de llaves	08/17/2013	08/17/2013
08/23/2013	Segmento minorista	Administración de Seguridades Físicas	HABILITANTE	NO	Clientes, productos y prácticas empresariales	ACCIDENTE CAUSADO A LA SEÑORA NOEMÍ BAILON BALCAZAR, AL DESPRENDERSE UN PORCELANATO DE LA PARED DEL EDIFICIO DE LA AGENCIA GRAN COLOMBIA	Peso de porcelanato muy elevado para colocar en fachada de Agencia	Procesos	1	Improbable	1	Bajo	$ 226.11	NO	$ 226.11	Modificación de estructura de fachada de agencia	08/23/2013	08/30/2013

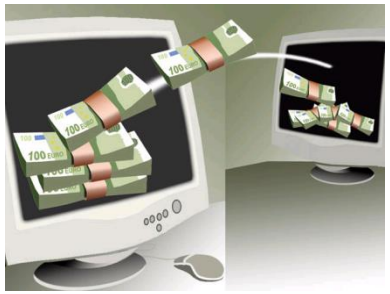
Tipos de eventos

Fraude interno:

- Falsificación por ausencia de controles.
- Apropiación de recursos económicos o materiales.
- Inadecuada información confidencial.

Fraude externo:

- Emisión de cheques sin fondos.
- Falsificación por falta de seguridades de información.



Tipos de eventos

Prácticas laborables y Seguridad del ambiente de trabajo:

- Reclamos por compensación e indemnización al personal.
- Violación de normas de salud o seguridad.
- Todo tipo de discriminación.

Daños a los activos físicos:

- Terrorismo.
- Vandalismo.

Tipos de eventos

Interrupciones del negocio y fallas en los sistemas:

- Fallas en el software.
- Fallas en el hardware.
- Problemas de telecomunicaciones.

Deficiencias en la ejecución de procesos, en las relaciones con proveedores y otros:

- Error en el ingreso de datos.
- Documentación de respaldo incompleta.

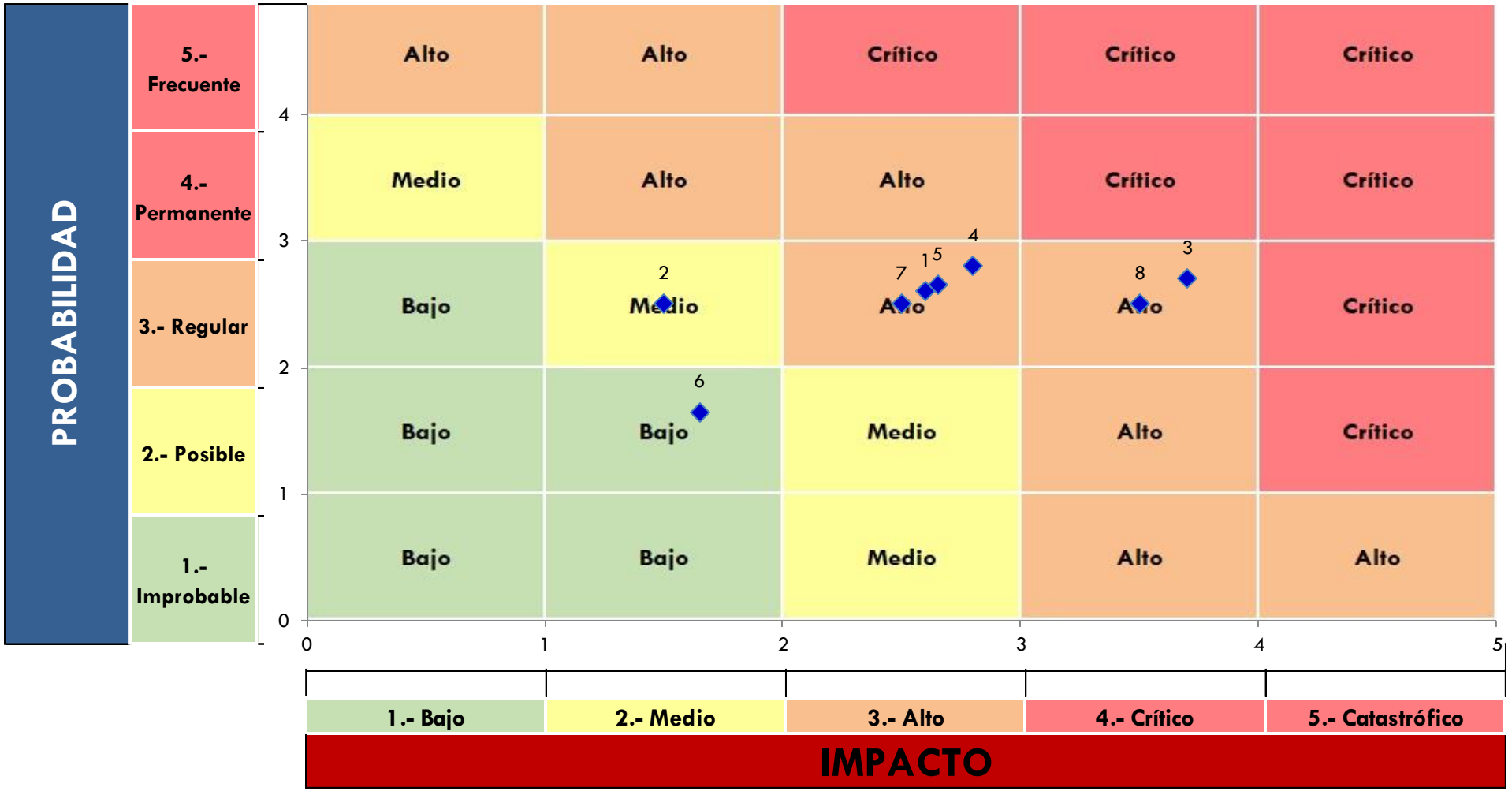
Practicas relacionadas con Proveedores, los productos y el negocio:

- Manejo inadecuado de información de proveedores.
- Prácticas contrarias a la competencia.

Principales Fuentes para identificar riesgos operativos

- ✓ Informes de Auditoria Interna
- ✓ Informes de Auditoria Externa
- ✓ Informes de Organismos de Control (SB, SEPS, etc.)
- ✓ Análisis de Procesos - Talleres de Riesgo Operacional

Registro de eventos de riesgo operativo



Seguridad de información

Seguridad de la Información

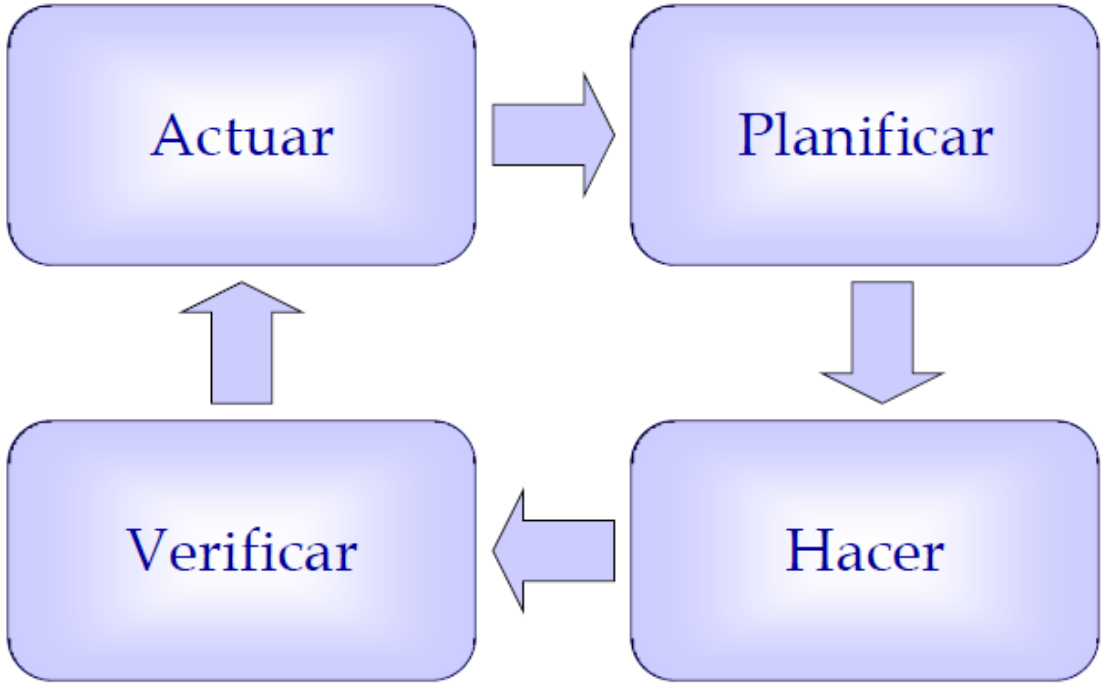
- La Información es un activo que como cualquier otro activo importante del negocio, tiene valor para la organización, consecuentemente necesita **“Protección Adecuada”.**

- Tipos de Información
  - Impresos o escritos en papel.
  - Almacenada electrónicamente.
  - Transmite por correo o en forma electrónica.
  - La que se muestra en videos corporativos.
  - Lo que se habla en conversaciones.
  - Estructura corporativa de información.

- OBSTÁCULOS
  - Falta de conciencia de usuarios finales.
  - Presupuesto.
  - Falta de apoyo de la alta gerencia.
  - Falta de Entrenamiento.
  - Pobre definición de responsabilidades.
  - Falta de herramientas.
  - Aspectos legales.

SGSI SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

Está basado en el Modelo utilizado por las NORMAS ISO en general:



Ciclo de Vida de los Sistemas de Seguridad

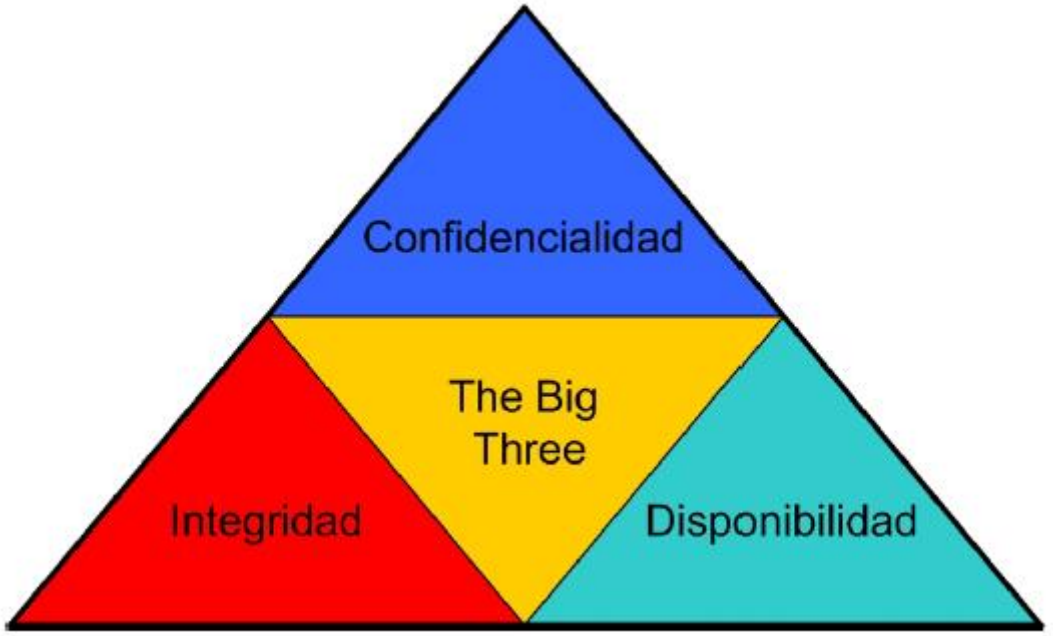
Los conceptos que representan los tres principios básicos de la seguridad informática son

Confidencialidad: es la prevención de los accesos intencionales o no intencionales a la información clasificada.

Integridad: el concepto de integridad agrupa:

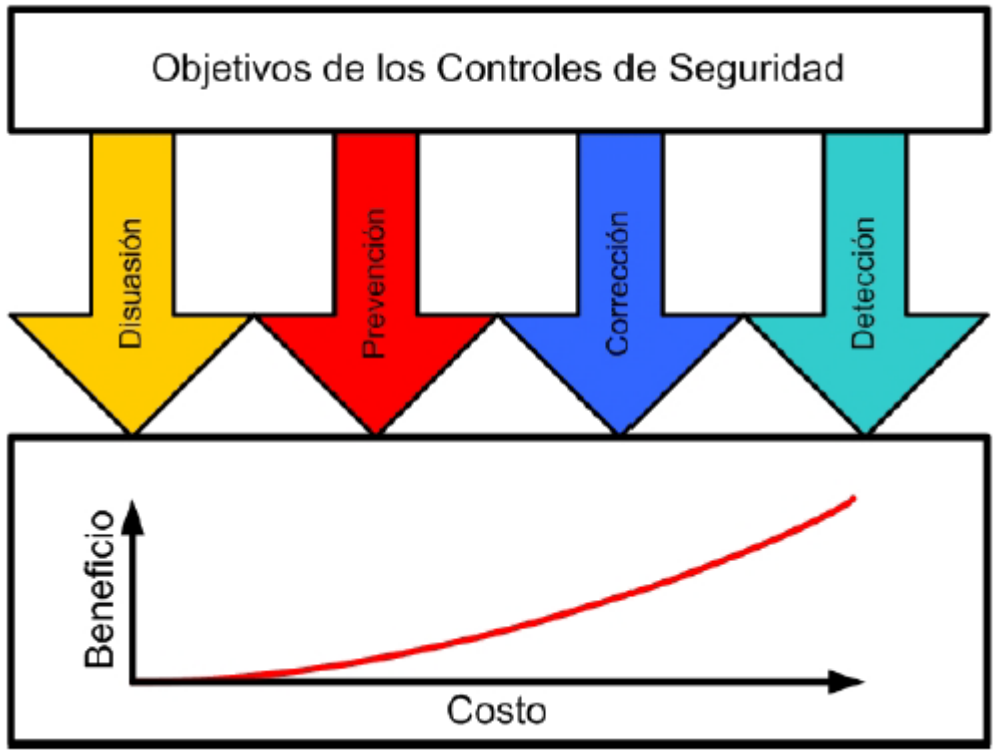
- No permitir las modificaciones de la información por medio de personal o procesos no autorizados.
- La información es interna y externamente consistente.

Disponibilidad: el concepto de disponibilidad garantiza que los servicios de seguridad estén en línea y no conlleven a un problema de acceso a la información.

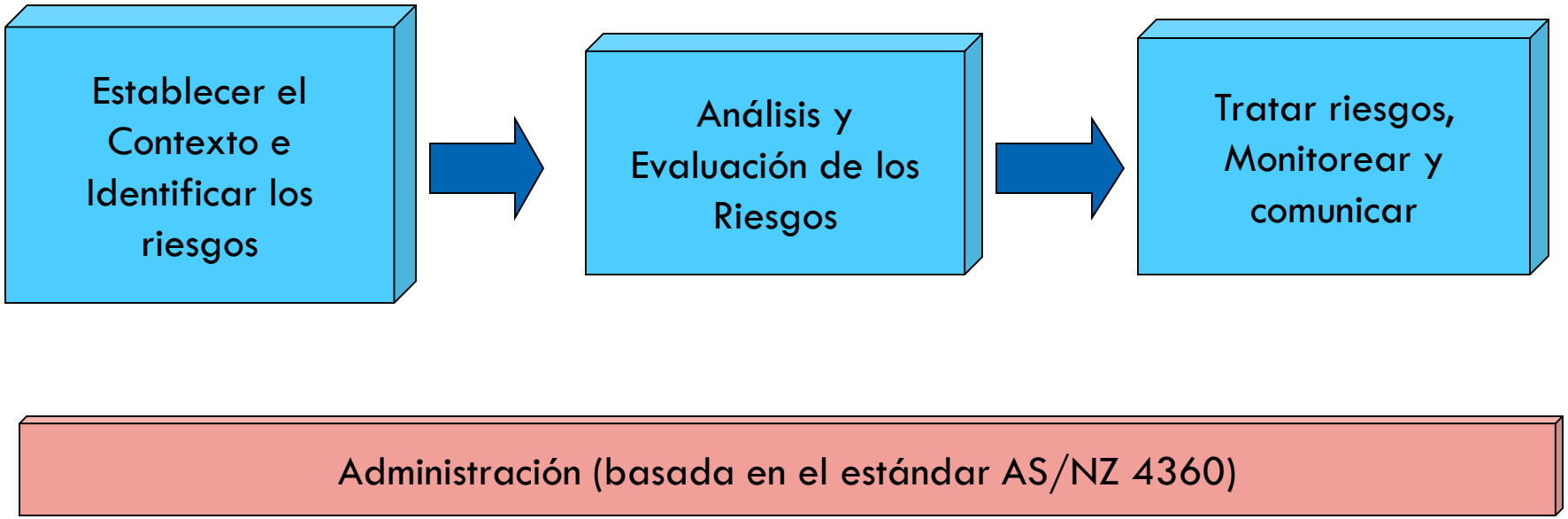


Objetivos de los controles de Seguridad

El objetivo de los controles de seguridad es reducir las vulnerabilidades a niveles tolerables y minimizar los efectos de los ataques. El proceso que evalúa los distintos escenarios y estima las potenciales perdidas es el Risk Analysis. Los diferentes controles son:



Fases del proceso de seguridad Evaluación



Criterios de clasificac

SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

EIN GEWINN FÜR ALLE Die Genossenschaften

DGRV DIE GENOSSENSCHAFTEN

Criterios de clasificación de la información

- Procedimiento de Identificación de Activos de Información
  - Identificación de los procesos de negocio a los cuales se realizará el procedimiento de inventario.
  - Identificar los responsables del proceso de negocio.
  - Revisión de flujo de información del proceso e identificación de:
    - Información
    - Contenedores físicos o electrónicos
    - Medios de transporte de la información

Criterios de clasificación de la información

- Procedimiento de Clasificación
  - Rol de la Alta Gerencia en la definición de los criterios de clasificación.
  - Procedimiento de Clasificación
  - Determinación del nivel de criticidad y sensibilidad del activo de información (CID).

Tecnología de la información

Tecnología de la Información

Plan de Contingencia	• Conjunto de procedimientos alternativos a la operatividad normal de la entidad cuya finalidad es la de permitir su funcionamiento, buscando minimizar el impacto financiero que pueda ocasionar cualquier evento inesperado específico. El plan de contingencia se ejecuta el momento en que se produce dicho evento
Plan de Reanudación	• Especifica los procesos y recursos para mantener la continuidad de las operaciones en la misma ubicación del problema.
Plan de Recuperación	• Especifica los procesos y recursos para recuperar las funciones del negocio en una ubicación alterna dentro o fuera de la institución

Respaldos y custodia de información (backups externos)

Qué es una copia de seguridad

- La información almacenada por el proveedor deberá estar a disposición permanente de la entidad y a través de ésta, del organismo de control, por medio de los canales o mecanismos que disponga para el efecto. La información es de estricta confidencialidad y no podrá ser comercializada o utilizada para otros fines distintos a los manejados por la entidad dueña de la información La notificación de término del contrato deberá ser informada por el proveedor con la debida anticipación, con el propósito de garantizar la continuidad de las operaciones de la entidad.

- En caso de terminación del contrato de servicios de infraestructura, plataforma y/o software, la información será devuelta por el proveedor a la entidad de forma inmediat4 conservando un respaldo de seguridad por un período de al menos tres meses debiendo observar estricta confidencialidad y el impedimento para utilizarla y comercializarla.

- Las entidades referidas en este artículo y la Corporación deberán informar al consejo de administración sobre el detalle de los servicios a ser contratados que incluya el análisis de los riesgos operativos, legales, tecnológicos, de seguridad y continuidad a los que se exponen al adoptar este servicio; así como los controles para mitigarlo;

Qué es una copia de seguridad

- En el sentido más académico, una copia de seguridad es un proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperarlos en caso de fallo del primer alojamiento de los datos.
- En el ámbito empresarial podríamos definir la copia de seguridad como la salvaguarda de nuestro negocio, una medida indispensable para garantizar su continuidad y conservar la confianza que nuestros clientes han depositado en nuestra organización. De lo contrario, podríamos proyectar una imagen negativa y generar desconfianza.

¿Por qué hacer copias de seguridad?

- Lo más probable es que manejes información importante y confidencial y se depende de ella para que el negocio siga adelante. La pérdida de esta información supondría la pérdida de horas de trabajo y de proyectos que tendría graves consecuencias para la continuidad del negocio.
- Hay que tener en cuenta que los soportes donde recogemos esa información suelen tener una vida útil limitada (averías, desgastes…) y están sujetos a diversos riesgos y/o amenazas (accidentes, ataques...). Por estos motivos tenemos que implementar las medidas para proteger el mayor activo que almacenamos en dichos soportes, la información, así que empecemos a hacer copias de seguridad.

Criterios de clasificación de la información

- Por el nivel de accesibilidad o confidencialidad:
  - Confidencial: accesible solo por la dirección o personal concreto.
  - Interna: accesible solo al personal de la empresa.
  - Pública: accesible públicamente.
- Por su utilidad o funcionalidad:
  - Información de clientes y proveedores.
  - Información de compras y ventas.
  - Información de personal y gestión interna.
  - Información sobre pedidos y procesos de almacén.
- Por el impacto en caso de robo, borrado o pérdida:
  - Daño de imagen.
  - Consecuencias legales.
  - Consecuencias económicas.
  - Paralización de la actividad.

Criterios de clasificación de la información

CATEGORÍA	DEFINICIÓN	TRATAMIENTO
Confidencial	Información especialmente sensible para la organización. Su acceso está restringido únicamente a la Dirección y a aquellos empleados que necesiten conocerla para desempeñar sus funciones. También datos de carácter personal, en particular los de categorías especiales.	Esta información debe marcarse adecuadamente. Se deben implementar todos los controles necesarios para limitar el acceso únicamente a aquellos empleados que necesiten conocer la información. En caso de sacarla de las instalaciones de la empresa en formato digital, debe cifrarse. Para los datos de carácter personal, se deben tener en cuenta la protección y garantías indicadas en la legislación sobre la materia.
Interna	Información propia de la empresa, accesible para todos sus empleados. Por ejemplo, la política de seguridad de la compañía, el directorio de personal u otra información accesible en la intranet corporativa.	Esta información debe estar adecuadamente etiquetada y accesible para todo el personal. No debe difundirse a terceros, salvo autorización expresa de la dirección de la empresa.
Pública	Cualquier material de la empresa sin restricciones de difusión. Por ejemplo, información publicada en la página web o materiales comerciales.	Esta información no está sujeta a ningún tipo de tratamiento especial.

LA ESTRATEGIA 3-2-1 DE LAS COPIAS DE SEGURIDAD

- Una buena práctica a la hora de realizar copias de seguridad es adoptar la estrategia 3-2-1 que se basa en diversificar las copias de seguridad para garantizar que siempre haya alguna recuperable. Sus claves de actuación son las siguientes:
  - ❖ 3: Mantener 3 copias de cualquier fichero importante: el archivo original y 2 backups.
  - ❖ 2: Almacenar las copias en 2 soportes distintos de almacenamiento para protegerlas ante distintos riesgos. Si tuviéramos las dos copias en el mismo tipo de soporte, ambos pueden verse afectados por el mismo fallo de funcionamiento y por tanto poner en peligro las dos copias al mismo tiempo.
  - ❖ 1: Almacenar 1 copia de seguridad fuera de nuestra Cooperativa, lo que también se conoce como backup offsite. La copia de seguridad en la nube es una clara opción de este tipo de copia.

Almacenamiento en nube

- La nube: el almacenamiento en la nube se basa en salvaguardar nuestras copias de seguridad en servidores de terceros. Por lo tanto, nuestra única preocupación será la de exigir las garantías de seguridad pertinentes a la empresa que se encargue de facilitarnos dicho servicio.
- Las ventajas del almacenamiento en la nube son claras:
  - ✓ Poseemos una copia de seguridad fuera de la empresa.
  - ✓ Nos asegura la disponibilidad de los datos en cualquier momento y, por tanto, la continuidad de negocio.
  - ✓ La copia está protegida ante cualquier incidente que pueda ocurrir dentro de la organización.

Almacenamiento en nube

- En cuanto a las desventajas, cabe destacar:
  - ✓ La confidencialidad, puesto que estamos enviando la información con la que trabajamos a un tercero. Por lo tanto, se deberán firmar Acuerdos de Nivel de Servicios (ANS) con el proveedor, que garanticen la disponibilidad, integridad, confidencialidad y control de acceso a las copias.
  - ✓ Dependencia de la conexión a Internet a la hora de restaurar las copias de seguridad.
  - ✓ Se necesita un ancho de banda de subida elevado para garantizar el envío de las copias en un tiempo adecuado.

Como dijo el científico Stephen Hawking:
“La inteligencia es la habilidad de adaptarse al cambio”

¡No te extingas, Adáptate!

EIN GEWINN FÜR ALLE
Die Genossenschaften

DGRV
DIE GENOSSENSCHAFTEN

DGRV
DIE GENOSSENSCHAFTEN

Muchas Gracias – Vielen Dank

Roger Chamba González

0994722443

rchamba@gmail.com

cooperación alemana
DEUTSCHE ZUSAMMENARBEIT

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

EIN GEWINN FÜR ALLE
Die Genossenschaften

DGRV
DIE GENOSSENSCHAFTEN