

# Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Oficina de Sistemas

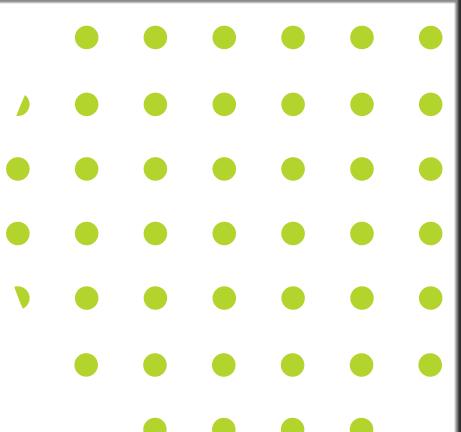
2024



**Indeportes Antioquia**  
calle 48#70 - 180. Medellín. Tel: 520 08 90  
[www.ind deportesantioquia.gov.co](http://www.ind deportesantioquia.gov.co)



# Objetivo



Caracterizar los activos de información de INDEPORTES ANTIOQUIA. Establecer e implementar una adecuada identificación, clasificación, valoración, disposición documental, publicación, seguimiento y mejora, de los activos de información adquiridos o propios, los cuales desarrolla o produce y comparte INDEPORTES ANTIOQUIA de acuerdo a las necesidades de las partes interesadas y de acuerdo con la legislación aplicable, requisitos legales, técnicos, operativos y de gestión aplicables.

Se aplica a todos los procesos estratégicos, misionales, y de apoyo de INDEPORTES ANTIOQUIA. Este Inicia con la identificación, clasificación, valoración y disposición documental como fases para la obtención de los activos, y se termina con la publicación de los activos de información y su actualización respectiva.

# Alcance

# Metodología

## Gestión de riesgos de seguridad de la información basado en ISO 27005

Esta norma suministra soporte a los conceptos que se especifican en la ISO IEC 27001 la cual facilita la implementación satisfactoria de la seguridad de la información con base en el enfoque de gestión del riesgo. Esta norma se puede aplicar a todo tipo de Organizaciones que determine gestionar los riesgos de la seguridad de la información.

Esta norma se puede aplicar a todo tipo de Organizaciones que determine gestionar los riesgos de la seguridad de la información

ISO 27001  
SGSI

6.1.2 Valoración de riesgos de la seguridad de la información

6.1.3 Tratamiento de riesgos de la seguridad de la información

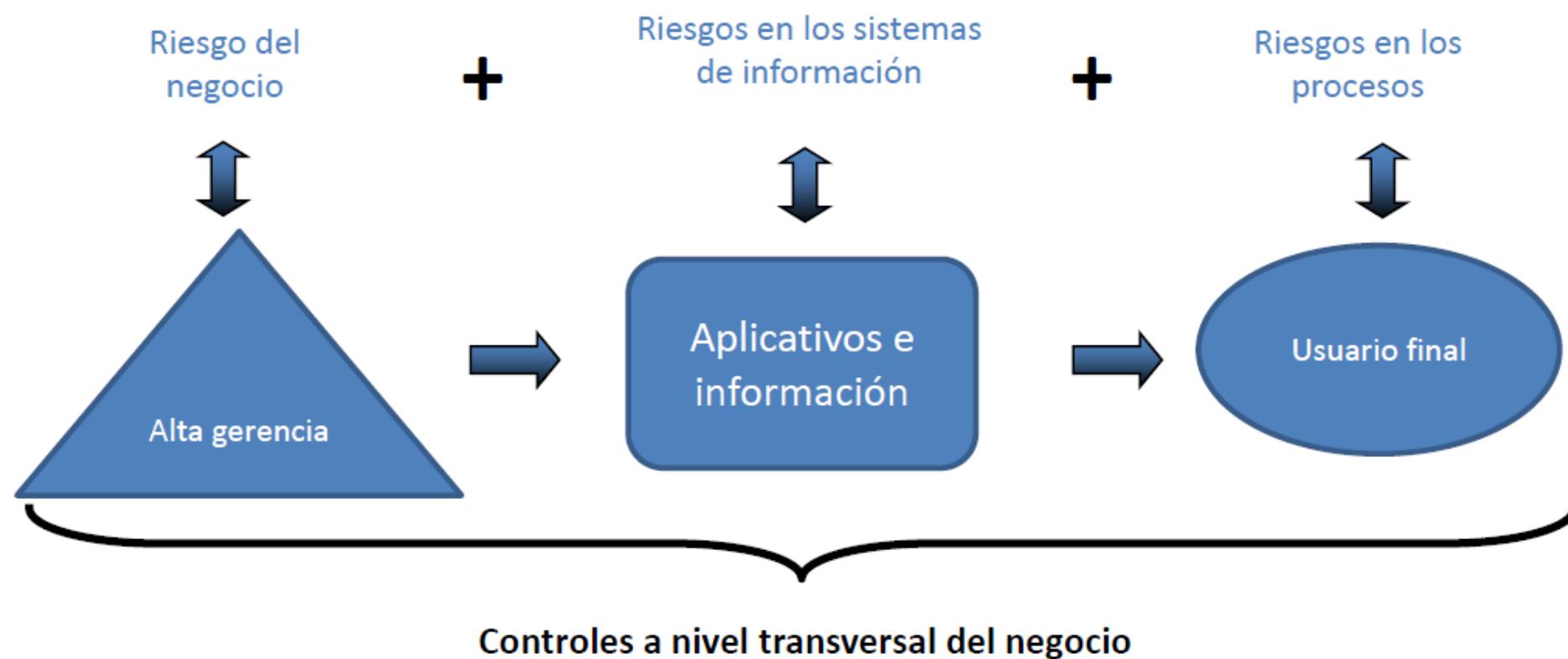


# Oportunidades

El propósito es gestionar/explotar las oportunidades de negocio y se enfoca en la inversión.

De naturaleza ofensiva.

Éxito de una vulnerabilidad por una amenaza en un activo al cual se le debe asignar un valor monetario estimado por rangos (por ej Entre U 1 y U 10 millones) se evalúa la probabilidad de ocurrencia del evento, por ej El virus es diario, semanal, etc Clasificarlos en alto, medio o bajo.



# Impacto

# Por qué ISO 27005?

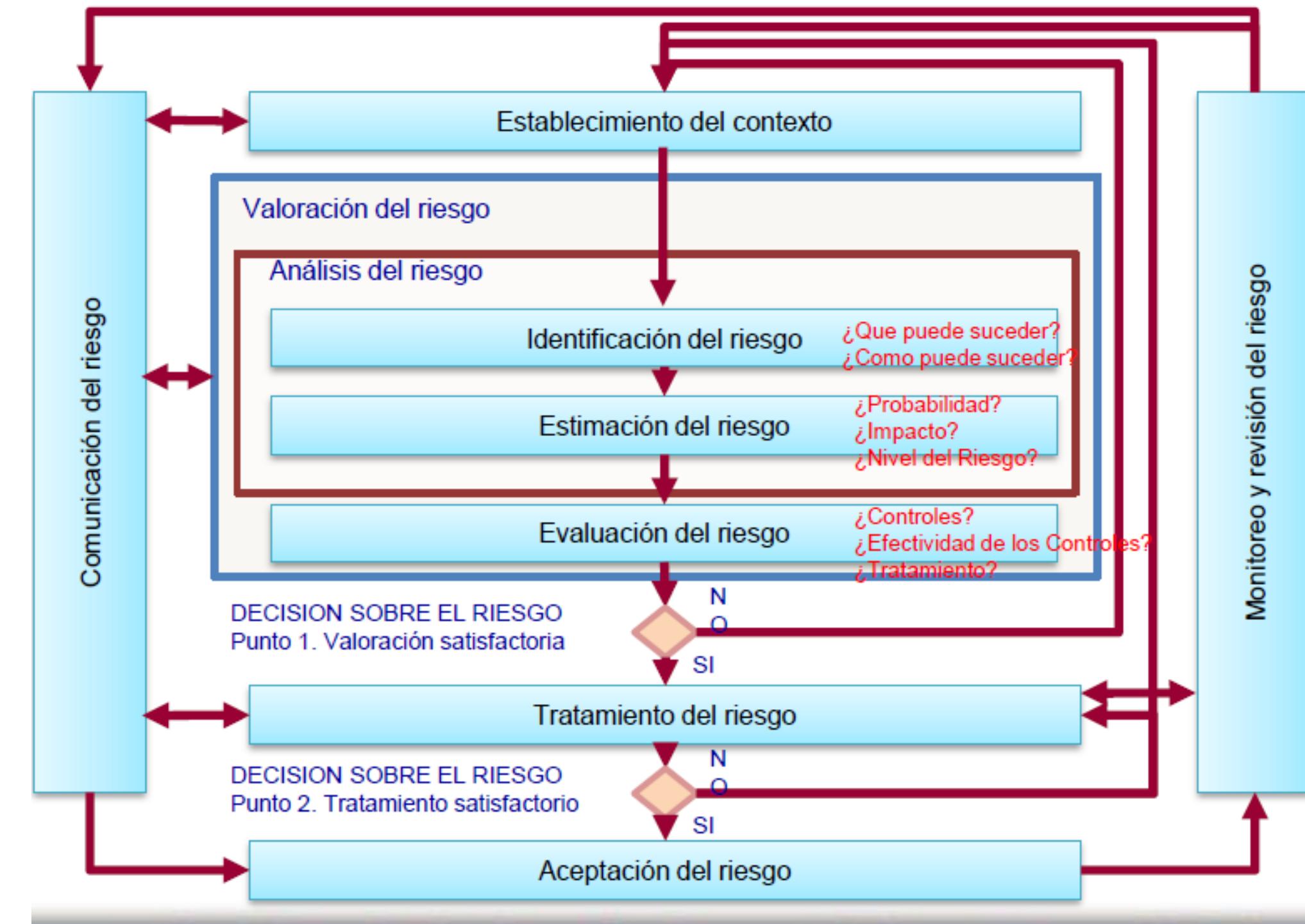


Buscando eficiencia y eficacia de los procesos , un Sistema de gestión de riesgos cuenta con estas características y principios:

- Crea y protege el valor, pues contribuye al logro de los objetivos
- La gestión del riesgo es parte integral de todos los procesos
- Su salidas son fundamentales en la toma de decisiones
- Se ocupa de la incertidumbre
- Es sistemática, estructurada y oportuna
- Se basa en la mejor información disponible
- Es específica
- Toma en cuenta los factores humanos y culturales de la Organización
- Es transparente e inclusiva pues se ubica en todos los procesos
- Es dinámica, iterativa y orientada al cambio
- Facilita la mejora continua

# Proceso de gestión del riesgo

Basado en ISO-IEC 27005



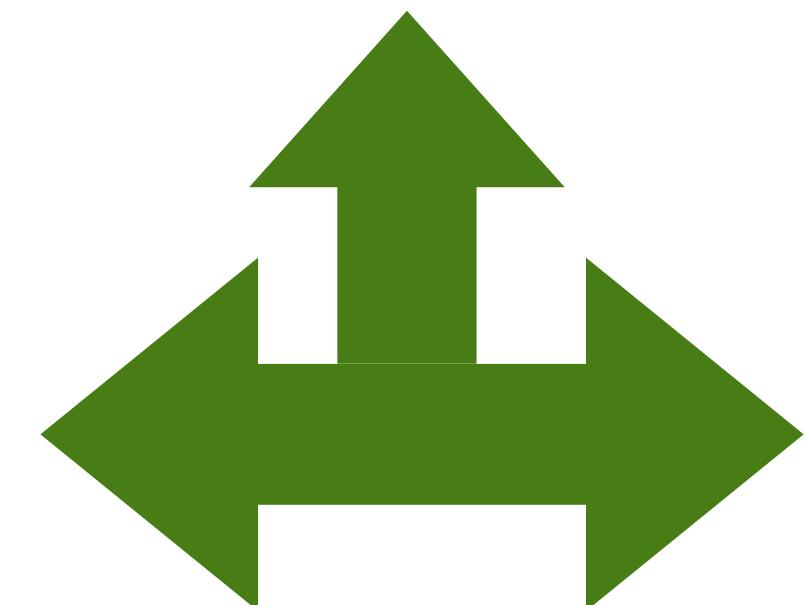
# Contexo

La Organización articula sus objetivos y define componentes externas e internas a considerar para establecer el alcance y los criterios de desempeño del riesgo.

Condiciones externas e internas que podrían generar impactos en el cumplimiento de los objetivos

- Ambiente
- social y cultural
- Entorno político
- Cumplimiento, legal y reglamentaria
- Tecnología
- Entorno económico
- Competitividad
- Impulsores

- Cultura Organizacional
- Gobierno, estructura, funciones y responsabilidades
- Normas, directrices, procesos
- Componentes técnicos
- Tecnología Interna
- Clientes
- Aspectos sicosociales



# Identificación de los activos TI



Se requiere identificar los activos para luego realizar la valoración del riesgo.

Se identifican dos clases de activos

## PRIMARIOS

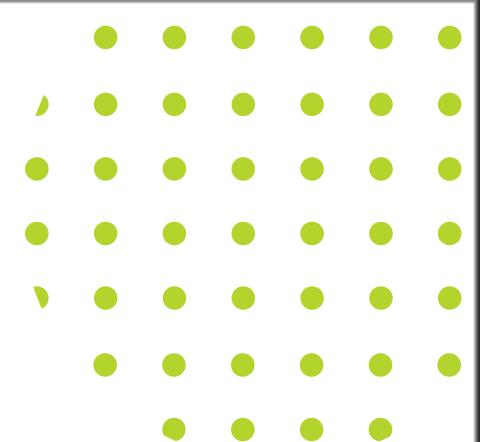
Actividades y procesos misionales, tecnología propietaria, aquellos con requisitos legales y contractuales

Información de procesos misionales, de alto costo de procesamiento, almacenamiento, transmisión y recuperación

## SECUNDARIOS

- Hardware
- Software
- Redes y conectividad
- Servicios (Subcontratistas/proveedores/ Personas a cargo de toma de decisiones (Conocimiento del negocio)

# Clasificación de Activos



Resumen			
Ítem	Código	Clasificación	Tipo
1	IF1	Información Física 1	Documental
2	IF2	Información Física 2	
3	S1	Herramientas para la Operación	Software
4	S2	Software Gestión	
5	R1	Red	Infraestructura
6	SL	Servidor Local	
7	EC	Equipo de computo	Equipos
8	AL	Almacenamiento.	Almacenamiento
9	CN	Conocimiento del negocio	Intangible y RH

# Amenaza

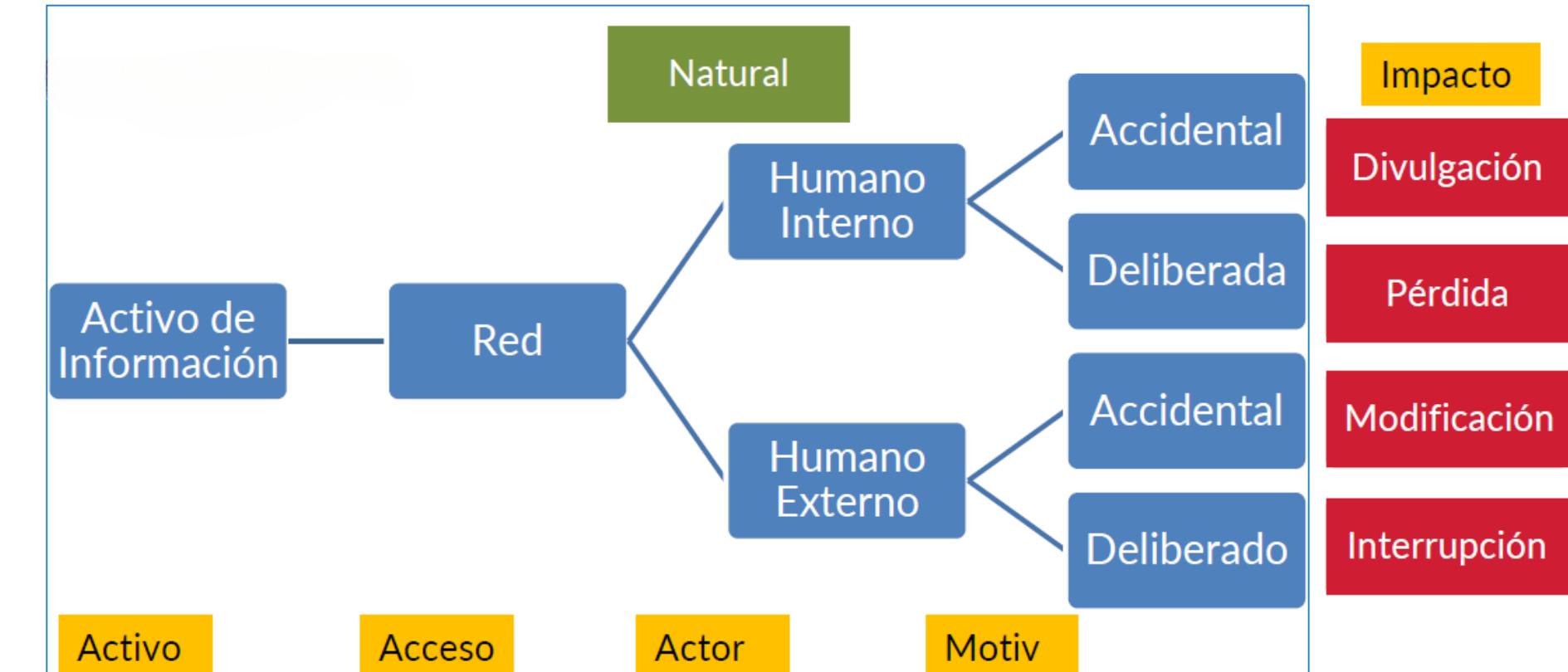
Están presentes en cada sistema o activo bajo las premisas de:

**Confidencialidad**  
**Disponibilidad**  
**Integridad**

**El propósito es reducir el impacto negativo de naturaleza defensiva**

**Escenario (donde una acción o suceso ( compromete la seguridad de un Activo de Información**

**Causa**  
**Motivo o circunstancia**



Ejemplos:

- Daño físico ( accidentes, fuego, etc)
- Introducción de código malicioso al sistema
- Accesos/cambios no autorizados
- Illegalidad de software
- Fraudes/robos de identidad
- Pérdida inesperada de los servicios críticos
- Accidentes ocasionados por eventos de la naturaleza

# Vulnerabilidad

Ejemplos:

Actividad No.2 Riesgos de la Información		
ACTIVO DE INFORMACIÓN	AMENAZA	VULNERABILIDAD
Centro de cómputo	Inundación	Ubicación del Data Center en áreas cercanas a ríos, lagunas.
Equipos de Comunicaciones	Pérdida de los servicios de T.I .	Ausencia de política de Continuidad del Negocio.
Recurso Humano	Pérdida de personal clave.	Ausencia de planes de sucesión.
Aplicativos "core del negocio"	Fallos de los procesos que afecten la Confidencialidad / Disponibilidad / Integridad.	Defectos de construcción de software

La entidad está en riesgo cuando:

- Defectos o daños de cualquier activo de Información.
- Interrupciones no programadas.
- Modificación, interceptación o alteración de datos sin las debidas autorizaciones.

Además:

- Pérdida de operación o continuidad
- Fallos o defectos sin previsión de la infraestructura de T.I.
- Imposibilidad de cumplir la promesa de servicio a los usr. Internos y externos

# Riesgos

## ¿RIESGO = INCERTIDUMBRE?

Es la potencialidad que una amenaza explote las vulnerabilidades de los A.I., se convierta en un desastre y afecten los objetivos de la Organización (económicas, ambientales, imagen, reputación...

Puede ser positivo o negativo

### Gestión del Riesgo.

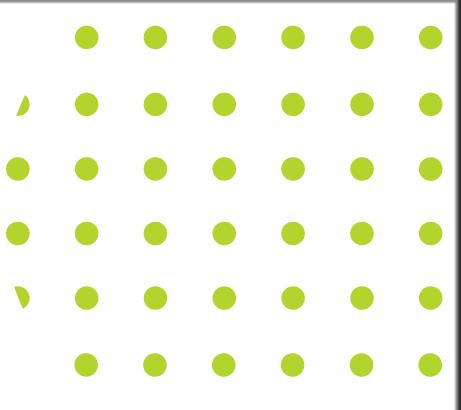
Es una práctica metodológica y sistemática que se ejecuta para identificar, medir, clasificar y definir los procedimientos, políticas y acciones

OBJETIVO

### Controles:

**M**itigar  
**E**vitar  
**T**ransferir  
**A**sumir

# Riesgos



## Ciclo de la gestión de riesgos

EVALUACIÓN

IDENTIFICACIÓN

CLASIFICACIÓN

ANÁLISIS

CONTROLES  
DE TI

PLANEACIÓN

ORGANIZACIÓN

TRATAMIENTO

MONITOREO

EVALUACIÓN

CONTROL

# Modelo de gestión de riesgos

Los siguientes 9 pasos comprenden el modelo de gestión de riesgos.

Inicia en el CONTEXTO y finaliza en el diseño de LOS CONTROLES

1. ESTABLECIMIENTO DEL CONTEXTO EXTERNO E INTERNO
2. CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

CLASIFICACION DE ACTIVOS DE INFORMACION				
TIPOS DE ACTIVOS INDEPORTES ANTIOQUIA				
Documental	Software	Infraestructura	Servicios	Intangibles
TRD Cada	Mesa de ayuda SysAid	Redes	Copias de respaldo (SaaS)	Conocimiento del negocio
	Sicof.	Indemed y bienestar	servidor evm.pdc01-ind	
	Hércules.	Directorio activo ppal	servidor evm-papp02-ind	
	Mercurio.	Indemed y bienestar		
	Software Ofimatico	Directorio activo sec.		
		Equipo de computo		
		Equipo movil		

# Modelo de gestión de riesgos

RIESGO TECNOLÓGICO	ACTIVOS DE INFORMACIÓN	AMENAZAS
COMPROMISO DE LA INFORMACION	Recurso Humano	Recuperación de información de medios reciclados
		Divulgación de Información confidencial
		Robo de Información
	Infraestructura	Falsificación de Información
		Interceptación de Información no autorizada
		Espionaje
ACCIONES NO AUTORIZADAS	Software	Hurto o perdida de equipos
		Copia o uso ilegal del Software
		Uso no autorizado del activo
	Recurso Humano	Ingreso al centro de computo sin autorización
		Suplantación de Identidad
		Fraude
PERDIDA DE SERVICIOS ESCENCIALES	Infraestructura	Robo de Información
		Energía Eléctrica
		Corto Circuito
		Agua
FALLAS TECNICA O DAÑO FISICO	Infraestructura	Aire acondicionado
		Fallas en el monitoreo de la Red
		Obsolencia de equipos
EVENTO NATURAL	Infraestructura	Vencimiento de Licencias
		Incendio
		Sismo
CIBERATAQUES INFORMATICOS	Infraestructura	Inundaciones
		Denegación de servicios
		Inyección SQL
		Ataque de Fuerza Bruta
		Exploits
		Puertas traseras
	Software	Malware (Virus)
		Denegación de servicios
	Proveedores	Inyección SQL
		Malware (Virus)
	Conocimiento del Personal	Denegación de servicios
		Ataque de Ingeniería social
		Ataque por phishing
		Ciberestafas

## 3. CLASIFICACIÓN DE AMENAZAS Y VULNERABILIDADES A LOS ACTIVOS DE INFORMACION

Vulnerabilidades para la Seguridad de la Información y Ciberseguridad	
Desconocimiento de Políticas de seguridad por parte de los empleados	
Falla en la instalación de Parches de seguridad y sistema en servidores y equipos de computo	
Incumplimiento en el procedimiento control de cambios	
Falla en el licenciamiento del servidor de Antivirus	
Falta de conocimiento en el monitoreo del servidor de Antivirus	
Falta de una herramienta de Gestión de Incidentes y control de licenciamiento	
Errores en la programación de Software	
Errores Humanos intencionados	
Falta de Mantenimiento preventivo y correctivo a los activos de Información	
Falta de capacitación y certificación para el personal que administra la Infraestructura	
Falta de capacitación y certificación para el personal de seguridad y Ciberseguridad	
Falta de capacitación y concientización a los usuarios sobre las buenas prácticas de la Seguridad y Ciberseguridad	
Falta de Herramienta de Monitoreo de la Red en tiempo Real	
Falta de una herramienta SIEM y SOC que nos ayude con la gestión de incidentes de seguridad y Ciberseguridad	
Falla de Copias de respaldo de información	
Falta de acuerdos de niveles de servicio con proveedor de tecnología	
Falta de acuerdos de confidencialidad con empleados y proveedores	
Falta de motivación y buen ambiente laboral para los empleados	
Falta de un plan de renovación tecnológica de los equipos de computo y Software	
Falta de Segregación de roles y funciones	
Falta de documentación de los procesos y procedimientos	
Falta de identificación y posterior remediación de vulnerabilidades técnicas	
Esta permitido el uso de equipos portátiles corporativos fuera de la organización.	
Incumplimiento en procedimientos de borrado seguro de equipos corporativos	
Falta de herramienta LDP (Data Loss Prevention)	
Falta de implementación de controles de acceso físicos y lógicos a ambientes	
Falta de parametrización de accesos a los activos en función de perfil de usuario	
Falta de suministros energéticos de contingencia	
Ausencia de planificación, implementación y evaluación del proceso de replicación de datos.	
Ausencia de un plan de continuidad del negocio y plan de recuperación de desastres	
Ausencia de un proceso de administración de riesgos operativos	
No tener ubicado el servidor web en DMZ	
No contar con un sistema de detección y prevención de intrusiones (IDS/IPS)	
No tener actualizadas las firmas de la protección de punto final	
Falta de una herramienta SIEM y SOC que nos ayude con la gestión de incidentes de seguridad y Ciberseguridad	
No se aplica validación de datos en aplicaciones	
No se configuran métodos restrictivos tales como "LIMIT" en las bases de datos	
No supervisar y/o administrar modificaciones automáticas en las aplicaciones	
Generar mensajes de error externos que pueda revelar información sobre el sistema o la estructura de la base de datos utilizada	
Usuario root accesible a través de SSH	
No tener implementadas políticas de contraseñas seguras en las plataformas tecnológicas de la compañía	
No bloquear cuentas después de varios intentos de autenticación fallidos	
No actualizar el Software frecuentemente	

# Modelo de gestión de riesgos



## 4. ESCENARIO DE RIESGOS.

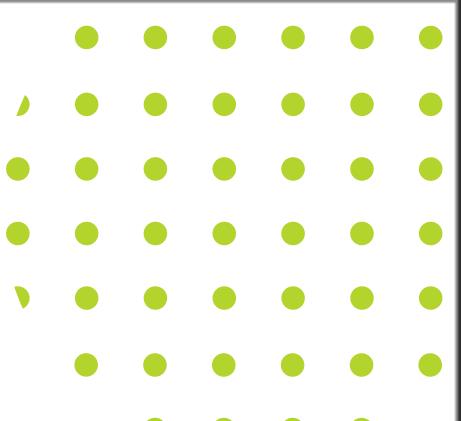
1. Existe un activo de información
2. Existe un factor amenazante para ese activo
3. Existe una vulnerabilidad asociada a ese activo
4. Existe un activo que permita la acción de la amenaza, sabes por qué?

Porque el activo está **vulnerable**

Matriz que incluye los Activos de Información de la Organización. Enfrentado con las amenazas para cada uno de los activos

CARACTERIZACION DE ACTIVOS DE INFORMACIÓN				
Activos de Información	Causas (el porqué [Amenaza])	Descripción general de la Causa	VULNERABILIDAD	Escenario del riesgo
Software	Recuperación de información de medios reciclados	Acceder a la información de manera fraudulenta	incumplimiento en procedimientos de borrado seguro de equipos corporativos	EMPLEADOS no realizan las funciones asignadas y se permite el acceso no permitido a datos de INDEPORTES ANTIOQUIA
Hardware	Hurto o perdida de equipos		Esta permitido el uso de equipos portátiles corporativos fuera de la organización.	Personas no autorizadas acceden a información de INDEPORTES ANTIOQUIA
Información Física/Digital	Fuga de información		Falta de herramienta LDP (Data Loss Prevention)	
Red	Intercepción de información por la red		Falta de una herramienta SIEM y SOC que nos ayuda con la gestión de incidentes de seguridad y Ciberseguridad	INDEPORTES ANTIOQUIA permite ataques informáticos a través de su perímetro
Servicios	Divulgación de información por terceras partes		Falta de acuerdos de confidencialidad con empleados y proveedores	Empleados y proveedores divulan información de INDEPORTES ANTIOQUIA

# Modelo de gestión de riesgos



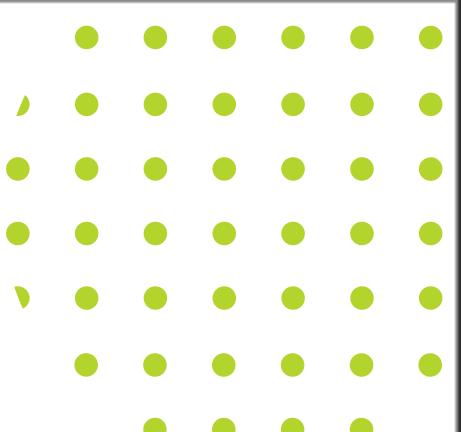
## 5. CRITERIOS DEL RIESGOS

Existen descriptores (1,2,3,4,5) para determinar y calificar:

- Es posible?
- Me impacta?

GESTION DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN			
Probabilidad	Impacto	Objetivo del Control	Control Propuesto
poco frecuente	Insignificante	Controlar el acceso a la información solo a las personas autorizadas para hacerlo.	POLÍTICA DE BORRADO SEGURO POLÍTICA Y PROCEDIMIENTO DE COPIAS DE RESPALDO DE INFORMACIÓN
poco frecuente	Moderado	Controlar el acceso a la información solo a las personas autorizadas para hacerlo.	SEGREGACIÓN DE FUNCIONES Y CONTROLES DE ACCESO POLÍTICA Y PROCEDIMIENTO DE COPIAS DE RESPALDO DE INFORMACIÓN

# Modelo de gestión de riesgos



## 6. CALIFICACIÓN ESCENARIO DE RIESGOS.

PROBABILIDAD  
DE  
OCURRENCIA

IMPACTO EN  
LAS  
OPERACIONES

ESCENARIO	PROBABILIDAD	IMPACTO OPERACIÓN	Riesgo P*Impacto
EVENTO NATURAL -- INFORM. FÍSICA 1	Muy poco probable	1	Sin impacto
EVENTO NATURAL -- INFORM. FÍSICA 2	Muy poco probable	1	Sin impacto
EVENTO NATURAL -- REDES	Poco probable	2	Muy bajo
EVENTO NATURAL -- EQUIPO DE CÓMPUTO	Muy poco probable	1	Muy bajo
PERDIDA DE SERVICIOS ESCENCIALES -- REDES	Poco probable	2	Muy bajo
PERDIDA DE SERVICIOS ESCENCIALES -- SERVIDOR LOCAL	Probable	3	Muy bajo
PERDIDA DE SERVICIOS ESCENCIALES -- EQUIPO DE CÓMPUTO	Probable	3	Muy bajo
FALLAS TECNICAS -- DOMINA DIGITAL F_E	Poco probable	2	Alto
FALLAS TECNICAS -- SOFTWARE GESTION F_E	Poco probable	2	Alto
FALLAS TECNICAS -- REDES	Poco probable	2	Muy bajo
FALLAS TECNICAS -- SERVIDOR LOCAL	Poco probable	2	Muy bajo
FALLAS TECNICAS -- EQUIPO DE CÓMPUTO	Poco probable	2	Muy bajo
FALLAS TECNICAS -- EQUIPO MÓVIL	Poco probable	2	Muy bajo
DAÑO FÍSICO -- INFORM. FÍSICA 1	Muy poco probable	1	Sin impacto
DAÑO FÍSICO -- INFORM. FÍSICA 2	Muy poco probable	1	Sin impacto
DAÑO FÍSICO -- REDES	Muy poco probable	1	Muy bajo
DAÑO FÍSICO -- SERVIDOR LOCAL	Poco probable	2	Muy bajo
DAÑO FÍSICO -- EQUIPO DE CÓMPUTO	Poco probable	2	Muy bajo
DAÑO FÍSICO -- EQUIPO MÓVIL	Poco probable	2	Muy bajo
DAÑO FÍSICO -- ALMACENAMIENTO	Muy poco probable	1	Alto

# Modelo de gestión de riesgos

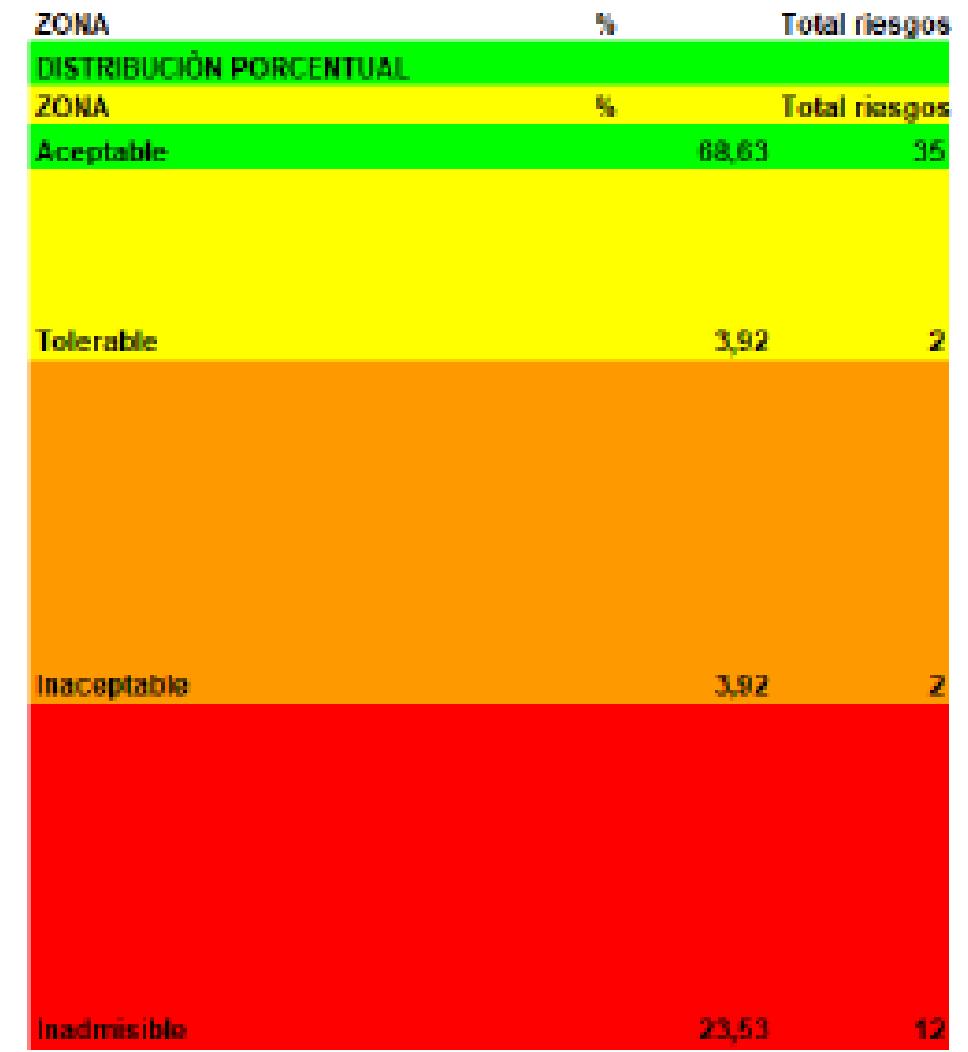
## 7. Mapa de Riesgos

Muestra gráfica del estado de los procesos.

Probabilidad	Impacto	Impacto				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
	valor	1	2	3	4	5
Casi seguro	5					
Probable	4					
Possible	3					
Improbable	2					
Raro	1					

DETALLE DE RIESGOS:

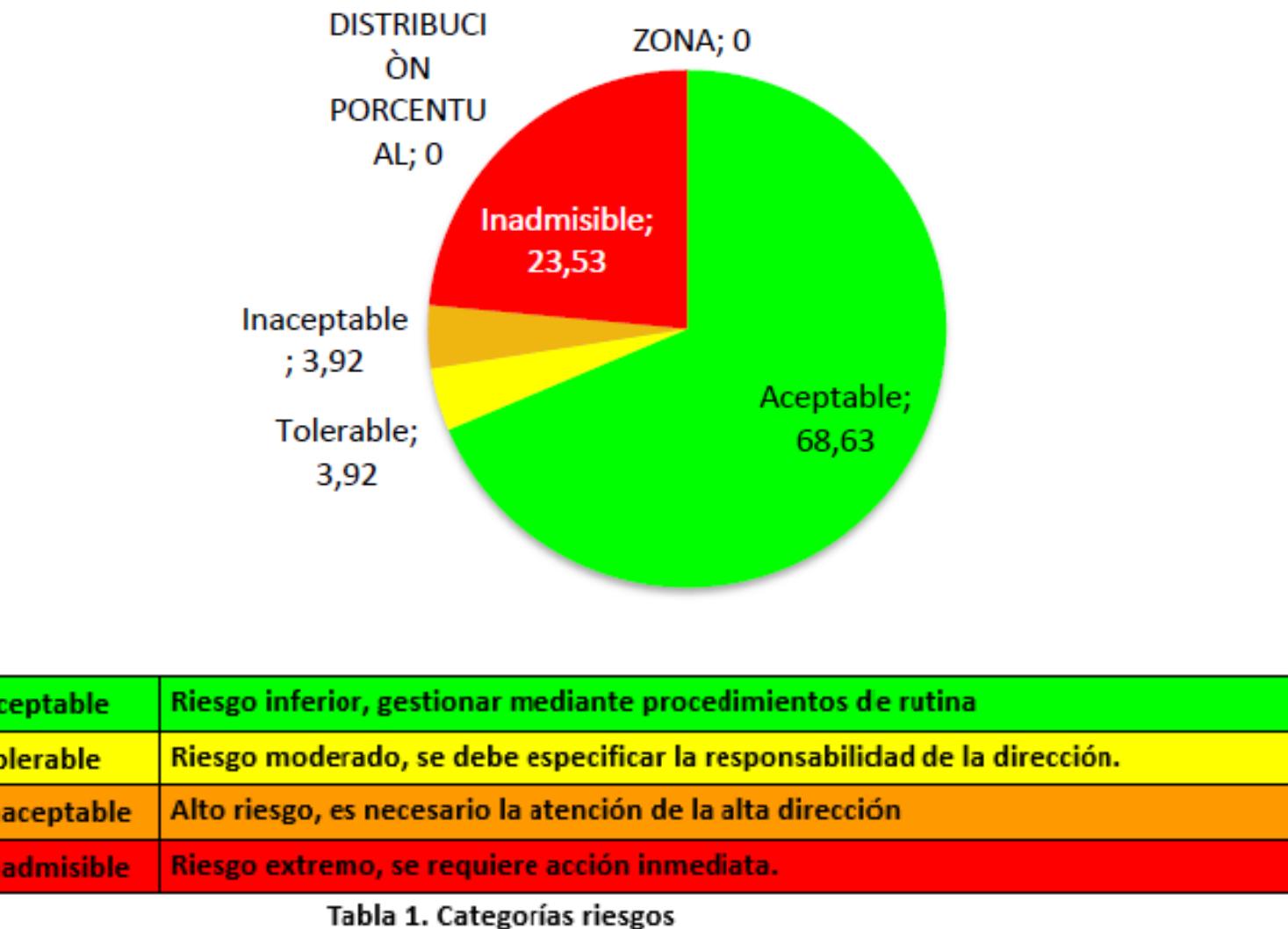
PERDIDA DE SERVICIOS ESCENCIALES -- SERVIDOR LOCAL    PERDIDA DE SERVICIOS ESCENCIALES -- EQUIPO DE CÓMPUTO	ACCIONES NO AUTORIZADAS -- REDES	EVENTO NATURAL -- REDES    PERDIDA DE SERVICIOS ESCENCIALES -- REDES    FALLAS TECNICAS -- REDES    FALLAS TECNICAS -- SERVIDOR LOCAL    FALLAS TECNICAS -- EQUIPO DE COMPUTO    FALLAS TECNICAS -- EQUIPO MÓVIL    DAÑO FÍSICO -- SERVIDOR LOCAL    DAÑO FÍSICO --	DAÑO FÍSICO -- ALMACENAMIENTO    DAÑO FÍSICO -- SERVIDOR F_E	ATAQUES INFORMÁTICOS -- ALMACENAMIENTO    ATAQUES INFORMÁTICOS -- SERVIDOR F_E    ATAQUES INFORMÁTICOS -- CONOCIMIENTO NEGOCIO    COMPROMISO DE LA INFORMACIÓN -- CONOCIMIENTO NEGOCIO	ACCIONES NO AUTORIZADAS -- CONOCIMIENTO NEGOCIO    COMPROMISO DE LA INFORMACIÓN -- DOMINA DIGITAL F_E    COMPROMISO DE LA INFORMACIÓN -- SOFTWARE GESTION F_E	FALLAS TECNICAS -- DOMINA DIGITAL F_E    FALLAS TECNICAS -- SOFTWARE GESTION F_E    PERSONAL NO SATISFECHO -- DOMINA DIGITAL F_E    PERSONAL NO SATISFECHO -- CONOCIMIENTO NEGOCIO
---	----------------------------------	---	--	--	---	--



# Modelo de gestión de riesgos

## 8. Análisis Mapa de Riesgos

La línea punteada demarca la zona de mayor riesgo de cada proceso



# Modelo de gestión de riesgos

Potencial Impacto		
Calificación	Atributo	Descripción
1	Insignificante	Sin perjuicios
2	Menor	Es controlable
3	Moderado	Requiere intervención de terceros
4	Mayor	Pérdida de capacidad , efectos nocivos
5	Catastrófico	Imposibilidad de reacción

Probabilidades de Ocurrencias		
Calificación	Atributo	Descripción
1	Raro	Ocurrencia excepcional
2	Improbable	Difícil que ocurra
3	Possible	Normalmente NO ocurre
4	Probable	Existen razones que creer que ocurrirá
5	Frecuente	Normalmente ocurre

Controles		
Calificación	Atributo	Descripción
1	Incontrolable	Ausencia de control con respecto a la probabilidad de ocurrencia y la posibilidad de gestionar las consecuencias
2	Débil	Controles insuficientes para prevenir o mitigar el riesgo o <b>NO SE CONOCEN</b>
3	Moderado	Los controles <b>NO</b> permiten la gestión de todos los sucesos de riesgos potenciales
4	Fuerte	Los controles económicamente viables se gestionan. Se hace seguimiento y monitoreo

Matriz de Niveles de Riesgos					
Probabilidad de Ocurrencia	Impacto Potencial				
	1	2	3	4	5
5					
4					
3					
2					
1					

# Modelo de gestión de riesgos



## 9. Caracterización y atributos de los Controles

- Código Riesgo
- Categoría
- Nombre del riesgo
- Control
- Tipo de control(Correctivo/ Detectivo)
- Objetivo
- Guía de implementación
- Métricas
- Plan de monitoreo
- Responsable
- Resultado esperado
- Cronograma
- Presupuesto