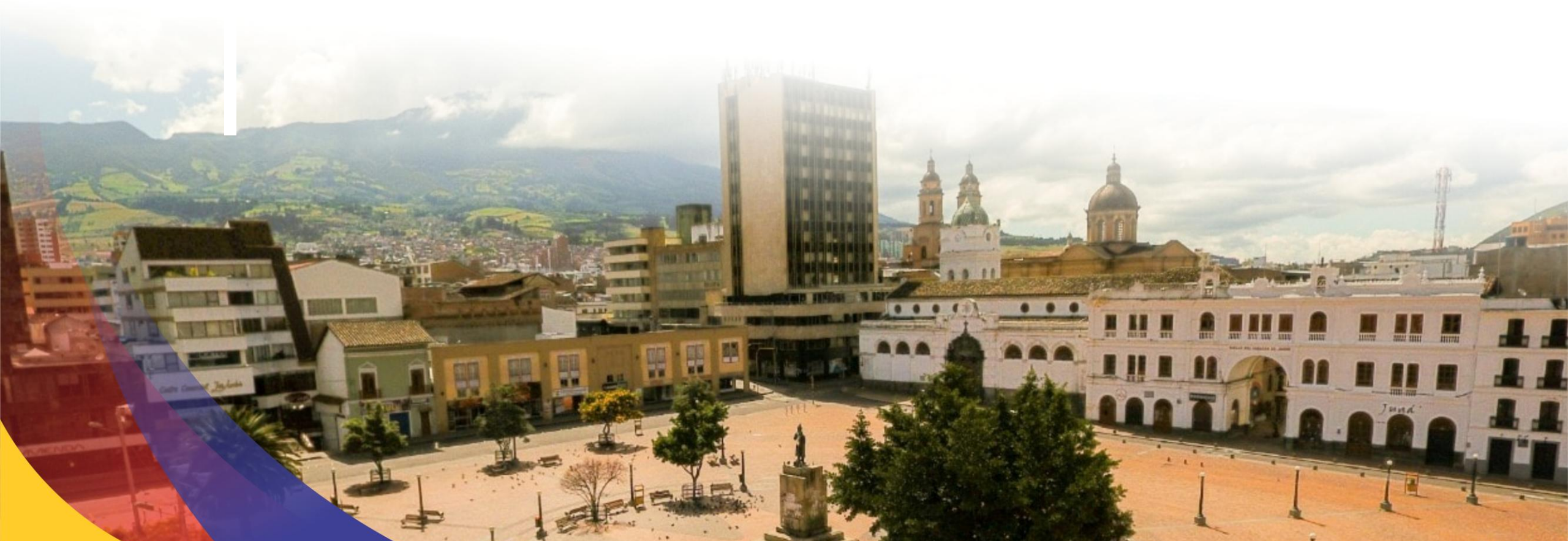
ALCALDÍA
DE PASTO

@AlcaldíaPasto

ALCALDÍA
DE PASTO

RIESGOS PARA LA SEGURIDAD DE LA INFORMACIÓN



RIESGOS PARA LA SEGURIDAD DE LA INFORMACIÓN

Manual de Riesgos — Alcaldía de Pasto | Guía para la Gestión Integral del Riesgo v7 (DAFP), Capítulo V | MSPI · MinTIC

TOLERANCIA: BAJA

ALCALDÍA DE PASTO

¿QUÉ SON?

Eventos que pueden comprometer la confidencialidad, integridad o disponibilidad de los activos de información y datos de los ciudadanos y de la entidad.

SUBCATEGORÍAS DEL RIESGO

Confidencialidad
Acceso no autorizado a información reservada o datos personales.

Integridad
Alteración o manipulación indebida de la información.

Disponibilidad
Interrupción del acceso a los sistemas y servicios.

Ciberseguridad
Ataques externos o internos a la infraestructura digital.

Privacidad
Tratamiento inadecuado de datos personales (Ley 1581 de 2012).

¿QUÉ ES UN ACTIVO DE INFORMACIÓN?

Todo dato, sistema, plataforma digital, base de datos, registro físico o electrónico, infraestructura tecnológica o conocimiento institucional necesario para el cumplimiento de los objetivos de la entidad.

TIPOS DE ACTIVOS DE INFORMACIÓN (Guía GIR v7 – DAFP / MSPI)

- Información y datos
- Sistemas de información / software
- Hardware (TI)
- Soporte de almacenamiento
- Servicios (internet, intranet)
- Recursos humanos
- Instalaciones
- Redes

CLASIFICACIÓN DEL ACTIVO — según Confidencialidad, Integridad y Disponibilidad (ISO/IEC 27001)

ALTA
2 o las 3 propiedades (C-I-D) calificadas en nivel alto.

MEDIA
Una propiedad alta, o al menos una en nivel medio.

BAJA
Las tres propiedades (C-I-D) en nivel bajo.

Marco normativo: Ley 1581 de 2012 · Decreto 1377 de 2013 · Ley 1273 de 2009 · Decreto 1078 de 2015 · ISO/IEC 27001:2022 · MSPI (MinTIC) · Guía GIR v7 – DAFP, Cap. V

DEFINICIÓN

¿Qué son los riesgos de seguridad de la información?

Son los eventos que pueden comprometer la Confidencialidad, la Integridad o la Disponibilidad de los activos de información de la entidad.

Aplican a todos los procesos que gestionen, almacenen, procesen o transmitan información institucional o de los ciudadanos.

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

NIVEL DE TOLERANCIA

BAJO

Todo riesgo residual que supere el nivel Bajo requiere un plan de tratamiento obligatorio.

MARCO NORMATIVO

Normas que sustentan la gestión de este riesgo

Ley 1581 de 2012	Obliga a garantizar confidencialidad, integridad y disponibilidad de las bases de datos con información personal.
Decreto 1377 de 2013	Reglamenta el tratamiento de datos sensibles: salud, menores, datos biométricos y financieros.
Ley 1273 de 2009	Tipifica los delitos informáticos: acceso abusivo, daño informático e interceptación de datos.
Decreto 1078 de 2015 · Gobierno Digital	Lineamientos de seguridad digital: gestión de riesgos, continuidad y respuesta a incidentes.
MSPI — MinTIC	Marco técnico para implementar controles de seguridad basado en ISO/IEC 27001:2022.
Guía GIR v7 — DAFP (2025)	Actualiza el enfoque de riesgo de seguridad digital y los criterios de valoración de activos.

CONCEPTO CLAVE

¿Qué es un activo de información?

Todo dato, sistema, plataforma digital, base de datos, registro físico o electrónico, infraestructura tecnológica y conocimiento institucional necesario para cumplir los objetivos de la entidad.

En una frase:

si tiene valor para la entidad, es necesario para su operación y debe protegerse — es un activo de información.

- Una base de datos de ciudadanos
- Un servidor o equipo de cómputo crítico
- El conocimiento de un proceso clave en un manual

CLASIFICACIÓN POR TIPO

Tipos de activos de información

ALCALDÍA DE PASTO

1

Información y datos

Bases de datos, contratos, manuales, procedimientos, auditorías.

2

Software y aplicaciones

Software de aplicación, sistemas de información, herramientas de desarrollo.

3

Hardware — dispositivos TI

Equipos de cómputo críticos para la operación de la entidad.

4

Soportes de almacenamiento

USB, discos duros, CD, SAN, NAS.

5

Servicios

Internet, páginas de consulta, directorios compartidos, intranet.

6

Recursos humanos

Personas que producen, custodian o usan la información.

7

Instalaciones

Espacios físicos donde se procesa o resguarda información.

8

Redes

Infraestructura de comunicaciones y conectividad.

Pasos para identificar y valorar los activos

ALCALDÍA DE PASTO

PASO 1

Listar los activos por cada proceso

PASO 2

Identificar el dueño y el custodio del activo

PASO 3

Clasificar los activos por tipo (hardware, software, etc.)

PASO 4

Clasificar la información

PASO 5

Determinar la criticidad del activo

PASO 6

Identificar si hay Infraestructura Crítica Cibernética Nacional

VALORACIÓN DEL ACTIVO

De la Confidencialidad, Integridad y Disponibilidad a la Criticidad

ALCALDÍA DE PASTO

Cada activo se valora en tres propiedades, cada una en nivel Alta, Media o Baja. El resultado define la criticidad del activo.

Confidencialidad

Información Pública Reservada / Clasificada / Pública

Integridad

Alta (A) · Media (M) · Baja (B)

Disponibilidad

Alta (1) · Media (2) · Baja (3)

NIVEL DE CRITICIDAD RESULTANTE

ALTA	2 o las 3 propiedades en nivel alto
MEDIA	1 propiedad alta, o al menos una media
BAJA	Todas las propiedades en nivel bajo

DIMENSIÓN	PREGUNTA QUE DEBO HACERME	NIVEL	¿QUÉ SIGNIFICA?	EJEMPLO
CONFIDENCIALIDAD	**¿Quién puede ver la información?**	**Información Pública Reservada**	Su acceso está restringido por una razón establecida legalmente.	Información de una investigación con acceso restringido.
CONFIDENCIALIDAD	**¿Quién puede ver la información?**	**Información Pública Clasificada**	Es pública, pero contiene información que debe protegerse, como ciertos datos personales.	Base de datos con nombres, documentos y teléfonos personales.
CONFIDENCIALIDAD	**¿Quién puede ver la información?**	**Información Pública**	Puede ser conocida y consultada por cualquier ciudadano.	Horarios de atención, informes publicados, noticias.
CONFIDENCIALIDAD	**¿Quién puede ver la información?**	**No clasificada**	No tiene una clasificación asignada dentro del esquema.	Información pendiente de clasificación.
INTEGRIDAD	**¿Qué pasa si alguien modifica la información?**	**Alta (A)**	Una modificación incorrecta puede generar consecuencias graves.	Datos de nómina, valores de contratos o información financiera crítica.
INTEGRIDAD	**¿Qué pasa si alguien modifica la información?**	**Media (M)**	Una modificación puede generar inconvenientes importantes, pero no críticos.	Cronograma de actividades de una dependencia.
INTEGRIDAD	**¿Qué pasa si alguien modifica la información?**	**Baja (B)**	Una modificación tendría consecuencias menores.	Material informativo de apoyo.
INTEGRIDAD	**¿Qué pasa si alguien modifica la información?**	**No clasificada**	No se ha determinado el nivel de impacto de una modificación.	Información pendiente de valoración.
DISPONIBILIDAD	**¿Qué pasa si no puedo acceder a la información cuando la necesito?**	**Alta (1)**	No disponer de ella puede generar consecuencias graves.	Sistema necesario para una operación crítica.
DISPONIBILIDAD	**¿Qué pasa si no puedo acceder a la información cuando la necesito?**	**Media (2)**	No disponer de ella genera inconvenientes, pero puede esperarse o recuperarse.	Informe mensual de seguimiento.
DISPONIBILIDAD	**¿Qué pasa si no puedo acceder a la información cuando la necesito?**	**Baja (3)**	Que no esté disponible genera poco impacto.	Documento histórico que se consulta ocasionalmente.
DISPONIBILIDAD	**¿Qué pasa si no puedo acceder a la información cuando la necesito?**	**No clasificada**	No se ha determinado su nivel de disponibilidad.	Información pendiente de valoración.

ACTIVO	TIPO	¿QUÉ ES?	EJEMPLO
Base de datos de beneficiarios	**Primario**	Información que tiene valor directo para la entidad	Datos de beneficiarios
Información de nómina	**Primario**	Información necesaria para cumplir una función	Salarios y pagos
Presupuesto municipal	**Primario**	Información fundamental para la gestión	Presupuesto aprobado
Expediente contractual	**Primario**	Información que soporta directamente un proceso	Contrato y documentos asociados
Servidor	**Secundario**	Infraestructura que almacena/procesa información	Servidor institucional
Base de datos	**Secundario**	Tecnología que almacena información	Base de datos SQL
Sistema de información	**Secundario**	Aplicación que permite gestionar información	Sistema financiero
Computador	**Secundario**	Equipo utilizado para acceder/procesar información	PC de funcionario
Red institucional	**Secundario**	Permite transportar/comunicar información	Red de la Alcaldía
Sistema de copias de seguridad	**Secundario**	Permite respaldar y recuperar información	Backup institucional

SUBCATEGORÍAS DEL RIESGO

Cinco formas en que se materializa el riesgo

Confidencialidad	Integridad	Disponibilidad	Ciberseguridad	Privacidad de la información
Acceso no autorizado a información reservada o datos personales por personal no habilitado.	Alteración o manipulación dolosa o accidental de información institucional o de ciudadanos.	Interrupción o pérdida de acceso a sistemas que afecta la prestación del servicio.	Ataques externos (ransomware, phishing, DDoS) o internos a la infraestructura digital.	Tratamiento inadecuado de datos personales, en contravención de la Ley 1581 de 2012.

FACTORES DE RIESGO

Amenazas y vulnerabilidades

AMENAZA

Causa potencial de un incidente no deseado que puede provocar daño a un sistema o a la organización.

- Daño físico
- Eventos naturales
- Pérdida de servicios esenciales
- Compromiso de la información
- Fallas técnicas
- Acciones no autorizadas

VULNERABILIDAD

Debilidad de un activo o control que puede ser explotada por una o más amenazas.

- Hardware
- Software
- Red
- Personal
- Lugar (instalaciones)
- Organización

La amenaza es la causa inmediata; la vulnerabilidad es la causa raíz que la hace posible.

Controles para mitigar los riesgos

Preventivo	**Automático**	El sistema restringe el acceso a módulos críticos tras 3 intentos fallidos y alerta al administrador.
Preventivo	**Manual**	Se validan trimestralmente los perfiles de acceso a los sistemas de información.
Detectivo	**Automático**	El sistema de monitoreo genera alertas ante accesos fuera de horario o desde ubicaciones atípicas.
Detectivo	**Manual**	Se revisan mensualmente los logs de acceso a los sistemas críticos.
Correctivo	**Manual**	Se activa el protocolo de respuesta a incidentes en máximo 4 horas ante una brecha de datos.

SEGUIMIENTO

Indicadores clave de riesgo (KRI)

Indicador	Frecuencia	Responsable	Umbral de alerta
Índice de incidentes de seguridad reportados	Mensual	Jefe TIC	Rojo: > 1 incidente en sistemas críticos
% de cuentas de usuario sin auditoría de perfil	Trimestral	Jefe TIC	Amarillo: > 10% · Rojo: > 20%
Cobertura de copias de respaldo (backups)	Mensual	Jefe TIC	Amarillo: < 90% · Rojo: < 80%
Tiempo promedio de atención de incidentes	Trimestral	Jefe TIC	Amarillo: > 8 h · Rojo: > 24 h
% de servidores capacitados en seguridad digital	Semestral	TH / TIC	Amarillo: < 80% · Rojo: < 60%

ALCALDÍA
DE PASTO

GRACIAS

@AlcaldíaPasto