Gestión del Riesgo de Seguridad de la Información - ISO 27001:2022
Indeportes Antioquia

Fecha de elaboración: enero 2026

1. Introducción

En la era de la Cuarta Revolución Industrial, la gestión de la información ha dejado de ser una tarea técnica de soporte para convertirse en la columna vertebral de la administración pública. Para **Indeportes Antioquia**, como ente rector del deporte, la educación física y la recreación en el departamento, la información no es solo un conjunto de datos; es el historial de vida de nuestros atletas, el soporte de la ejecución presupuestal y el motor de la transparencia institucional.

El presente documento, titulado **" Gestión del Riesgo de Seguridad de la Información"**, surge como una respuesta proactiva a las amenazas crecientes en el ciberespacio. Su implementación busca garantizar que los procesos misionales, como el fomento deportivo y la alta competencia, operen sobre una infraestructura resiliente, capaz de resistir incidentes y proteger la privacidad de los ciudadanos.

Fundamentos de la Gestión del Riesgo

La Tríada de la Seguridad de la Información

Todo el esfuerzo de este documento se orienta a proteger tres propiedades fundamentales de la información en Indeportes:

- **Confidencialidad:** Garantizar que la información sea accesible solo para quienes están autorizados (ej. historias clínicas de deportistas).
- **Integridad:** Salvaguardar la exactitud y completitud de los datos, evitando modificaciones no autorizadas (ej. registros de nómina o contratos).
- **Disponibilidad:** Asegurar que los sistemas y datos estén listos para ser usados cuando la entidad lo requiera (ej. plataforma de inscripción a eventos).

Filosofía del Riesgo: De lo Reactivo a lo Preventivo

Tradicionalmente, la seguridad de la información se veía como una respuesta a fallos (instalar un antivirus tras un virus). Este documento propone un cambio de paradigma basado en la **prevención**. Mediante la identificación de amenazas (como el *phishing* o desastres naturales) y vulnerabilidades (como software sin actualizar), Indeportes puede anticiparse a los hechos.

Compromiso de la Alta Dirección

La implementación exitosa de la gestión del riesgo requiere el respaldo absoluto de la Gerencia. La seguridad de la información no es un gasto, sino una inversión en estabilidad. Este documento define las responsabilidades de cada funcionario, estableciendo que la seguridad es una cultura institucional donde cada miembro de Indeportes actúa como la primera línea de defensa contra los riesgos digitales.

Para que el documento de **Gestión del Riesgo de Seguridad de la Información** de **Indeportes Antioquia** tenga validez técnica y sea auditable, los objetivos deben estar redactados bajo la metodología SMART (Específicos, Medibles, Alcanzables, Relevantes y con un tiempo definido).

2. Objetivo General

Establecer y formalizar el marco metodológico para la identificación, análisis, evaluación y tratamiento de los riesgos asociados a los activos de información en **Indeportes Antioquia**, con el fin de fortalecer la toma de decisiones estratégicas, garantizar la continuidad de los procesos misionales y asegurar el cumplimiento de los pilares de confidencialidad, integridad y disponibilidad de la información bajo los estándares de la norma ISO/IEC 27005 y la Política de Gobierno Digital y su componente habilitador seguridad y privacidad de la información.

Objetivos Específicos

2.1. Identificar y valorar los activos de información institucionales (físicos, digitales y humanos), estableciendo su nivel de criticidad para la entidad según su impacto en los procesos misionales, administrativos y de apoyo.

2.2. Identificar las amenazas y vulnerabilidades que afectan el entorno tecnológico y operativo de la entidad, permitiendo anticipar escenarios de riesgo que puedan comprometer la seguridad de los datos de deportistas, funcionarios y contratistas.

2.3. Determinar el nivel de riesgo inherente y residual de los activos mediante una metodología de análisis cualitativa y cuantitativa, facilitando la construcción de una matriz de riesgos priorizada que guíe la inversión en seguridad.

2.4. Definir e implementar planes de tratamiento de riesgos que incluyan controles técnicos, administrativos y físicos, con el objetivo de mitigar, transferir, evitar o aceptar los riesgos de acuerdo con el apetito de riesgo definido por la Alta Dirección.

2.5. Fomentar una cultura de seguridad digital en todos los niveles de Indeportes Antioquia, mediante programas de sensibilización y capacitación que reduzcan el riesgo asociado al factor humano y al uso inadecuado de las herramientas tecnológicas.

2.6. Establecer mecanismos de monitoreo y revisión continua del perfil de riesgo institucional, asegurando que los controles implementados sean efectivos y que el modelo se adapte a las nuevas ciber amenazas y cambios en el entorno normativo.

3. Marco Legal Aplicable y Consecuencias

La Gestión del Riesgo de Seguridad de la Información en la entidad no es una actividad discrecional; se fundamenta en un complejo entramado normativo que busca proteger el interés público y los derechos ciudadanos.

3.1. Marco Legal Nacional y Específico

Norma	Descripción y Aplicación en Indeportes
Constitución Política (Art. 15)	Define el derecho al **Habeas Data**. Obliga a la entidad a conocer, actualizar y rectificar la información recogida en sus bases de datos.
Ley 1581 de 2012	**Ley General de Protección de Datos Personales.** Es la base para el tratamiento de datos de deportistas, menores de edad y contratistas.
Ley 1712 de 2014	**Ley de Transparencia y del Derecho de Acceso a la Información.** Define qué información es pública y cuál es reservada o clasificada.
Ley 1273 de 2009	**Ley de Delitos Informáticos.** Establece penas por el acceso abusivo a sistemas, interceptación de datos y daño informático.
Decreto 1078 de 2015	Reglamenta el sector de las TIC. Establece los lineamientos de la **Política de Gobierno Digital** y el Modelo de Seguridad y Privacidad (MSPI).
Resolución 500 de 2021 (MinTIC)	Define los lineamientos mínimos de seguridad y privacidad que deben cumplir las entidades públicas.
Resolución 746 de 2022 (MinTIC)	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución número 500 de 2021.
Circular Externa 002 (SIC)	Instrucciones sobre medidas de seguridad, reporte de incidentes y debida diligencia en el tratamiento de datos.
Resolución 2025000825	Por medio de la cual se adopta la política de estándares de seguridad de la información y uso de recursos informáticos en Indeportes Antioquia
Resolución 2025000814	Por medio de la cual se adopta actualización a la de política de protección y tratamiento de datos personales en Indeportes Antioquia.
NTC ISO 27001:2022	Norma técnica requisitos para la implementación del sistema de gestión de seguridad de la información, ciberseguridad y protección a la privacidad.
NTC ISO 27005:2022	Norma técnica para la gestión de riesgos de seguridad de la información
NTC ISO 31000:2018	Norma técnica para directrices de gestión del riesgo

3.2. Consecuencias de la No Implementación

La omisión en la gestión de riesgos de seguridad conlleva impactos en tres dimensiones fundamentales para un organismo público:

a. **Consecuencias Administrativas y Financieras**

- ✓ **Multas de la SIC:** La Superintendencia de Industria y Comercio puede imponer multas de hasta **2.000 salarios mínimos mensuales legales vigentes (SMMLV)** por vulneraciones a la Ley 1581.
- ✓ **Cierre de Operaciones:** En casos extremos, se puede ordenar la suspensión del tratamiento de datos, lo que paralizaría procesos como la contratación o el pago a ligas deportivas.
- ✓ **Indemnizaciones:** Demandas de responsabilidad civil por parte de ciudadanos cuyos datos hayan sido filtrados o mal utilizados.

b. **Consecuencias Disciplinarias y Penales**

- ✓ **Sanciones de la Procuraduría:** El incumplimiento de las directrices de Gobierno Digital (MIPG) constituye una falta disciplinaria para el representante legal y el jefe de la oficina de TI, que puede derivar en **suspensión o destitución e inhabilidad**.
- ✓ **Procesos Penales:** En caso de fuga de información por dolo o negligencia grave, los implicados pueden enfrentar penas de prisión por delitos como "Violación de datos personales" (Art. 269F del Código Penal).

c. **Impacto Institucional y Reputacional**

- ✓ **Pérdida de Confianza:** La filtración de historias clínicas de deportistas de alto rendimiento o datos de menores de edad genera un daño irreparable a la imagen de Indeportes y la Gobernación de Antioquia.
- ✓ **Afectación al FURAG:** Una baja calificación en la dimensión de TI del Modelo Integrado de Planeación y Gestión (MIPG) afecta el ranking nacional de la entidad y su capacidad de gestión de recursos.

3.3. Responsabilidad Solidaria

Es imperativo recordar que, en Indeportes Antioquia, la responsabilidad por la seguridad de la información es **solidaria**. Esto significa que tanto el personal de planta como los contratistas de prestación de servicios están sujetos a este marco legal, y el desconocimiento de la norma no exime de su cumplimiento.

4. Metodología para la Gestión del Riesgo (Interpretación de la Matriz)

La metodología adoptada por **Indeportes Antioquia** se basa en un análisis semicuantitativo que evalúa la probabilidad de ocurrencia y el impacto de las amenazas sobre los activos de información.

4.1. Criterios de Calificación de Probabilidad (Frecuencia)

La probabilidad mide la posibilidad de que una amenaza aproveche una vulnerabilidad existente en los activos de información de la entidad. Se asigna un valor numérico (peso) que será fundamental para el cálculo del riesgo inherente.

4.1.1. Tabla de Escalas de Probabilidad

De acuerdo con la metodología establecida en la **Matriz de Riesgo de seguridad de la información**, se definen los siguientes cinco niveles de frecuencia:

Nivel de Probabilidad	Descripción de la Frecuencia	Peso (Valor)	Interpretación Técnica
Muy Baja	La actividad que conlleva el riesgo se ejecuta como **máximo 2 veces por año**.	**0.2**	Evento altamente inusual o excepcional.
Baja	La actividad que conlleva el riesgo se ejecuta de **3 a 24 veces por año**.	**0.4**	Actividades de periodicidad mensual o bimensual.
Media	La actividad que conlleva el riesgo se ejecuta de **24 a 500 veces por año**.	**0.6**	Actividades de frecuencia semanal o diaria moderada.
Alta	La actividad se ejecuta entre **500 y 5.000 veces por año**.	**0.8**	Actividades constantes y repetitivas durante la jornada.
Muy Alta	La actividad que conlleva el riesgo se ejecuta **más de 5.000 veces por año**.	**1.0**	Procesos automatizados o transacciones masivas continuas.

4.1.2. Factores para la Determinación de la Probabilidad

Para asignar uno de los niveles anteriores en la matriz, el analista de riesgos de Indeportes debe considerar los siguientes factores:

1. **Volumen de Transacciones:** Cuantas más veces se procese un dato (ej. registros en **SICOF** o inscripciones en **HÉRCULES**), mayor es la exposición y, por ende, su frecuencia.
2. **Exposición del Activo:** Un activo expuesto a internet (portal web) tiene una frecuencia de amenaza superior a un activo en la red local (servidor de archivos interno).
3. **Histórico de Incidentes:** Se deben revisar los logs de la Mesa de Ayuda y de Seguridad para verificar si la amenaza se ha materializado previamente en periodos similares.
4. **Complejidad de la Tarea:** Actividades manuales ejecutadas con alta frecuencia tienen una probabilidad de error humano superior a los procesos automatizados.

4.1.3. Aplicación en la Matriz

En la columna **"% Probabilidad inherente"** de la matriz de Indeportes, se debe seleccionar el peso correspondiente (0.2 a 1.0). Este valor, al multiplicarse por el peso del **Impacto**, determinará si el riesgo se ubica en una zona **Baja, Moderada, Alta o Extrema**.

Ejemplo de Aplicación:

Si estamos evaluando el riesgo de "Acceso no autorizado a la base de datos de deportistas" y el sistema recibe consultas 100 veces al día (aprox. 24.000 al año), la probabilidad debe calificarse como Muy Alta (1.0) debido a la altísima frecuencia de la actividad.

4.2. Criterios de Calificación de Impacto

El impacto representa la magnitud del daño o las consecuencias negativas sobre los activos de información y los procesos de la entidad. Se califica en una escala de 1 a 5, donde cada nivel tiene un peso porcentual que influye directamente en el cálculo del riesgo.

4.2.1. Dimensiones de Valoración del Impacto

La entidad evalúa el impacto bajo dos criterios principales. En caso de que un riesgo afecte ambas dimensiones de forma distinta, se debe seleccionar el nivel de impacto **más alto** alcanzado.

Nivel de Impacto	Peso (Valor)	Criterio de Afectación Económica (SMLMV)	Criterio de Afectación Reputacional
Leve	**0.2**	Afectación menor a 10 $SMLMV$.	El riesgo afecta la imagen de algún área específica de la organización sin trascender al resto de la entidad.
Menor	**0.4**	Entre 10 y 50 $SMLMV$.	Afecta la imagen interna, siendo de conocimiento general para funcionarios, Junta Directiva y proveedores.
Moderado	**0.6**	Entre 50 y 100 $SMLMV$.	Afecta la imagen de la entidad ante usuarios de relevancia o grupos de interés vinculados al logro de objetivos.
Mayor	**0.8**	Entre 100 y 500 $SMLMV$.	Efecto publicitario negativo y sostenido a nivel del sector administrativo, departamental o municipal.
Catastrófico	**1.0**	Mayor a 500 $SMLMV$.	Afectación de la imagen a nivel nacional, con efecto publicitario crítico y sostenido en medios de comunicación del país.

4.2.2. Aplicación de los Criterios en la Evaluación

Para determinar el impacto en la matriz, el responsable debe analizar las siguientes variables adicionales:

- ✓ **Criterio Legal y de Cumplimiento:** Se considera el nivel de las sanciones que podrían imponer entes de control (SIC, Procuraduría, Contraloría). Una multa de la SIC por incumplimiento de la Ley 1581 de 2012 suele clasificarse como impacto **Mayor** o **Catastrófico** debido a su cuantía.
- ✓ **Criterio Operativo:** Se evalúa cuánto tiempo tardaría la entidad en recuperar su operación normal.
- ✓ *Leve:* Interrupción de minutos.
- ✓ *Catastrófico:* Pérdida total de bases de datos misionales sin posibilidad de recuperación inmediata.
- ✓ **Criterio de Información (Privacidad):**
- ✓ Si se filtran datos públicos: Impacto **Leve/Menor**.
- ✓ Si se filtran datos sensibles o de menores de edad (deportistas): Impacto **Mayor/Catastrófico**.

4.2.3. Cálculo del Riesgo Inherente

Una vez definida la **Probabilidad (P)** (punto 4.1) y el **Impacto (I)** (punto 4.2), la entidad obtiene el nivel de riesgo mediante la fórmula:

Riesgo Inherente = Probabilidad \Impacto
Este resultado determinará la ubicación del riesgo en la **Matriz de Calor**, clasificándolo en las zonas de severidad: **Bajo, Moderado, Alto o Extremo**.

Ejemplo de Aplicación:

Un riesgo con probabilidad Media (0.6) e impacto Moderado (0.6) daría un resultado de 0.36. Según la escala de la entidad (donde0.6 \ 0.6 se cruza en la matriz), este riesgo se clasificaría como Moderado, requiriendo acciones de control preventivo.

4.3. Matriz de Calor y Niveles de Severidad

Cruzando la Probabilidad (P) y el Impacto (I), se determina la **Zona de Riesgo**. Según los datos del archivo, los niveles de severidad se definen así:

- ✓ **BAJO:** Riesgo tolerable. Se aceptan con monitoreo periódico.
- ✓ **MODERADO:** Requiere atención y definición de controles preventivos.
- ✓ **ALTO:** Riesgo significativo; exige implementación de controles de seguridad inmediatos.
- ✓ **EXTREMO:** Riesgo crítico; requiere intervención inmediata de la Gerencia y planes de contingencia urgentes.

4.4. Evaluación de Controles y Riesgo Residual

La metodología interpretada del anexo permite pasar del **Riesgo Inherente** (sin controles) al **Riesgo Residual** (con controles) evaluando los controles bajo los siguientes atributos:

1. **Tipo de Control:** Preventivo, Detectivo o Correctivo.
2. **Implementación:** Si el control está documentado, si se aplica con frecuencia y si existe evidencia de su ejecución.
3. **Calificación del Control:** Se resta el valor de la efectividad del control al riesgo inherente para obtener la zona de riesgo final.

4.5. Tratamiento del Riesgo

Una vez evaluada la severidad del riesgo (Bajo, Moderado, Alto o Extremo), la Oficina de TIC y el Comité de Riesgos de la entidad deben seleccionar una de las cuatro estrategias de tratamiento. Esta decisión busca llevar el riesgo a un nivel **Residual** que la entidad esté dispuesta a tolerar.

4.5.1. Estrategias de Tratamiento en Indeportes

- ✓ **Reducir (Mitigar):** Es la estrategia principal para riesgos **Altos o Extremos** (ej. *Pérdida de expedientes de Acciones de Tutela*). Consiste en aplicar controles del **Anexo A de la ISO 27001** para disminuir la probabilidad o el impacto.
- ✓ **Adaptación a la realidad:** Para el riesgo de "Acceso no autorizado a información fiscal", Indeportes aplica controles de **Clasificación (A.5.7)** y **Respaldos (A.8.13)**. La efectividad aumenta si el control es **Preventivo y Automático** (ej. cifrado automático de bases de datos) en lugar de manual.
- ✓ **Compartir (Transferir):** Se utiliza cuando el impacto financiero es muy alto o la entidad no tiene la capacidad técnica para mitigar el riesgo por sí sola.
- ✓ **Adaptación a la realidad:** El alojamiento de la plataforma **HÉRCULES** en la nube de un tercero especializado transfiere la responsabilidad de la disponibilidad física y la seguridad del centro de datos al proveedor, bajo estrictos Acuerdos de Nivel de Servicio (SLA).
- ✓ **Evitar:** Implica eliminar la causa del riesgo mediante el cambio o la supresión de un proceso.
- ✓ **Adaptación a la realidad:** Ante el riesgo de "Deterioro físico de documentos legales por incendio", la entidad opta por **Evitar** el almacenamiento físico prolongado, migrando hacia expedientes 100% digitales con firmas electrónicas y custodia en repositorios seguros.
- ✓ **Aceptar (Asumir):** Se aplica únicamente a riesgos en zona **Baja** o donde el costo del control supera el beneficio.
- ✓ **Adaptación a la realidad:** Pequeños retrasos en la actualización de información no crítica en el portal web pueden ser aceptados, siempre que no afecten los pilares de transparencia o legalidad.

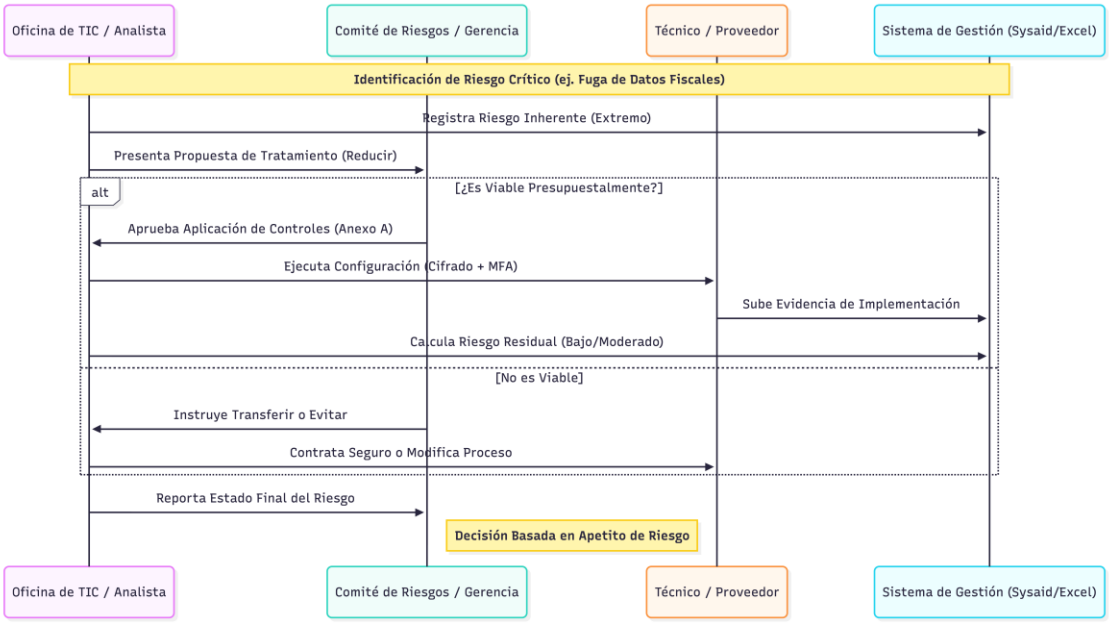
4.5.2. Cálculo de la Efectividad del Control

Según la metodología interna de Indeportes, la capacidad de un control para reducir el riesgo depende de sus atributos. Un tratamiento es más efectivo si cumple con:

- ✓ **Tipo de Control:** Preferencia por **Preventivo** (Peso 0.25) sobre Correctivo (0.1).
- ✓ **Implementación:** Preferencia por **Automático** (0.25) sobre Manual (0.1).
- ✓ **Cualidades:** El control debe estar **Documentado**, tener una **Frecuencia** definida y contar con **Evidencia** de ejecución para ser considerado válido en la auditoría del FURAG.

Diagrama de Secuencia: Proceso de Tratamiento del Riesgo

Este diagrama representa el flujo de decisión desde que se detecta un riesgo crítico hasta que se verifica la efectividad de la solución.



Interpretación del Diagrama:

- ✓ **Validación de Viabilidad:** Refleja la realidad administrativa donde la Gerencia debe autorizar recursos para controles de alto costo.
- ✓ **Evidencia de Implementación:** Clave para los procesos de calidad y control interno de la entidad.
- ✓ **Ciclo de Cierre:** El riesgo no desaparece, se transforma en un "Riesgo Residual" que debe seguir siendo monitoreado.

5. Controles de Seguridad (Basados en el Anexo A de ISO 27001)

Los controles son las salvaguardas que reducen la probabilidad de ocurrencia o el impacto de una amenaza. En la entidad, estos se dividen en cuatro categorías principales según el nuevo marco de la norma.

5.1. Controles Organizacionales y de Clasificación

Estos controles establecen el "quién", el "qué" y el "cómo" se maneja la información en Indeportes, transformando el manejo empírico en un proceso estandarizado y auditable.

5.1.1. A.5.7 Clasificación de la Información (El "Qué")

La matriz de riesgos identifica como causa raíz la *"Falta de clasificación de confidencialidad"*. Para mitigar el riesgo de divulgación no autorizada de expedientes judiciales o información tributaria, Indeportes adopta el siguiente esquema de etiquetado:

- ✓ **Información Pública:** Datos que por ley deben estar disponibles (Calendarios de eventos deportivos, resoluciones de presupuesto público, resultados de competencias). Su pérdida de confidencialidad tiene impacto **Leve**.
- ✓ **Información Interna:** Documentación técnica de uso exclusivo de funcionarios (Manuales de procesos de la Subgerencia Administrativa, guías de entrenamiento). Su divulgación genera impacto **Moderado**.
- ✓ **Información Confidencial (Nivel Crítico):**
- ✓ **Expedientes de Acciones Constitucionales:** Contienen datos sensibles de ciudadanos y atletas (Tutelas, historias clínicas,Acciones de Grupo).
- ✓ **Información Fiscal:** Declaraciones, cuentas de cobro y soportes de pago que, según la matriz, presentan riesgo de *"alteración o error afectando la exactitud de las declaraciones"*.
- ✓ **Datos de Menores de Edad:** Información de niños en programas de fomento deportivo.

Acción de Control: Todo archivo digital en la red de Indeportes o soporte físico debe llevar un metadato o sello de clasificación. Si un documento no está clasificado, se tratará por defecto como **Interno**.

5.1.2. A.5.15 Control de Acceso (El "Quién")

La vulnerabilidad detectada de *"Accesos amplios a información fiscal"* y *"Control de acceso débil"* exige una transición hacia un modelo basado en **Roles y Privilegios Mínimos**.

- ✓ **Principio de "Necesidad de Conocer":** Ningún funcionario de la Subgerencia Técnica tendrá acceso a los expedientes de la Oficina Jurídica, a menos que esté formalmente asignado a un caso.
- ✓ **Segregación de Funciones en Sistemas:** En herramientas como **SICOF** y **MERCURIO**, quien registra una obligación financiera no puede ser el mismo que autoriza el pago. Esto reduce el riesgo de *"Pérdida o alteración de evidencias de cumplimiento"*.
- ✓ **Revisión de Privilegios:** La Oficina de TIC realizará una auditoría trimestral de los usuarios con acceso a la información clasificada como **Confidencial**, eliminando accesos de personal que haya cambiado de cargo o terminado su contrato.

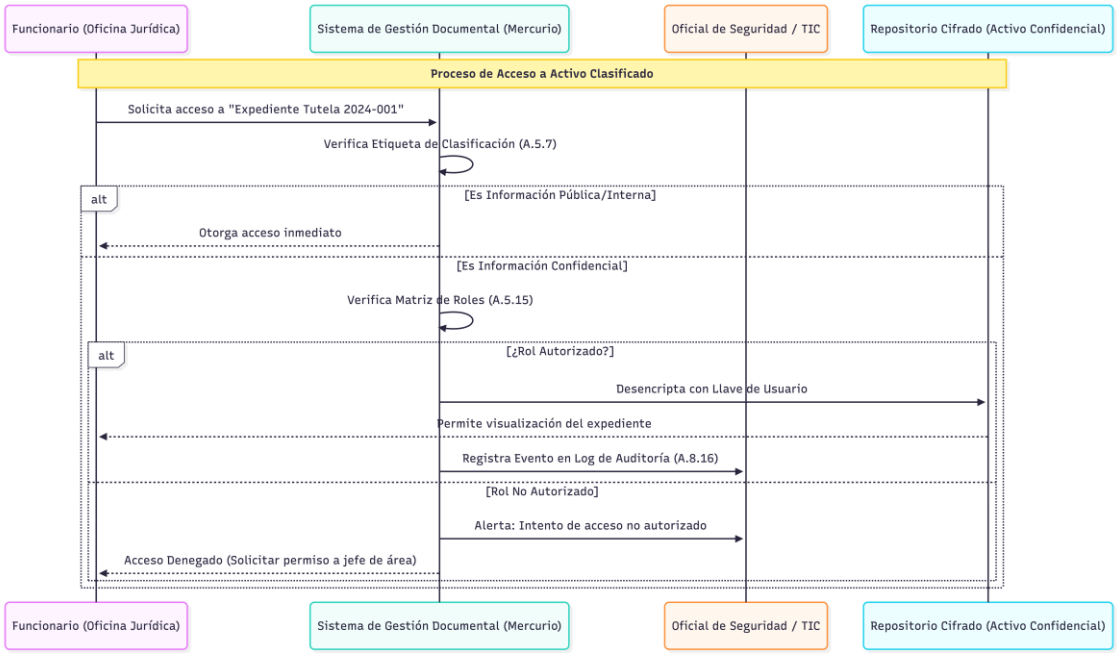
5.1.3. A.5.10 Uso Aceptable de Activos de Información

Dado que la matriz menciona la *"Dispersión de soportes digitales y físicos"*, se establece que la única ubicación autorizada para el almacenamiento de información misional es el servidor institucional o la nube oficial (OneDrive/SharePoint de la Gobernación). Queda prohibido el uso de memorias USB personales o servicios de almacenamiento gratuito para documentos de **Acciones Populares o Fiscales**.

Diagrama de Secuencia: Ciclo de Clasificación y Control de Acceso

Este diagrama representa cómo se procesa una solicitud de acceso a un activo crítico (ej. Expediente de Tutela) bajo los nuevos controles de seguridad.

Fragmento de código



La trazabilidad asegura cumplimiento ante la SIC y MinTIC

Beneficios de este flujo para Indeportes:

1. **Protección Legal:** Asegura que solo los abogados encargados vean las acciones de tutela, mitigando multas de la SIC.
2. **Reducción del Riesgo Residual:** Al automatizar la verificación de roles, el riesgo de "Fuga de información" pasa de **Extremo** a **Bajo/Moderado**.
3. **Trazabilidad Total:** En caso de una alteración accidental de un documento fiscal, el Log permite identificar exactamente quién realizó el cambio.

5.2. Controles de Gestión de Activos y Soportes

Estos controles aseguran que la información, una vez clasificada, sea almacenada, recuperada y protegida durante todo su ciclo de vida, evitando la pérdida de trazabilidad en procesos financieros y legales.

5.2.1. A.8.13 Respaldos de Información (Backups)

La matriz de riesgos de la entidad señala un nivel de riesgo **Extremo** para la información tributaria debido a un *"respaldo limitado de declaraciones y soportes"*.

- ✓ **Estandarización en Indeportes:** Se debe implementar una política de respaldo basada en la regla **3-2-1** (3 copias, 2 medios diferentes, 1 fuera de la sede).
- ✓ **Frecuencia y Cifrado:** Los respaldos de archivos maestros fiscales, nómina de deportistas y expedientes judiciales deben ser **Semanales y Cifrados** (AES-256).
- ✓ **Pruebas de Restauración:** No basta con copiar los datos; la Oficina de TIC debe realizar simulacros de restauración mensuales para garantizar que, ante un Ransomware, la entidad pueda recuperar su operación en menos de 4 horas.

5.2.2. A.5.23 Gestión de Versiones y Archivo Maestro

Una de las causas raíz identificadas es la *"Inexistencia de control de versiones"*, lo que genera errores en las respuestas a acciones populares o tutelas.

- ✓ **Control de Cambios Documental:** Se implementará un sistema de numeración y control de cambios en el gestor documental (**MERCURIO**) para evitar que se envíen versiones obsoletas a entes judiciales.
- ✓ **Archivo Maestro Tributario:** Centralización de todos los soportes de pago, declaraciones y correcciones en un único repositorio seguro ("Single Source of Truth"). Esto elimina la vulnerabilidad de *"soportes dispersos"* en diferentes correos o carpetas locales.

5.2.3. A.7.7 Procesos de Información y Validación

Para mitigar la *"Validación interna limitada de cálculos"* mencionada en la matriz, este control exige:

- ✓ **Plantillas Estandarizadas:** Uso exclusivo de formatos oficiales de Indeportes para reportes y soportes financieros.
- ✓ **Validación Cruzada:** Implementación de un flujo de trabajo digital donde los cálculos fiscales sean validados por un segundo par antes de ser cargados al sistema nacional, dejando evidencia digital de la revisión.

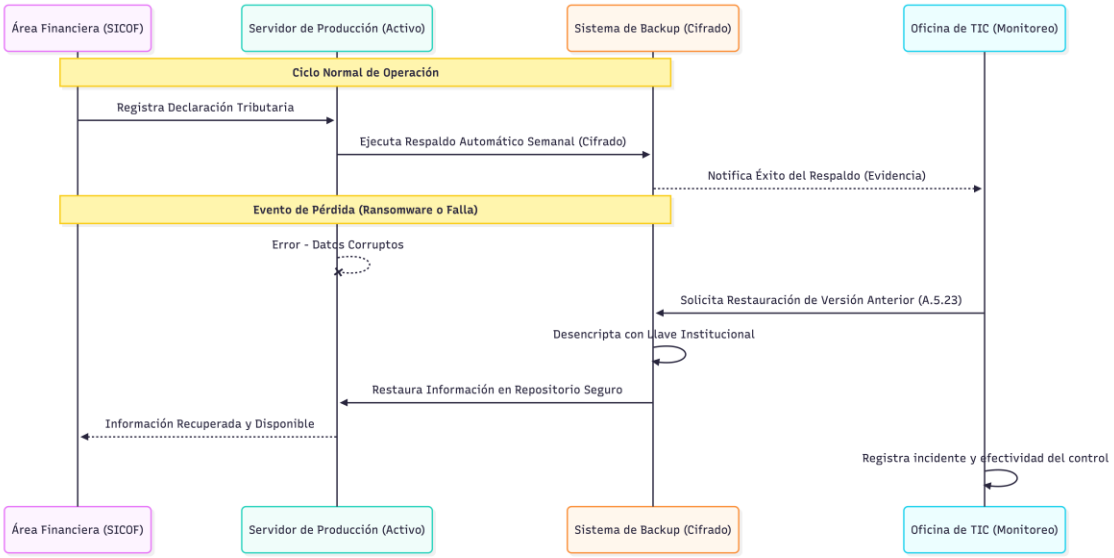
5.2.4. A.8.10 Eliminación de Información y Soportes Físicos

Considerando el riesgo de *"Daño físico en los archivos"* (incendio o deterioro):

- ✓ **Digitalización Certificada:** Los documentos físicos de gran valor (títulos, convenios con ligas) deben ser digitalizados y almacenados en medios protegidos.
- ✓ **Disposición Segura:** En caso de baja de equipos de cómputo (HP/Lenovo), se debe realizar un borrado seguro de discos duros para evitar que datos sensibles de atletas sean recuperados por terceros.

Diagrama de Secuencia: Gestión de Respaldo y Recuperación Fiscal

Este diagrama ilustra cómo funciona el control **A.8.13** ante un evento de pérdida de información en el área financiera.



Beneficios para Indeportes:

1. **Reducción del Riesgo Residual:** La probabilidad de pérdida de datos pasa de **Media** a **Muy Baja** gracias a la automatización.
2. **Cumplimiento del FURAG:** Proporciona las evidencias necesarias (Logs de éxito de backup) para las auditorías de Gobierno Digital.
3. **Seguridad Financiera:** Protege a la entidad de multas por mora causadas por la pérdida de soportes fiscales.

5.3. Controles Técnicos de Protección

Los controles técnicos se enfocan en la protección automatizada de los activos digitales, asegurando que la tecnología no sea solo un medio de almacenamiento, sino un entorno seguro y resiliente.

5.3.1. A.8.11 Controles Criptográficos (Cifrado)

Considerando la vulnerabilidad de *"carencia de respaldos cifrados"* y la sensibilidad de los datos de menores y expedientes de tutela:

- ✓ **Cifrado en Reposo:** Implementación de cifrado de disco (ej. BitLocker o VeraCrypt) en las estaciones de trabajo **HP/Lenovo** y en los volúmenes de almacenamiento donde residen las bases de datos de deportistas.
- ✓ **Cifrado en Tránsito:** Uso obligatorio de protocolos **TLS 1.2+** para el acceso a portales institucionales y el envío de información fiscal vía correo electrónico, asegurando que si la información es interceptada en la red, sea ilegible.

5.3.2. A.8.7 Protección contra Malware

Para mitigar el riesgo de *"Daño digital por virus o deterioro"* que afecte la integridad de los registros financieros y legales:

- ✓ **Estrategia Endpoint:** Instalación de agentes de protección avanzada (EDR) en todos los servidores y estaciones de trabajo de la entidad, con capacidad de bloqueo automático ante intentos de cifrado de archivos (Ransomware).
- ✓ **Escaneo de Correo:** Filtrado técnico en la plataforma de correo institucional para detectar enlaces de *phishing* dirigidos a funcionarios del área jurídica y financiera.

5.3.3. A.8.24 Gestión de Vulnerabilidades Técnicas

Basado en la vulnerabilidad de *"Control de acceso débil"* y sistemas con *"trazabilidad limitada"*:

- ✓ **Ciclo de Parchado:** Establecimiento de una ventana mensual de mantenimiento para aplicar parches de seguridad críticos en los servidores **Lenovo** y equipos de red **Mikrotik**.
- ✓ **Escaneo de Red:** Realización trimestral de escaneos de vulnerabilidades para identificar puertos abiertos innecesarios o servicios obsoletos en los servidores de **SICOF** y **MERCURIO**.

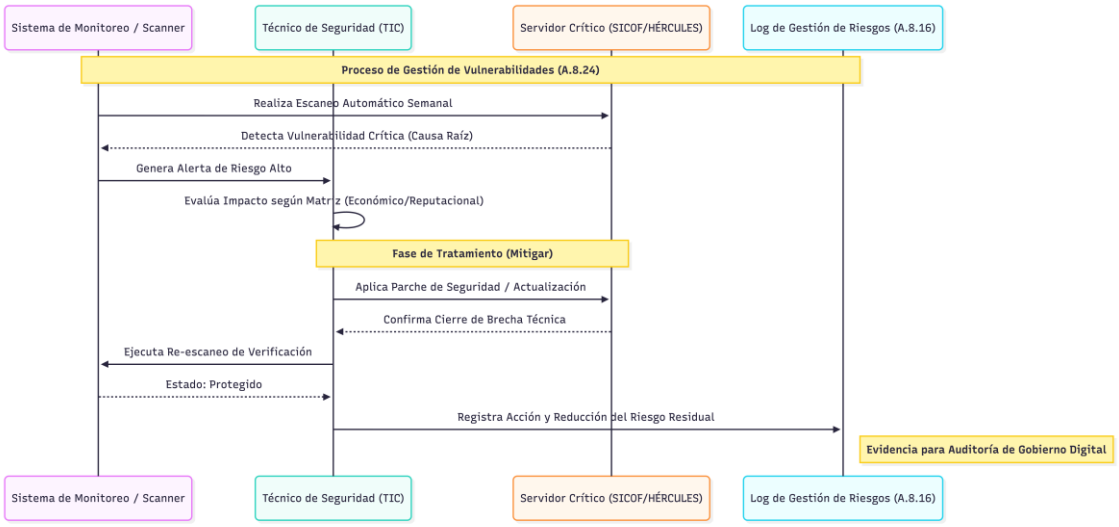
5.3.4. A.8.23 Seguridad en Redes y Acceso Remoto

Para proteger la integridad de la red ante la vulnerabilidad de *"seguridad en redes públicas"*:

- ✓ **Segmentación de Red (VLANs):** Separación técnica de la red administrativa de la red de invitados y de deportistas, evitando que una infección en un equipo externo se propague a los servidores fiscales.
- ✓ **VPN Institucional:** Uso obligatorio de túneles cifrados para el acceso remoto de contratistas y funcionarios a los sistemas de gestión, eliminando la exposición directa de los servidores a Internet.

Diagrama de Secuencia: Proceso de Detección y Mitigación de Vulnerabilidad Técnica

Este diagrama describe cómo la Oficina de TIC de Indeportes identifica un fallo técnico en un servidor crítico y aplica el tratamiento antes de que se materialice el riesgo.



Impacto de la Implementación en Indeportes:

1. **Protección de la Tríada:** El cifrado asegura la **Confidencialidad**, el antivirus la **Integridad** y el parchado la **Disponibilidad**.
2. **Cumplimiento Normativo:** Alinea a la entidad con la Resolución 500 de 2021 de MinTIC sobre estándares mínimos de ciberseguridad.
3. **Reducción de Pérdida Financiera:** Previene el costo asociado a la recuperación de datos tras un ataque, el cual podría superar los 500 SMLMV según los criterios de impacto catastrófico de la matriz.

5.4. Atributos de Efectividad del Control en Indeportes

La efectividad del control es el porcentaje de mitigación que se resta a la vulnerabilidad detectada. Según la matriz **de seguridad de la información.xlsx**, para que un control sobre la información fiscal o judicial sea válido, debe ser evaluado bajo cuatro componentes:

5.4.1. Tipo de Control (Naturaleza)

Define en qué momento actúa el control frente a la materialización de la amenaza.

- ✓ **Preventivo (Peso: 0.25):** Es el más valorado en la entidad. Actúa antes de que ocurra el incidente (ej. el Firewall que bloquea el acceso o el cifrado que impide leer el dato).

- ✓ **Detectivo (Peso: 0.15):** Actúa durante o inmediatamente después del evento (ej. alertas de inicio de sesión fallido en **SICOF**).
- ✓ **Correctivo (Peso: 0.10):** Actúa para reparar el daño (ej. restauración de backups después de un borrado accidental).

5.4.2. Forma de Implementación (Operatividad)

Determina si la ejecución del control depende del factor humano o de algoritmos.

- ✓ **Automático (Peso: 0.25):** El control se ejecuta sin intervención humana (ej. el sistema de gestión de versiones que guarda cambios automáticamente en **MERCURIO**). Es el atributo que más reduce el riesgo residual.
- ✓ **Manual (Peso: 0.10):** Depende de la voluntad y disciplina de un funcionario (ej. el cierre manual de las carpetas de archivo físico o la firma de actas).

5.4.3. Cualidades de Calidad (Atributos de Auditoría)

Para que la Oficina de Control Interno valide la reducción del riesgo, el control debe cumplir tres requisitos:

1. **Documentación:** ¿Existe un manual o procedimiento escrito que describa el control?
2. **Frecuencia:** ¿Se ejecuta con la periodicidad establecida (diaria, mensual, permanente)?
3. **Evidencia:** ¿Existe rastro físico o digital (logs, firmas, capturas) que demuestre que el control se aplicó?

5.4.4. Cálculo de la Calificación del Control

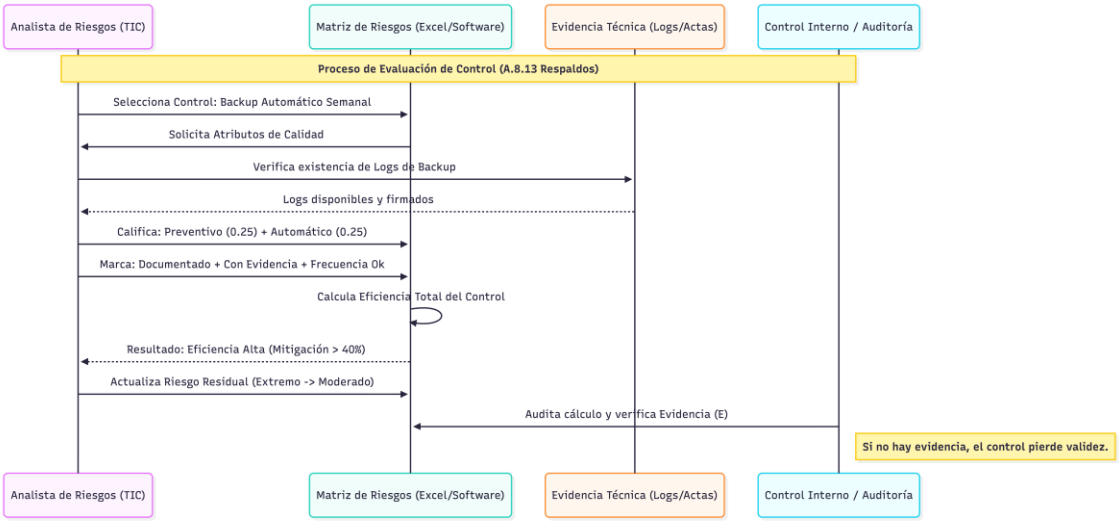
La suma de los pesos de estos atributos determina el **% de Eficiencia del Control**. Este valor se aplica a la Probabilidad e Impacto inherentes para obtener la **Zona de Riesgo Final**.

Caso Real de la Matriz: Un riesgo **Extremo** en "Información Tributaria" se reduce a **Moderado** si el control es:

- ✓ **Preventivo** (Cifrado de base de datos) + **Automático** + **Documentado** + con **Evidencia** técnica.

Diagrama de Secuencia: Evaluación de Efectividad de un Control

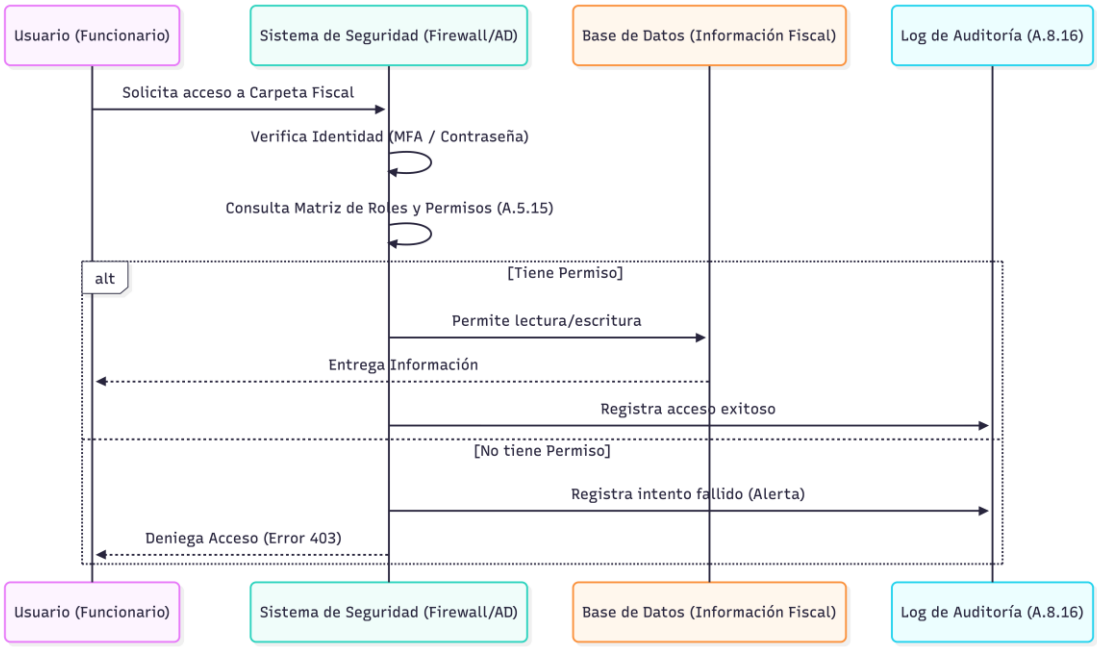
Este diagrama ilustra cómo el sistema de gestión de riesgos de Indeportes decide si un control propuesto es suficiente para bajar el nivel de severidad.



Impacto Institucional: Esta metodología permite que Indeportes Antioquia no solo implemente tecnología, sino que pueda **demostrar ante el Ministerio TIC y a los entes de control Departamentales y Nacionales** que sus controles son reales, medibles y efectivos, mejorando sustancialmente el puntaje en el **FURAG**.

Diagrama de Secuencia: Aplicación de un Control de Acceso (A.5.15)

Este diagrama muestra cómo interactúan los sistemas de Indeportes para proteger un activo confidencial (ej. Información Fiscal) ante una solicitud de acceso.


Usuario (Funcionario)
Sistema de Seguridad (Firewall/AD)
Base de Datos (Información Fiscal)
Log de Auditoría (A.8.16)
Solicita acceso a Carpeta Fiscal
Verifica Identidad (MFA / Contraseña)
Consulta Matriz de Roles y Permisos (A.5.15)
alt
[Tiene Permiso]
Permite lectura/escritura
Entrega Información
Registra acceso exitoso
[No tiene Permiso]
Registra intento fallido (Alerta)
Deniega Acceso (Error 403)
Usuario (Funcionario)
Sistema de Seguridad (Firewall/AD)
Base de Datos (Información Fiscal)
Log de Auditoría (A.8.16)

6. Gestión de Incidentes de Seguridad de la Información

El objetivo de este capítulo es establecer el protocolo de actuación inmediata ante eventos que comprometan la **confidencialidad, integridad o disponibilidad** de los activos de información de la entidad, minimizando el impacto legal y operativo.

6.1. Definiciones y Clasificación en Indeportes

La entidad debe diferenciar con precisión entre una anomalía rutinaria y una crisis de seguridad para optimizar el uso de sus recursos técnicos.

6.1.1. Categorización de Eventos vs. Incidentes

- ✓ **Evento de Seguridad de la Información:** Es cualquier ocurrencia observada en un sistema que indica una posible brecha de seguridad.
- ✓ *Ejemplo en Indeportes:* Un funcionario de la Subgerencia Administrativa reporta que su contraseña de **SICOF** no funciona, o se detecta un aumento inusual de tráfico en el portal web institucional.
- ✓ **Incidente de Seguridad de la Información:** Es un evento (o serie de eventos) confirmado que compromete las operaciones o los activos.
- ✓ *Ejemplo en Indeportes:* La confirmación de que un tercero accedió a los expedientes de **Acciones de Tutela** sin autorización o la eliminación accidental de soportes financieros del archivo maestro.

6.1.2. Clasificación por Niveles de Impacto (Basado en Matriz de seguridad de la información)

Los incidentes se clasifican según el daño potencial a la misión de Indeportes:

Nivel	Tipo de Incidente	Ejemplo Real en Indeportes
Bajo	Afectación mínima.	Caída del servicio de Wi-Fi en zonas comunes o pérdida de un documento público ya publicado en la web.
Medio	Afectación a procesos internos.	Indisponibilidad temporal del sistema **MERCURIO** que retrasa la radicación de correspondencia interna.
Alto	Compromiso de integridad o legalidad.	Alteración de resoluciones de apoyo a ligas deportivas o pérdida de trazabilidad en correcciones fiscales.
Crítico (Extremo)	Daño catastrófico / Legal nacional.	Secuestro de datos (Ransomware) en servidores financieros, fuga de datos sensibles de menores de edad o pérdida de expedientes judiciales originales.

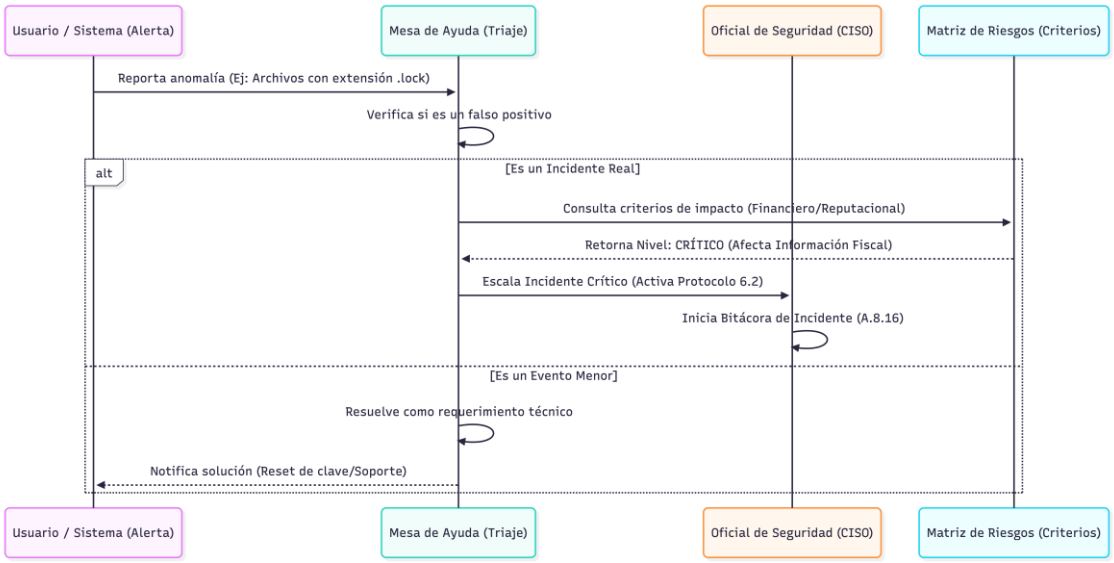
6.1.3. Clasificación por Tipología Técnicas

Para el reporte ante el **CERT** departamental o nacional, Indeportes clasifica los incidentes en:

1. **Acceso no autorizado:** Violación de privilegios en el sistema **HÉRCULES**.
2. **Código Malicioso:** Infección por virus en las estaciones de trabajo **HP/Lenovo**.
3. **Denegación de Servicio (DoS):** Ataque que deja fuera de línea el portal de transparencia de la entidad.
4. **Uso Indebido:** Un funcionario utiliza información confidencial de deportistas para fines personales.
5. **Pérdida o Robo:** Extravío de un equipo de cómputo portátil o un disco duro de respaldo sin cifrar.

Diagrama de Secuencia: Clasificación y Triaje de un Incidente

Este diagrama muestra el flujo de decisión que sigue el equipo de TIC para determinar si una alerta es un incidente real y qué prioridad asignarle.



Este sistema de clasificación permite que, en época de cierres fiscales o auditorías de la Contraloría, Indeportes priorice la protección de los activos financieros sobre cualquier otra solicitud técnica, blindando la responsabilidad legal de los directivos.

6.2. Ciclo de Vida del Incidente (Protocolo de Respuesta)

El protocolo de respuesta se activa en el momento en que un evento de seguridad es validado como un incidente real. En Indeportes, este ciclo se rige por la velocidad de contención para evitar impactos **Catastróficos** (>500 SMLMV).

Fase 1: Detección, Reporte y Registro

- ✓ **Mecanismos:** La detección puede ser interna (alertas de los servidores **Lenovo/Mikrotik**) o externa (reporte de un funcionario en **Sysaid**).
- ✓ **Acción:** Se abre una **Bitácora de Incidente**. Según la matriz, es obligatorio el *"Registro de cambios y correcciones"* para asegurar la trazabilidad.
- ✓ **Evidencia:** Ticket de soporte con hora de inicio, descripción del activo afectado (ej. *Base de Datos de Acciones Populares*) y nivel de riesgo inicial.

Fase 2: Triaje y Clasificación Inmediata

- ✓ **Análisis:** El Oficial de Seguridad cruza el incidente con la **Matriz de Riesgos**.
- ✓ **Priorización:** Si el activo afectado es **Información Fiscal** o **Expedientes Jurídicos**, el incidente se clasifica automáticamente como **Prioridad Extrema**.
- ✓ **Notificación:** Se informa a los líderes de proceso afectados (Subgerente Administrativo o Jefe de la Oficina Jurídica).

Fase 3: Contención y Erradicación (Control A.8.24)

- ✓ **Aislamiento:** Ante un código malicioso, se desconectan los equipos de la red para evitar el acceso a redes públicas o la propagación.
- ✓ **Protección de Evidencia:** Se realiza una copia "bit a bit" de los discos afectados para análisis forense, cumpliendo con el control de *"trazabilidad de registros críticos"*.
- ✓ **Limpieza:** Se eliminan las vulnerabilidades que permitieron el ingreso (ej. cerrar puertos abiertos o actualizar parches de seguridad).

Fase 4: Recuperación y Restauración (Control A.8.13)

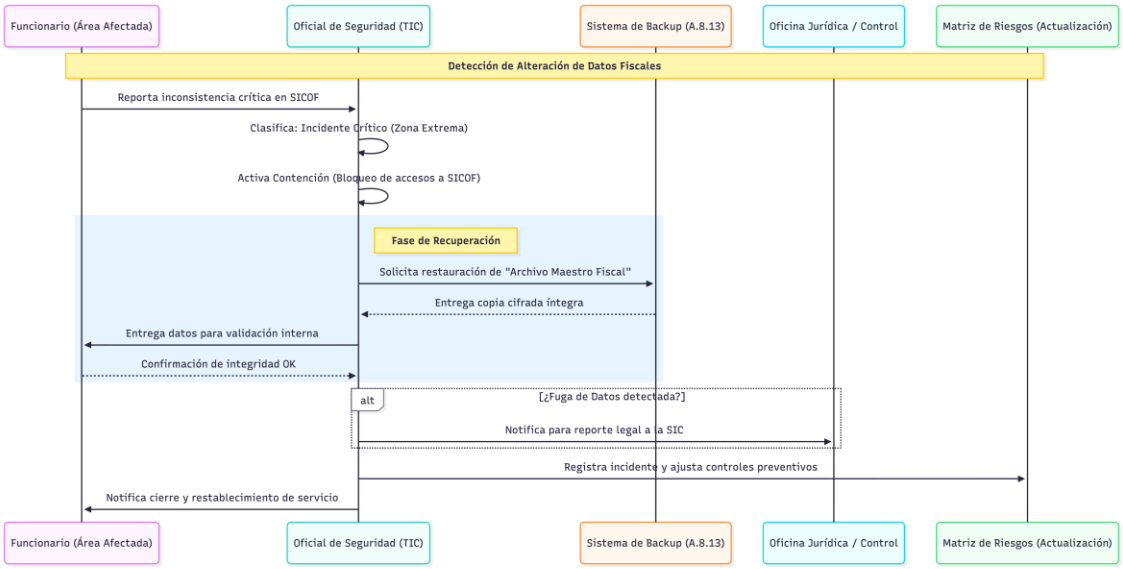
- ✓ **Validación de Backup:** Se accede al **Repositorio Cifrado** de copias de respaldo.
- ✓ **Restauración:** Se cargan los datos en un entorno seguro antes de pasarlos a producción.
- ✓ **Verificación:** El funcionario del área (Financiera/Jurídica) realiza una *"Validación interna previa de cálculos y registros"* para confirmar que la integridad de la información es total.

Fase 5: Notificación Normativa y Cierre

- ✓ **Reporte a la SIC:** Si hubo fuga de datos personales, el área jurídica inicia la notificación a la Superintendencia de Industria y Comercio (Ley 1581).
- ✓ **Lecciones Aprendidas:** Se analiza por qué falló el control preventivo y se actualiza la Matriz de Riesgos.
- ✓ **Cierre Documental:** Se archiva el informe técnico de cierre con las evidencias de la restauración y la eliminación de la amenaza.

Diagrama de Secuencia: Flujo de Respuesta a Incidente Extremo

Este diagrama visualiza la interacción entre los actores de Indeportes ante un riesgo materializado de alteración de información tributaria.



Este protocolo asegura que ante la *"dependencia de información de terceros"* mencionada en su matriz, la entidad siempre tenga la capacidad de verificar y restaurar sus propios registros maestros, evitando que un error externo paralice la seguridad financiera de Indeportes Antioquia.

6.3. Roles y Responsabilidades ante Incidentes

En Indeportes Antioquia, la gestión de incidentes no es responsabilidad exclusiva de la Oficina de TIC; requiere una actuación coordinada entre las áreas misionales y de apoyo, especialmente cuando se ve afectada la **Información Fiscal** o los **Expedientes Jurídicos**.

6.3.1. Oficial de Seguridad de la Información (CISO / Líder TIC)

Es el director de la respuesta ante incidentes. Sus responsabilidades incluyen:

- ✓ **Declaratoria de Incidente:** Clasificar la severidad (Baja a Extrema) según los criterios de la matriz.
- ✓ **Orden de Contención:** Autorizar el aislamiento de servidores o el corte de servicios de red para proteger los activos.
- ✓ **Análisis Forense:** Liderar la investigación de la "Causa Raíz" para identificar vulnerabilidades técnicas (A.8.24).

6.3.2. Equipo de Respuesta Técnica (Nivel 1 y 2 / Proveedores)

Encargados de la ejecución operativa de los controles del Anexo A:

- ✓ **Restauración (A.8.13):** Ejecutar la recuperación de datos desde los backups cifrados.
- ✓ **Limpieza de Sistemas:** Eliminar malware o cerrar puertos comprometidos en equipos **Mikrotik/Lenovo**.
- ✓ **Recolección de Evidencia:** Asegurar los registros de bitácora (A.8.16) para demostrar la trazabilidad del incidente.

6.3.3. Dueños de los Activos (Líderes de Áreas Financiera y Jurídica)

Son los responsables de la información contenida en los sistemas (SICOF, Mercurio):

- ✓ **Validación de Integridad:** Según la matriz, deben realizar la *"Validación interna previa de cálculos y plazos"* antes de dar por recuperado un servicio fiscal.
- ✓ **Evaluación de Impacto de Negocio:** Informar sobre las consecuencias de la indisponibilidad de sus archivos maestros ante la Gerencia.

6.3.4. Oficina Jurídica y de Control Interno

Actúan cuando el incidente tiene implicaciones legales:

- ✓ **Notificación Normativa:** Gestionar el reporte de brechas de datos personales ante la **Superintendencia de Industria y Comercio (SIC)**.
- ✓ **Cumplimiento:** Verificar que las acciones tomadas no vulneren la cadena de custodia en caso de procesos contra terceros.

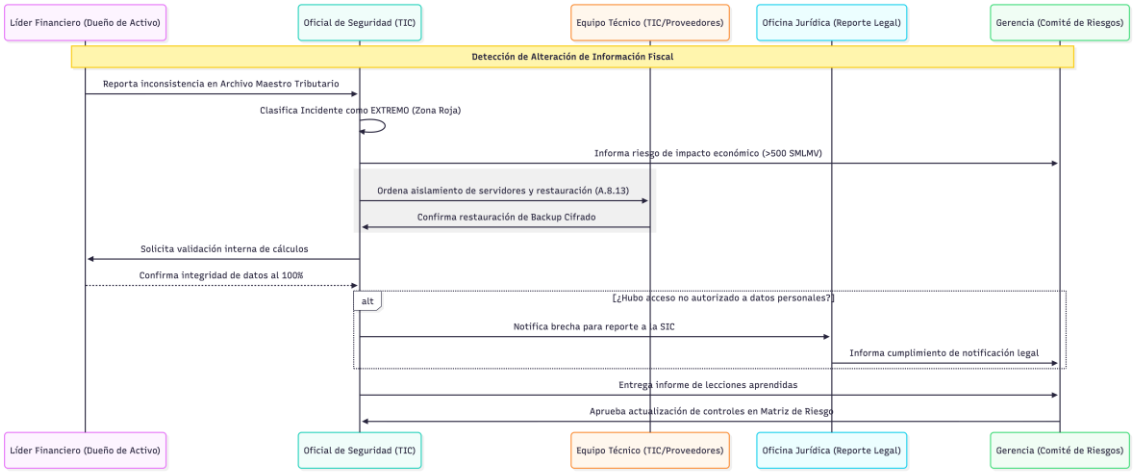
6.3.5. Comité de Riesgos / Alta Dirección

Su rol es estratégico y de soporte:

- ✓ **Aprobación de Recursos:** Autorizar gastos extraordinarios para la contención o contratación de servicios especializados de recuperación.
- ✓ **Comunicación Externa:** Emitir comunicados oficiales para proteger la reputación institucional ante impactos de nivel **Catastrófico**.

Diagrama de Secuencia: Interacción de Roles durante un Incidente Crítico

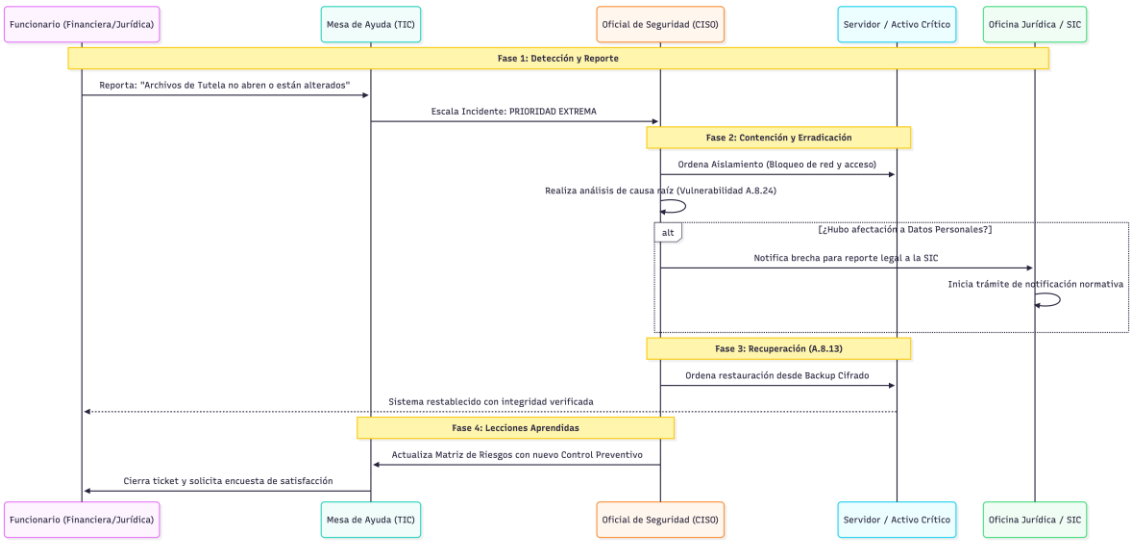
Este diagrama visualiza cómo fluye la responsabilidad en la entidad desde el descubrimiento de una alteración de datos hasta la validación final.



Esta asignación de roles asegura que el **Oficial de Seguridad** no sea el único responsable del éxito de la recuperación. La participación del **Líder Financiero** en la validación de los datos garantiza que el tratamiento del riesgo sea real y no solo un parche técnico, cumpliendo con la exigencia de la matriz de *"Registro obligatorio de cambios y correcciones"*.

Diagrama de Secuencia: Respuesta a Incidente de "Prioridad Extrema"

Este diagrama describe el flujo de acciones ante la detección de un acceso no autorizado o alteración de información confidencial en Indeportes.



Impacto de este capítulo en la entidad:

- ✓ **Resiliencia Operativa:** Asegura que Indeportes no se detenga ante ataques digitales.
- ✓ **Blindaje Legal:** Cumple con la obligación de reporte ante la SIC, evitando multas onerosas.
- ✓ **Mejora FURAG:** Demuestra la existencia de un protocolo de respuesta formal, elevando la madurez en la dimensión de TI.

7. Monitoreo y Revisión

El objetivo de este capítulo es establecer las actividades de seguimiento necesarias para verificar que los controles implementados funcionan correctamente y que el perfil de riesgo de la entidad se mantiene dentro de los niveles aceptables.

7.1. Seguimiento Permanente de Riesgos (Control A.8.16)

De acuerdo con la columna **"Seguimiento"** de la matriz institucional, el monitoreo no es anual, sino que se vincula a la frecuencia de la obligación o proceso.

- ✓ **Revisiones de Bitácoras (Logs):** La Oficina de TIC debe revisar semanalmente los registros de acceso a los activos críticos (Información Fiscal y Judicial) para detectar intentos de acceso no autorizados.
- ✓ **Verificación de Controles:** Cada mes se debe validar que los controles calificados como "Automáticos" en la matriz sigan operando sin intervención manual.

7.2. Indicadores Clave de Riesgo (KRI)

Para medir la salud de la seguridad en Indeportes, se establecen los siguientes indicadores:

1. **Efectividad de Backups:** (Copias exitosas / Total de copias programadas) x 100. Meta: 100%.
2. **Incidentes por Vulnerabilidades Conocidas:** Número de incidentes causados por falta de parches (A.8.24). Meta: 0.
3. **Tiempo de Respuesta a Incidentes Extremos:** Tiempo transcurrido desde la detección hasta la contención en procesos financieros.

7.3. Auditorías y Revisiones de Control Interno

- ✓ **Auditoría de Cumplimiento:** Semestralmente, la Oficina de Control Interno verificará la existencia de la **"Evidencia"** marcada en la matriz (actas, logs, capturas de pantalla).
- ✓ **Revisión por la Dirección:** El Comité de Riesgos de Indeportes se reunirá trimestralmente para revisar los riesgos que se mantienen en **"Zona Extrema"** y asignar recursos adicionales si el riesgo residual no ha disminuido.

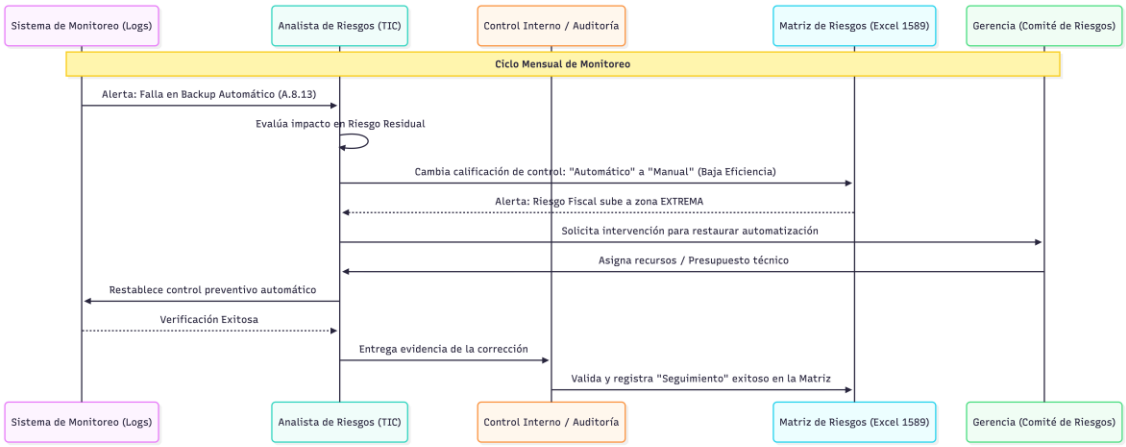
7.4. Actualización de la Matriz de Riesgos

La matriz debe actualizarse inmediatamente cuando:

- ✓ Se identifique una nueva vulnerabilidad técnica en los servidores **Lenovo/Mikrotik**.
- ✓ Ocurra un cambio normativo que afecte la gestión de datos personales (SIC).
- ✓ Se presente un incidente de seguridad que demuestre que un control actual es ineficaz.

Diagrama de Secuencia: Proceso de Monitoreo y Ajuste de Controles

Este diagrama ilustra cómo la entidad detecta un fallo en la efectividad de un control y procede a su ajuste para proteger la información fiscal.



El cumplimiento de este capítulo asegura que Indeportes Antioquia pueda responder satisfactoriamente a las auditorías del **MIPG (FURAG)**, demostrando que la gestión de riesgos no es un requisito de papel, sino una práctica institucional que garantiza la transparencia y la seguridad financiera del deporte en el departamento.

8. Matriz de Riesgos (Ejemplo de Contenido)

La matriz de riesgos permite visualizar la exposición de la entidad y la efectividad de los controles propuestos. A continuación, se presentan tres escenarios críticos extraídos y adaptados de la realidad institucional.

8.1. Estructura de la Matriz

La matriz se divide en cuatro bloques lógicos que permiten trazar el riesgo desde su origen hasta su mitigación final.

8.1.1. Bloque de Identificación y Contexto

En esta sección se define el activo y qué podría salir mal. Según la matriz de la entidad, los campos obligatorios son:

- ✓ **Proceso:** El área dueña de la información (ej. Acciones Constitucionales, Financiera, Fomento).
- ✓ **Activo de Información:** El elemento físico o digital a proteger (ej. Expediente de Tutela, Base de Datos de Deportistas).
- ✓ **Amenazas:** Acciones que pueden causar daño (Pérdida, alteración, acceso no autorizado).
- ✓ **Vulnerabilidades (Causa Raíz):** Debilidades que permiten la amenaza (Falta de clasificación, control de acceso débil, ausencia de backups).

8.1.2. Bloque de Evaluación del Riesgo Inherente

Es el cálculo del riesgo en su estado puro (sin controles). Se utiliza la fórmula:

Riesgo Inherente = P \ I
Donde:

- ✓ **Probabilidad (P):** Calificada de 0.2 a 1.0 según la frecuencia de la actividad.
- ✓ **Impacto (I):** Calificado de 0.2 a 1.0 según la afectación económica (SMLMV) y reputacional.
- ✓ **Zona de Riesgo:** Resultado del cruce en la matriz de calor (Bajo, Moderado, Alto, Extremo).

8.1.3. Bloque de Controles (Tratamiento)

Aquí se asocian las salvaguardas del **Anexo A de la ISO 27001**. La estructura de la matriz exige:

- ✓ **Control Anexo A:** El código específico de la norma (ej. A.8.13 para respaldos).
- ✓ **Descripción del Control:** La acción técnica o administrativa específica en Indeportes (ej. "Cifrado de disco en equipos HP").
- ✓ **Atributos de Eficiencia:** Calificación del control según sea **Preventivo/Detectivo** y **Automático/Manual**, sumado a la existencia de **Documentación** y **Evidencia**.

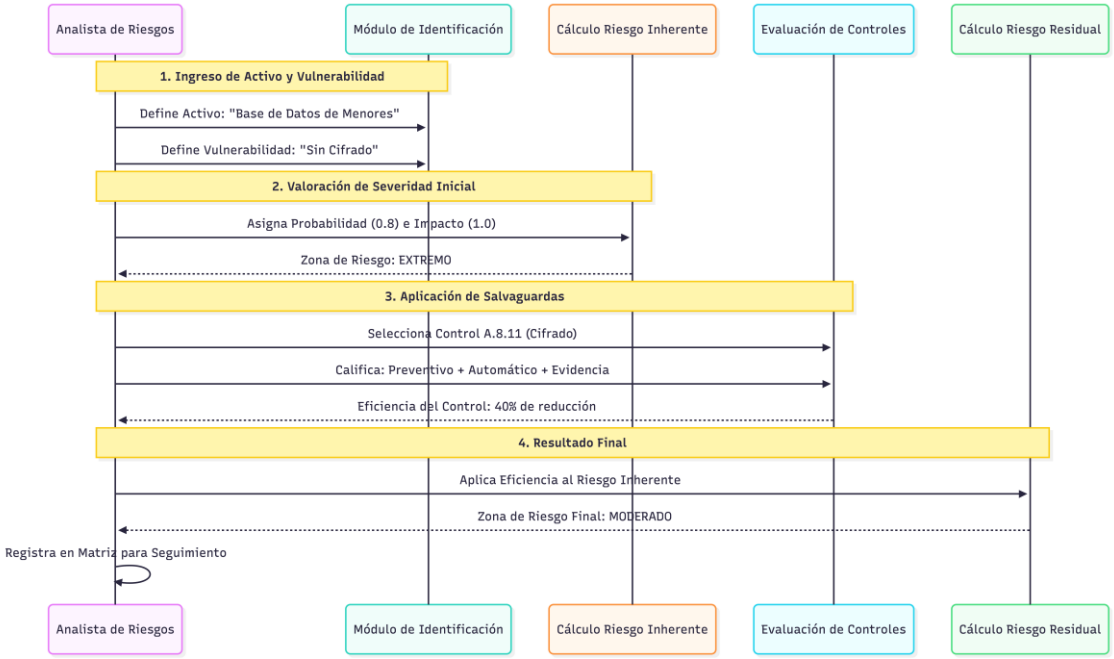
8.1.4. Bloque de Riesgo Residual y Seguimiento

Es el resultado final tras restar la eficiencia de los controles al riesgo inherente.

- ✓ **Zona de Riesgo Final:** El objetivo es que todos los riesgos críticos (Rojos) pasen a zonas aceptables (Verde/Amarillo).
- ✓ **Seguimiento:** Campo donde se registra la fecha y el resultado de la última verificación del control.
- ✓ **Estado:** Define si el riesgo está "Activo", "Mitigado" o "En Proceso".

Diagrama de Secuencia: Cálculo de la Estructura de Riesgo

Este diagrama muestra cómo los datos ingresados en la estructura de la matriz interactúan para generar el nivel de severidad final.



Esta estructura permite que Indeportes Antioquia cumpla con el Modelo Integrado de Planeación y Gestión (MIPG), ya que proporciona una trazabilidad matemática exacta de por qué un riesgo se considera controlado, facilitando la defensa ante auditorías externas de la Contraloría o la Procuraduría.

8.2. Ejemplo 1: Gestión Legal (Acciones de Tutela)

Este ejemplo ilustra cómo un activo de información sensible transita por la metodología de riesgos de la entidad.

8.2.1. Identificación del Riesgo

- ✓ **Activo de Información:** Expedientes de Acciones de Tutela (Digitales y Físicos).
- ✓ **Amenaza:** Pérdida, alteración o divulgación no autorizada de documentos judiciales o datos personales de las partes.
- ✓ **Vulnerabilidades (Causa Raíz):**
- ✓ Falta de clasificación de confidencialidad.
- ✓ Ausencia de control de acceso o registro de manejo de expedientes.
- ✓ Almacenamiento sin cifrado.
- ✓ Falta de respaldos digitales y físicos.

8.2.2. Valoración del Riesgo Inherente

Según los criterios de la entidad, el riesgo se valora antes de cualquier control:

- ✓ **Probabilidad:0.6 (Media)**. La actividad se ejecuta de 24 a 500 veces por año (frecuencia bimensual/semanal de tutelas).
- ✓ **Impacto:1.0 (Catastrófico)**. Una pérdida de un expediente original o un error en la respuesta puede generar un impacto mayor a 500 SMLMV o una afectación nacional a la imagen de la Gobernación.
- ✓ **Zona de Riesgo: EXTREMO** (Punto crítico en la matriz de calor).

8.2.3. Aplicación de Controles (Tratamiento)

Para reducir este riesgo, Indeportes aplica los controles del Anexo A de ISO 27001 con los siguientes atributos de eficiencia:

1. **A.5.7 Clasificación:** Etiquetado obligatorio como **"Confidencial - Información Sensible"**.
2. **A.5.15 Control de Acceso:** Repositorio en el sistema **MERCURIO** restringido únicamente a los abogados del área jurídica.
3. **A.8.13 Copias de Respaldo:** Sincronización diaria con la nube institucional cifrada.
4. **A.8.16 Registro y Monitoreo:** Activación de bitácoras para saber quién descargó o modificó un anexo judicial.

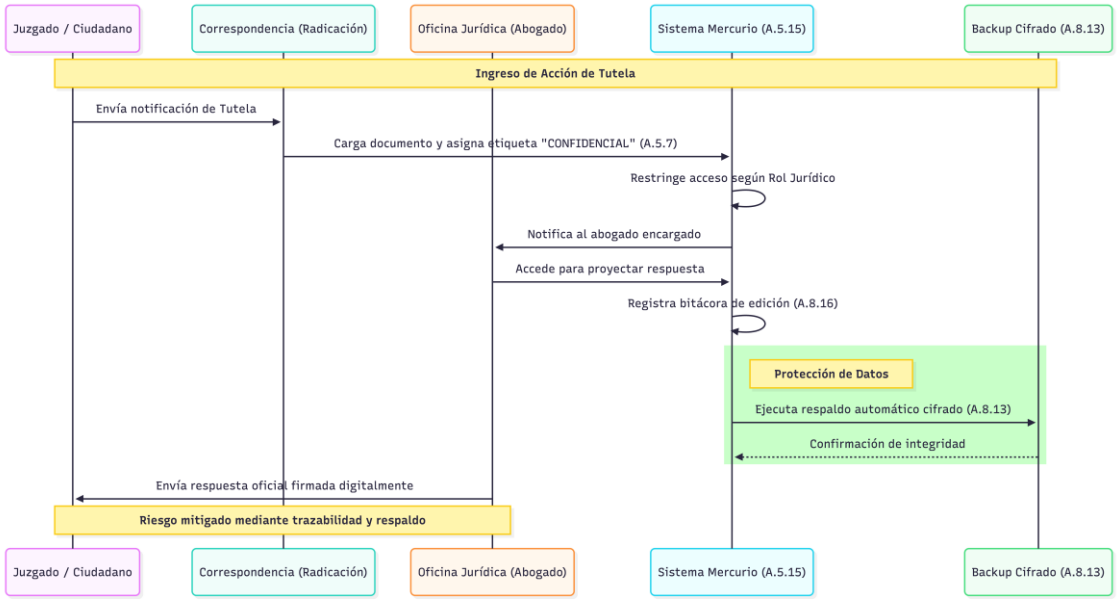
8.2.4. Cálculo del Riesgo Residual

Al aplicar controles **Preventivos** y **Automáticos** (con documentación y evidencia), la eficiencia del control es alta:

- ✓ **Impacto Residual:** Se reduce a **0.6 (Moderado)** al tener respaldos.
- ✓ **Probabilidad Residual:** Se reduce a **0.2 (Muy Baja)** gracias al control de acceso y monitoreo.
- ✓ **Zona de Riesgo Final: MODERADO**.

Diagrama de Secuencia: Ciclo de Vida y Protección de una Tutela

Este diagrama describe el flujo técnico-legal para asegurar que la información no sea alterada ni vista por personal no autorizado.



Este ejemplo permite a los funcionarios de **Indeportes Antioquia** comprender que la seguridad no es solo "no perder el papel", sino asegurar que el **dato digital** sea inalterable y auditable, protegiendo la defensa judicial de la entidad y los datos de los ciudadanos.

8.3. Ejemplo 2: Gestión Financiera (Información Tributaria)

Este ejemplo se centra en la protección del "Archivo Maestro Tributario", activo vital para la transparencia financiera de la entidad.

8.3.1. Identificación del Riesgo

- ✓ **Activo de Información:** Archivo maestro de declaraciones, soportes de pago, estados financieros y registros en **SICOF**.
- ✓ **Amenaza:** Pérdida, alteración, error en el cálculo o divulgación indebida de información tributaria ante entes de control.
- ✓ **Vulnerabilidades (Causa Raíz):**
- ✓ Trazabilidad débil en correcciones o ajustes manuales.
- ✓ Dispersión de soportes en correos electrónicos o carpetas locales.
- ✓ Falta de un archivo maestro centralizado y protegido.
- ✓ Validación interna limitada antes de los cargues oficiales.

8.3.2. Valoración del Riesgo Inherente

Siguiendo los parámetros técnicos del anexo:

- ✓ **Probabilidad:0.6 (Media)**. La frecuencia de la actividad se asocia a los calendarios tributarios (mensual/bimensual).
- ✓ **Impacto:1.0 (Catastrófico)**. Una inconsistencia puede generar multas superiores a 500 SMLMV y un efecto publicitario negativo a nivel país.
- ✓ **Zona de Riesgo: EXTREMO**.

8.3.3. Aplicación de Controles (Tratamiento)

Para mitigar la severidad, se han definido controles con una eficiencia del control superior al 40%, basándose en su naturaleza **Preventiva** y **Automática**:

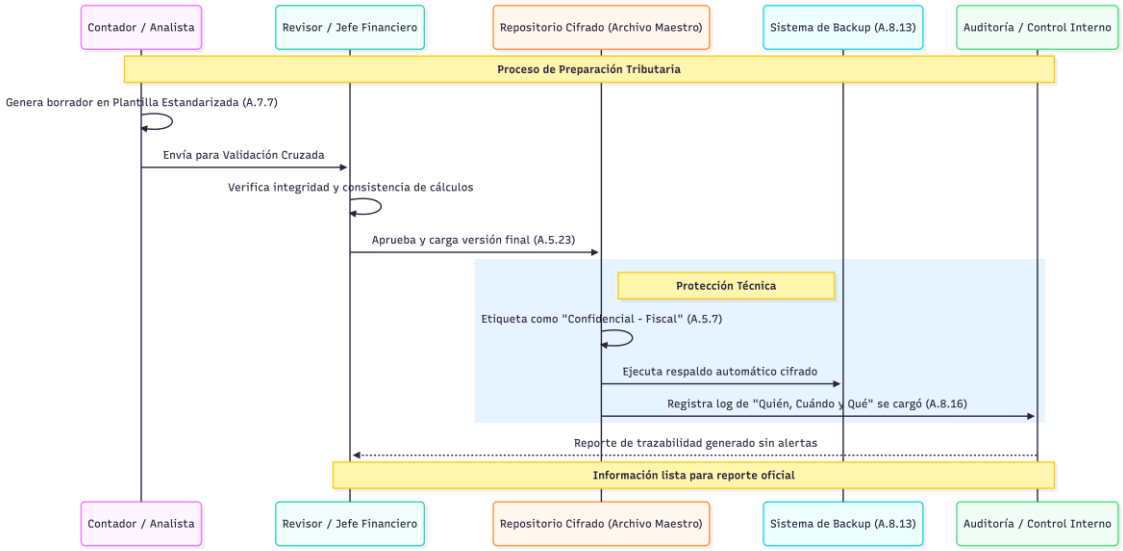
1. **A.5.23 Gestión de Versiones:** Implementación de un control estricto de cambios para que cada ajuste a una declaración sea trazable y aprobado por un supervisor.
2. **A.7.7 Seguridad en Procesos de Información:** Uso de **Plantillas Estandarizadas** para reportes, eliminando la manipulación de fórmulas en archivos individuales.
3. **A.8.13 Respaldos (Backups):** Copia de seguridad semanal del repositorio financiero, almacenada de forma cifrada y fuera de la red principal.
4. **A.8.16 Registro y Monitoreo:** Auditoría de registros en el sistema financiero para identificar quién realizó modificaciones en periodos cerrados.

8.3.4. Cálculo del Riesgo Residual

- ✓ **Impacto Residual:** Se mantiene en un nivel alto, pero la probabilidad de error humano o técnico disminuye drásticamente.
- ✓ **Probabilidad Residual:** Baja a **0.2 (Muy Baja)** gracias a la automatización y validación cruzada.
- ✓ **Zona de Riesgo Final: ALTO** (Se acepta en esta zona bajo la condición de monitoreo permanente por parte de la Subgerencia Administrativa).

Diagrama de Secuencia: Validación y Resguardo de Información Fiscal

Este diagrama ilustra el flujo de control para asegurar que un reporte financiero no sea alterado antes de su presentación ante los entes de control.



Con este ejemplo, **Indeportes Antioquia** asegura que su "memoria financiera" no dependa de la ubicación física de un papel o de la memoria de un funcionario. Al centralizar los soportes en un repositorio con control de versiones y backups automáticos, se elimina la vulnerabilidad de *"soportes dispersos"* y se garantiza una defensa sólida ante cualquier requerimiento de la DIAN o la Contraloría.

8.4. Ejemplo 3: Fomento Deportivo (Datos de Menores y Seguros)

Este ejemplo describe la protección de la información en los programas misionales de fomento, donde la entidad actúa como custodio de datos sensibles de la población deportista del departamento.

8.4.1. Identificación del Riesgo

- ✓ **Activo de Información:** Bases de datos de Programas de Apoyo Social, Pólizas de Seguros de Accidentes Deportivos y listados de beneficiarios.
- ✓ **Amenaza:** Fuga, manipulación o divulgación indebida de información personal y médica; errores en los listados asegurados; uso de versiones obsoletas para el reporte a aseguradoras.
- ✓ **Vulnerabilidades (Causa Raíz):**
- ✓ Controles débiles de acceso a repositorios compartidos.
- ✓ Trazabilidad limitada en la actualización de beneficiarios.
- ✓ Ausencia de protocolos claros para el tratamiento de **datos de menores de edad**.
- ✓ Envío de información a terceros (aseguradoras) sin canales cifrados.

8.4.2. Valoración del Riesgo Inherente

Dada la naturaleza de los datos (salud y menores):

- ✓ **Probabilidad:0.6 (Media)**. Actividad de seguimiento mensual o según vigencia de pólizas.
- ✓ **Impacto:1.0 (Catastrófico)**. Una filtración de datos de menores o la falta de cobertura por un error en la base de datos genera un impacto legal y reputacional nacional severo.
- ✓ **Zona de Riesgo: EXTREMO**.

8.4.3. Aplicación de Controles (Tratamiento)

Se implementan salvaguardas específicas para elevar la protección de la privacidad:

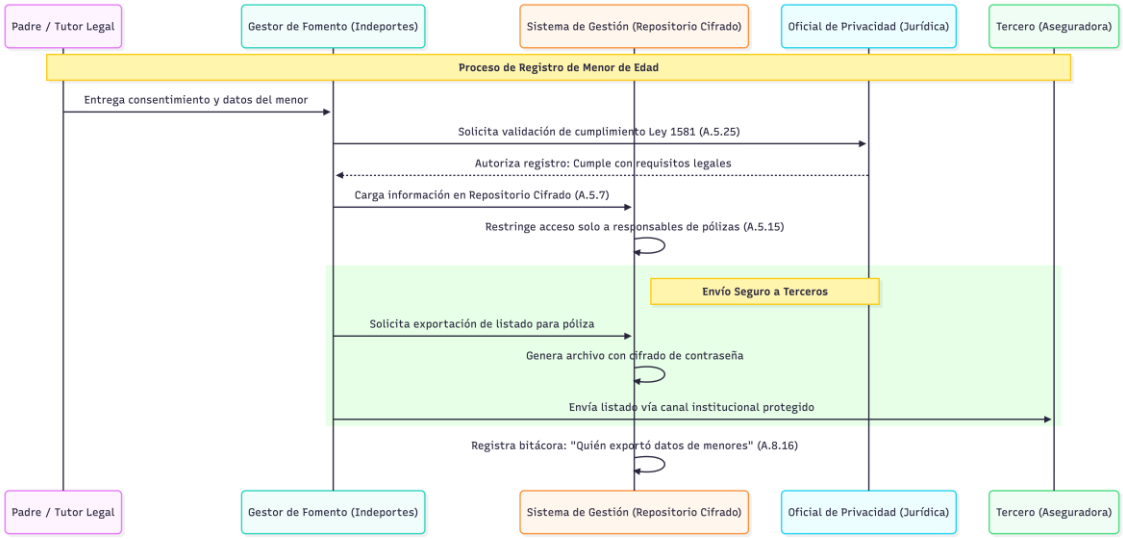
1. **A.5.25 Protección de Datos Personales (Crítico):** Implementación de formatos de consentimiento informado firmados por los padres o tutores legales para el tratamiento de datos de menores.
2. **A.5.7 Clasificación:** Etiquetado de bases de datos como **"Información Confidencial y Sensible - Datos de Salud/Menores"**.
3. **A.7.7 Seguridad en Procesos:** Implementación de una **"Doble Verificación"** (par cruzado) antes de enviar listados finales a las compañías aseguradoras.
4. **A.8.13 Respaldos:** Consolidación de un **Archivo Maestro de Pólizas** con respaldo semanal automático y cifrado.

8.4.4. Cálculo del Riesgo Residual

- ✓ **Impacto Residual:** Aunque el impacto legal sigue siendo alto, la probabilidad de error o fuga se mitiga.
- ✓ **Probabilidad Residual:** Se reduce a **0.2 (Muy Baja)** mediante la estandarización de formatos y el control de acceso.
- ✓ **Zona de Riesgo Final: MODERADO**.

Diagrama de Secuencia: Acceso y Tratamiento de Datos de Menores

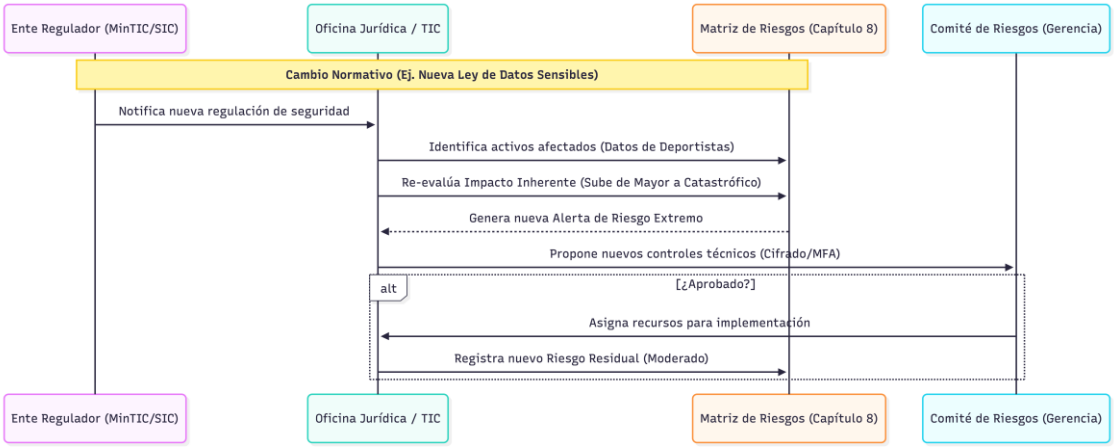
Este diagrama visualiza el flujo seguro para la actualización de un deportista menor de edad en el programa de seguros.



Con este control, **Indeportes Antioquia** blinda su proceso de fomento deportivo, asegurando que el beneficio social (la póliza de seguros) no se convierta en un riesgo legal. Al exigir el consentimiento informado y el cifrado de archivos, la entidad cumple con los más altos estándares de protección de la infancia y la adolescencia en el entorno digital.

Diagrama de Secuencia: Flujo de Actualización de la Matriz

Este diagrama describe cómo un cambio en el entorno de Indeportes (ej. nueva normativa) obliga a actualizar la matriz para mantener la protección.



La Matriz de Riesgos no es solo un cuadro; es la herramienta de navegación de Indeportes Antioquia. Al seguir estos ejemplos, la entidad asegura que sus procesos más sensibles (Legal, Financiero y Misional) cuenten con un escudo técnico validado por la norma ISO 27001 y las exigencias del MIPG.

9. Roles y Responsabilidades en Seguridad de la Información

La seguridad de la información en la entidad es un compromiso compartido. Para garantizar la protección de los activos (fiscales, judiciales y de fomento), se establece la siguiente estructura jerárquica y operativa:

9.1 Alta Dirección (Gerencia General y Subgerencias)

Como líderes estratégicos, su responsabilidad es garantizar que la seguridad sea una prioridad institucional.

Responsabilidades:

- ✓ Aprobar los recursos financieros para controles técnicos (como el cifrado de servidores Lenovo o licencias de seguridad).
- ✓ Designar al Oficial de Seguridad de la Información.
- ✓ Liderar con el ejemplo en el cumplimiento de las políticas de **ISO 27001**.
- ✓ Revisar trimestralmente el estado de los riesgos en el Comité de Gestión y Desempeño.

9.2. Oficial de Seguridad de la Información (CISO / Jefe de TIC)

Es el rol técnico-estratégico que coordina el SGSI (Sistema de Gestión de Seguridad de la Información).

Responsabilidades:

- ✓ Mantener actualizada la **Matriz de Riesgos de seguridad de la información**.
- ✓ Asegurar que los controles de **Respaldos (A.8.13)** y **Acceso (A.5.15)** se ejecuten automáticamente.
- ✓ Coordinar la respuesta ante incidentes de prioridad **Extrema**.
- ✓ Realizar el monitoreo de vulnerabilidades en los activos tecnológicos (HP, Lenovo, Mikrotik).

9.3. Dueños de los Procesos y Activos (Líderes de Área)

Son los jefes de las oficinas (Jurídica, Financiera, Fomento) que "viven" con la información diariamente.

Responsabilidades:

- ✓ Clasificar la información a su cargo (**Pública, Interna, Confidencial**).
- ✓ Validar la integridad de los datos tras un proceso de restauración.
- ✓ Definir quiénes de sus subordinados deben tener acceso a carpetas sensibles de **Tutelas** o **Impuestos**.
- ✓ Reportar inmediatamente cualquier sospecha de fuga de información.

9.4. Usuarios (Funcionarios y Contratistas)

Son la primera línea de defensa de la entidad.

Responsabilidades:

- ✓ Cumplir con la política de "Escritorio Limpio" y bloqueo de sesión.
- ✓ Utilizar únicamente los repositorios oficiales (Mercurio, OneDrive institucional) para almacenar soportes.
- ✓ Participar en las capacitaciones obligatorias de seguridad digital.
- ✓ No compartir contraseñas de acceso a **SICOF** o sistemas misionales.

9.5. Oficina de Control Interno

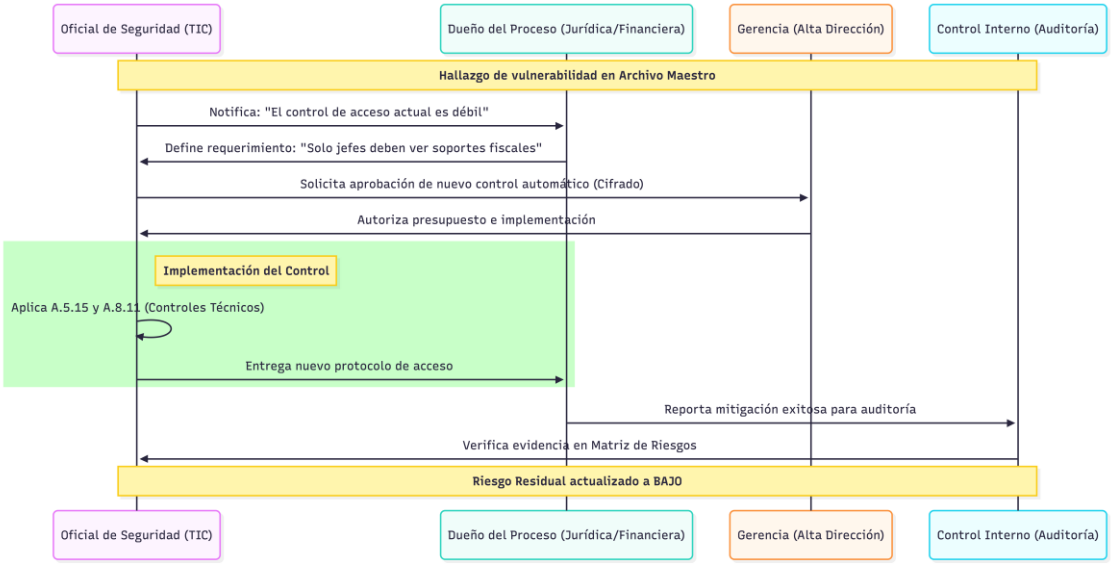
Actúa como el ente evaluador independiente.

Responsabilidades:

- ✓ Auditar semestralmente la efectividad de los controles descritos en la matriz.
- ✓ Verificar la existencia de **Evidencia** (logs, actas) que respalden la calificación de los controles.
- ✓ Reportar el nivel de madurez del SGSI ante el **FURAG**.

Diagrama de Secuencia: Interacción de Roles ante un Cambio en el Perfil de Riesgo

Este diagrama ilustra cómo colaboran los roles cuando se detecta una nueva vulnerabilidad crítica en los sistemas de la entidad.



La claridad en estos roles asegura que, ante un incidente o una auditoría, **Indeportes Antioquia** responda de manera coordinada. Al asignar responsables específicos a cada activo de información, se elimina la "Causa Raíz" de **trazabilidad limitada** identificada en la matriz institucional.

10. Inventario de Activos con Valoración Intrínseca

10.1. Criterios de Valoración (Tríada CID)

La valoración se realiza asignando un puntaje de **1 a 4** a cada una de las dimensiones de la seguridad, donde:

- ✓ **1 (Bajo):** El impacto de la pérdida es insignificante.
- ✓ **2 (Medio):** Impacto moderado, afecta procesos secundarios.
- ✓ **3 (Alto):** Impacto grave, afecta procesos misionales o legales.
- ✓ **4 (Crítico):** Impacto catastrófico, paraliza la entidad o genera sanciones nacionales.

Las dimensiones evaluadas son:

1. **Confidencialidad (C):** Necesidad de que la información no sea divulgada a personas no autorizadas.
2. **Integridad (I):** Necesidad de que la información se mantenga exacta, completa y sin alteraciones.
3. **Disponibilidad (D):** Necesidad de que la información sea accesible cuando se requiera.

10.2. Inventario Valorizado de Activos Críticos

Basándonos en la **Matriz de seguridad de la información**, hemos seleccionado los activos con mayor relevancia para los objetivos de Indeportes:

Activo de Información	Tipo de Activo	Confidencialidad (C)	Integridad (I)	Disponibilidad (D)	Valor Intrínseco (Máx)
Expedientes de Acciones de Tutela	Información / Legal	4	4	3	**4 (Crítico)**
Archivo Maestro Tributario	Información / Fiscal	3	4	4	**4 (Crítico)**
Historias Clínicas de Deportistas	Datos Sensibles	4	4	3	**4 (Crítico)**
Bases de Datos de Menores (Fomento)	Datos Personales	4	3	2	**4 (Crítico)**

Plataforma SICOF (Finanzas)	Software / Sistema	3	4	4	**4 (Crítico)**
Plataforma HÉRCULES (Deporte)	Software / Sistema	2	4	4	**4 (Crítico)**
Servidores Críticos (Lenovo)	Hardware	3	4	4	**4 (Crítico)**
Redes de Comunicaciones (Mikrotik)	Infraestructura	1	3	4	**4 (Crítico)**

10.3. Nivel de Criticidad del Activo

El valor intrínseco final del activo se define por el **valor máximo** obtenido en cualquiera de las tres dimensiones (C, I, D). Esto asegura que si un activo es vital en *Integridad* (como los estados financieros), sea tratado con la máxima prioridad, aunque su *Confidencialidad* sea menor.

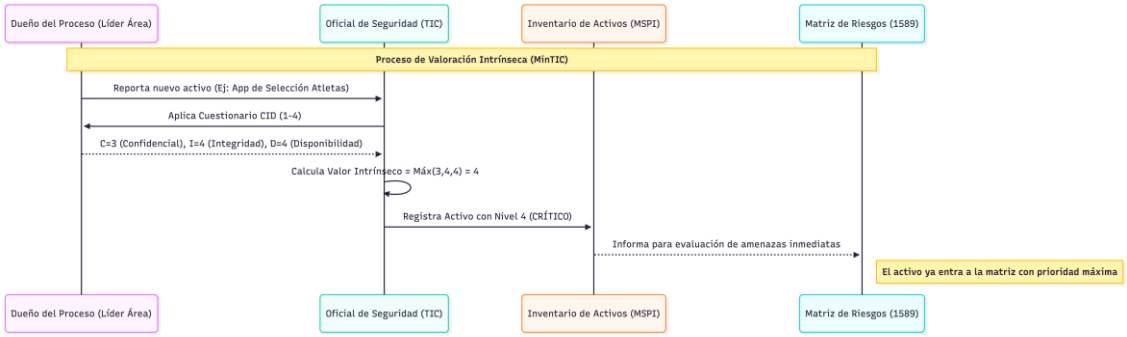
10.4. Análisis de Dependencias

De acuerdo con la guía del MinTIC, los activos no existen de forma aislada. La valoración intrínseca de la **Información** se hereda a los activos que la soportan:

- ✓ **Soporte Técnico:** Si el *Archivo Maestro Tributario* (Información) es nivel 4, el *Servidor Lenovo* (Hardware) donde se aloja adquiere automáticamente un nivel de criticidad 4.
- ✓ **Soporte Humano:** Los funcionarios del área financiera heredan la responsabilidad de nivel 4 en el manejo de sus credenciales.

Diagrama de Secuencia: Flujo de Valoración de un Nuevo Activo

Este diagrama representa cómo Indeportes debe valorar un activo antes de incluirlo en la matriz de riesgos, asegurando que se identifique su importancia real desde el inicio.



10.5. Beneficios de la Valoración para Indeportes

1. **Optimización Presupuestal:** Permite invertir en alta disponibilidad (servidores espejo) solo para activos con $D=4$.
2. **Cumplimiento MSPI:** Facilita la generación del reporte de activos críticos exigido por el MinTIC en las auditorías de Gobierno Digital.
3. **Priorización de Incidentes:** Ante dos fallas simultáneas, la Mesa de Ayuda atenderá primero el activo con mayor valor intrínseco.

11. Declaración de Aplicabilidad (SoA)

La SoA es el enlace directo entre la **Matriz de Riesgos (Capítulo 8)** y la estrategia técnica de la entidad. No basta con aplicar el control; el MinTIC exige documentar *por qué* se aplica y *cómo* se verifica.

11.1. Resumen de Aplicabilidad por Dominios

De los 4 dominios de la norma ISO 27001:2022, Indeportes prioriza los controles que blindan la información financiera y legal:

Dominio	Total Controles	Aplicados	Justificación de Selección
Organizacionales (5)	37	28	Gestión de activos, relaciones con proveedores y cumplimiento legal.
Personas (6)	8	8	Sensibilización y términos de contratación.
Físicos (7)	14	10	Seguridad en oficinas, archivos físicos y perímetros.
Tecnológicos (8)	34	30	Cifrado, backups, redes y gestión de incidentes.

11.2. Mapa de Controles Críticos (Extracto del SoA)

A continuación, se detallan los controles identificados como "obligatorios" en la matriz **de seguridad de la información.xlsx** para los procesos de **Gestión Legal, Financiera y Fomento**:

Código ISO	Nombre del Control	Estado	Justificación (Vínculo con Riesgo)
A.5.7	Clasificación de la información	**Sí**	Necesario para diferenciar datos públicos de datos sensibles de menores.
A.5.15	Control de acceso	**Sí**	Mitiga el acceso no autorizado a expedientes de tutelas y fallos judiciales.
A.5.23	Gestión de versiones	**Sí**	Vital para evitar el uso de archivos maestros tributarios obsoletos.

A.5.25	Protección de datos personales	**Sí**	Obligación legal (Ley 1581) para datos de deportistas.
A.8.11	Cifrado (Criptografía)	**Sí**	Protege los backups y datos de salud en reposo y tránsito.
A.8.13	Copias de respaldo	**Sí**	Garantiza la disponibilidad ante Ransomware o fallos de hardware.
A.8.16	Registro de eventos (Logs)	**Sí**	Provee trazabilidad de quién modificó información fiscal.

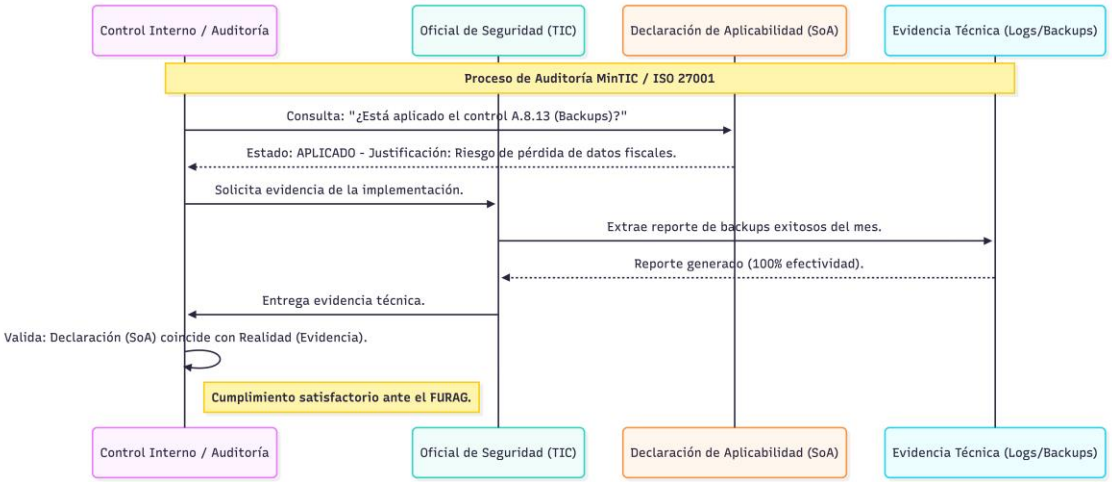
11.3. Justificación de Exclusiones

La norma ISO 27001 y el lineamiento dictado por MinTIC en su Documento maestro del MSPI, permite excluir controles siempre que se justifique. Ejemplo para Indeportes:

- ✓ **Control A.8.25 (Seguridad en el desarrollo de software):** Excluido temporalmente si la entidad no realiza desarrollo propio (in-house) y solo adquiere software comercial (como **SICOF**), trasladando la responsabilidad al proveedor mediante cláusulas contractuales.

Diagrama de Secuencia: Validación de Cumplimiento del SoA

Este diagrama ilustra cómo la entidad verifica que lo declarado en el SoA se cumple realmente en la operación diaria.



11.4. Mantenimiento del SoA

La Declaración de Aplicabilidad no es estática. Debe revisarse:

1. **Anualmente:** Durante la autoevaluación del MIPG.
2. **Ante cambios tecnológicos:** Si se migra a la nube (Cloud computing), se deben activar nuevos controles (ej. A.5.23 sobre servicios en la nube).
3. **Tras incidentes graves:** Para evaluar si un control excluido debería ser activado.

12. Definición del Apetito y Capacidad de Riesgo

12.1. Apetito de Riesgo

El **Apetito de Riesgo** es el nivel de riesgo que **Indeportes Antioquia** está dispuesto a aceptar en la búsqueda de sus objetivos institucionales antes de considerar que es necesario aplicar medidas de tratamiento.

- ✓ **Declaración Institucional:** Indeportes Antioquia tiene un apetito de riesgo **BAJO**. La entidad no está dispuesta a aceptar riesgos que comprometan la integridad de los datos de menores, la confidencialidad de los procesos judiciales o la transparencia de los recursos financieros.
- ✓ **Criterio de Aceptación:** Solo los riesgos ubicados en la zona **BAJA** de la matriz de calor (puntaje resultante ≤ 0.12 según pesos de la matriz de seguridad de la información) se consideran dentro del apetito y pueden ser "Aceptados" bajo monitoreo.

12.2. Capacidad de Riesgo

Es el nivel máximo de riesgo que la entidad puede soportar antes de que se produzca un incumplimiento grave de su misión o una quiebra técnica/legal.

- ✓ **Capacidad Financiera:** Definida por el impacto "Catastrófico" (> 500 SMLMV). Superar este umbral pondría en riesgo la ejecución presupuestal del fomento deportivo departamental.
- ✓ **Capacidad Legal:** Determinada por la capacidad de respuesta ante la **SIC** o la **Procuraduría**. La pérdida de personería jurídica o el cierre de sistemas misionales por sanción excede la capacidad de la entidad.
- ✓ **Capacidad Operativa:** Tiempo máximo de caída de servicios críticos (como **SICOF**) de 24 horas. Superar este tiempo se considera fuera de la capacidad operativa.

12.3. Tolerancia al Riesgo (Umbrales de Acción)

La tolerancia es la variación aceptable en el cumplimiento del apetito. Indeportes establece los siguientes umbrales basados en la **Matriz de Calor**:

Zona de Riesgo	Nivel de Tolerancia	Acción Requerida
BAJO	Dentro del Apetito	Aceptar y realizar seguimiento semestral.

MODERADO	Tolerancia Límite	Definir controles preventivos obligatorios; seguimiento trimestral.
ALTO	Fuera de Tolerancia	Implementar tratamiento inmediato (Reducir/Transferir); reporte a Subgerencia.
EXTREMO	Inaceptable	Intervención inmediata de la Gerencia; cese de actividad si no hay control.

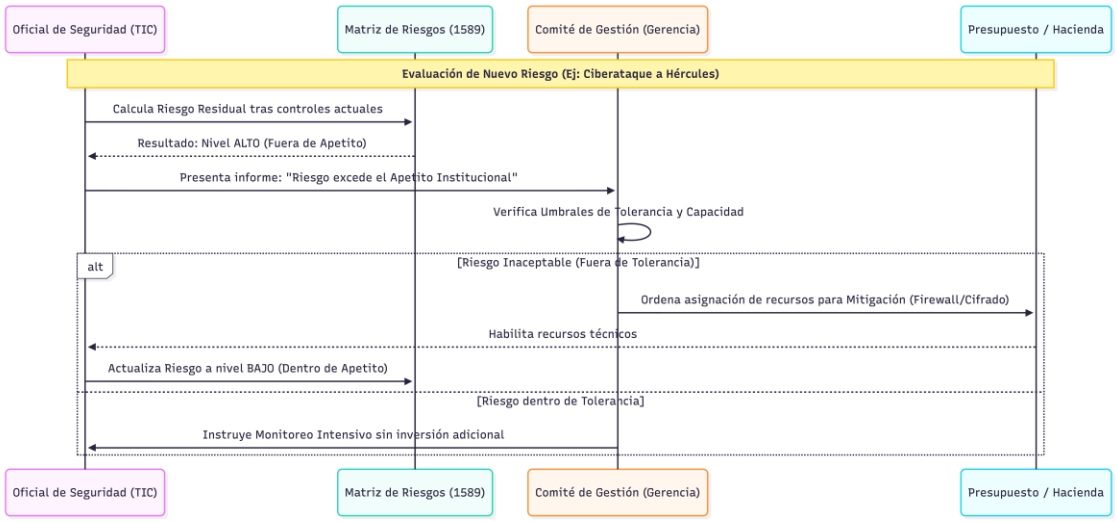
12.4. Matriz de Decisión según Apetito de Riesgo

Para asegurar que los recursos se asignen de manera eficiente, toda solicitud de presupuesto para ciberseguridad se evaluará bajo este flujo:

1. **¿El Riesgo Residual es > Moderado?** Aprobación prioritaria de recursos.
2. **¿El Riesgo afecta Activos Críticos (Valor 4)?** Aprobación inmediata.
3. **¿El costo del control supera la Capacidad de Riesgo?**Se opta por **Transferir** (Seguros) o **Evitar** (Cambio de proceso).

Diagrama de Secuencia: Validación de Apetito en la Toma de Decisiones

Este diagrama ilustra cómo la Gerencia de Indeportes utiliza el concepto de apetito para autorizar o rechazar el tratamiento de un riesgo.



Note right of C: Decisión alineada con los objetivos del MinTIC

Beneficios para Indeportes:

- ✓ **Blindaje Administrativo:** Los directivos tienen un sustento técnico para decidir cuándo invertir en tecnología.
- ✓ **Cumplimiento MinTIC:** Satisface el requisito del MSPI de definir formalmente el apetito de riesgo.
- ✓ **Enfoque en lo Crítico:** Evita el gasto de recursos en riesgos bajos, concentrándose en los que superan la capacidad de la entidad.

13. Plan de Continuidad (BCP) y Recuperación (DRP)

El objetivo es garantizar que los procesos críticos (Jurídico, Financiero y Fomento) no se detengan o se restablezcan en el menor tiempo posible.

13.1. Análisis de Impacto al Negocio (BIA)

Basándonos en la **Matriz de seguridad de la información** y la valoración de activos del **Capítulo 11**, definimos los tiempos de recuperación para los servicios críticos:

- ✓ **RTO (Recovery Time Objective):** Tiempo máximo permitido para restablecer un servicio tras una caída.
- ✓ **RPO (Recovery Point Objective):** Cantidad máxima de datos que la entidad se permite perder (medido en tiempo desde el último backup).

Proceso Crítico	Sistema / Activo	RTO (Tiempo de Recuperación)	RPO (Pérdida de Datos)
Gestión Financiera	SICOF / Archivo Maestro	8 Horas	24 Horas (Último Backup)
Gestión Jurídica	MERCURIO / Expedientes	4 Horas	12 Horas
Fomento Deportivo	HÉRCULES / Pólizas	12 Horas	24 Horas

13.2. Plan de Continuidad del Negocio (BCP)

Es la estrategia para seguir operando **mientras** los sistemas están caídos.

- ✓ **Modo de Contingencia Manual:** En caso de caída de **MERCURIO**, la Oficina Jurídica activará un libro radicador físico o planilla Excel encriptada temporal para no interrumpir los términos de las tutelas.
- ✓ **Comunicación de Crisis:** Protocolo para informar a los deportistas y proveedores sobre retrasos en pagos o procesos debido a la contingencia.

14.3. Plan de Recuperación ante Desastres (DRP)

Es el conjunto de acciones técnicas para reconstruir los sistemas tecnológicos.

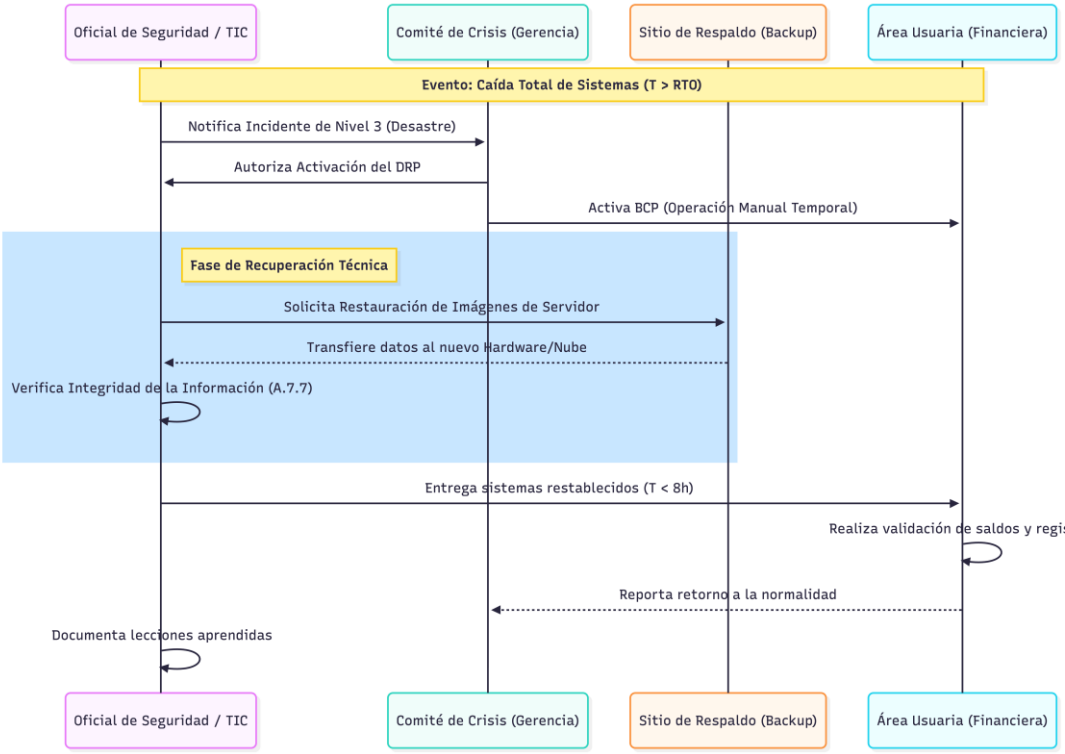
- ✓ **Estrategia de Restauración:** Priorización del servidor de base de datos sobre los servidores de aplicaciones.
- ✓ **Sitio de Respaldo:** Uso de la infraestructura de la Gobernación de Antioquia o nube híbrida para levantar servicios críticos si el hardware local (**Lenovo/Mikrotik**) sufre daño físico.
- ✓ **Pruebas de Escritorio:** Realización de un simulacro semestral de restauración de datos para garantizar que el **RTO** de 8 horas es cumplido por el equipo de TIC.

13.4. Niveles de Activación del Plan

1. **Nivel 1 (Incidente Menor):** Falla de un equipo individual. Se resuelve con soporte técnico estándar.
2. **Nivel 2 (Interrupción Parcial):** Caída de un servidor o del internet local. Se activan canales de backup (Mikrotik Dual-WAN).
3. **Nivel 3 (Desastre):** Pérdida total de datos o acceso al edificio. Se activa el BCP/DRP total y el Comité de Crisis.

Diagrama de Secuencia: Activación del DRP ante un Desastre Tecnológico

Este diagrama visualiza cómo actúa Indeportes cuando un evento crítico (ej. Ransomware o falla eléctrica mayor) paraliza la gestión financiera.



El diseño del BCP/DRP asegura que Indeportes Antioquia sea una entidad resiliente. Al tener metas claras de RTO y RPO, se reduce el riesgo de incumplimiento legal ante jueces y la pérdida de confianza de los deportistas, cumpliendo con el componente de "Continuidad" del Modelo de Seguridad del MinTIC.