Universidad Distrital Francisco José de Caldas

Facultad de Ingeniería

Maestría en Gestión y Seguridad de la Información

Proyecto metodología de gestión de riesgos

Juan David Mendoza Vargas – 20211020061

Andrés Felipe Pulido Suárez – 20211020049

Juan Sebastián Colorado Caro - 20202673001

Hamilton Camilo Espitia Rozo - 20211020038

Laura Daniela Cubillos Escobar - 20211020045

Miguel Angel Leguizamon Paez

Bogotá, Colombia

Septiembre de 2025

Proyecto metodología de gestión de riesgos

Tabla de contenido

Proyecto metodología de gestión de riesgos

1. Introducción

La seguridad de la información constituye un pilar fundamental en los procesos de transformación digital, dado que las organizaciones deben garantizar la protección de sus activos tecnológicos frente a posibles incidentes que comprometan su operación. Dentro de este contexto, el Banco de Bogotá ha implementado un proyecto estratégico de automatización en la creación de repositorios con el fin de optimizar la gestión, mejorar la trazabilidad y asegurar la gobernanza de sus desarrollos internos.

Sin embargo, la centralización y automatización inherente a este proceso agrega riesgos significativos, en especial aquellos relacionados con el manejo de credenciales y accesos privilegiados junto con la protección de información confidencial. El propósito de este proyecto fue aplicar una metodología de gestión de riesgos, utilizando los lineamientos de MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) para la valoración de activos, junto con los controles del Anexo A de ISO/IEC 27001:2022 para la identificación y evaluación de ciber-riesgos.

A través de este proceso riguroso, que incluyó la valoración de activos como credenciales privilegiadas y repositorios y la revisión de controles mediante auditoría y entrevistas estructuradas, se lograron identificar, analizar y evaluar las amenazas específicas que afectan el proceso. Dicho análisis ha culminado exitosamente en la elaboración de la Declaración de Aplicabilidad (SOA), que define con precisión el estado actual y el plan de tratamiento necesario para alcanzar el estado de madurez deseado. El presente trabajo detalla los resultados de la valoración cualitativa de los 12 ciber-riesgos identificados y propone el roadmap estratégico que fortalecerá la protección de los activos de información y la continuidad de los servicios de la organización.

2. Contextualización del proceso

2.1. Nombre de la Organización.

Banco de Bogotá.

2.2. Nombre del proceso o servicio

Automatización en la creación de repositorios de código.

2.3. Detalle de la información que es procesada

El proceso gestiona principalmente metadatos y configuraciones críticas para el desarrollo de software. La información tratada incluye:

- **Código fuente de aplicaciones:** Propiedad intelectual del banco y lógica de negocio.
- **Credenciales privilegiadas:** Secretos, tokens y contraseñas para el acceso y la administración de los repositorios y otros sistemas.
- **Datos de configuración:** Parámetros de conexión a bases de datos, librerías y configuraciones de entorno.
- **Información de trazabilidad:** Registros sobre a qué equipo pertenece un repositorio, a qué aplicación sirve y qué colaboradores tienen acceso.
- **Documentación técnica:** Manuales y guías de uso y configuración de los proyectos.

2.4. Descripción del proceso

Como parte de su estrategia de transformación digital, el Banco de Bogotá ha implementado un proyecto para automatizar la creación de repositorios de código. El objetivo es estandarizar y optimizar la gestión tecnológica, asegurando la gobernanza y trazabilidad de los desarrollos internos.

El servicio de automatización garantiza que cada nuevo repositorio se cree con una estructura predefinida, incluyendo la información esencial para identificar su propietario, la aplicación asociada y los colaboradores involucrados. Adicionalmente, el proceso configura automáticamente las librerías base y asigna los permisos de acceso correspondientes, reduciendo errores manuales y agilizando el ciclo de vida del desarrollo.

Aunque este proceso centralizado mejora la eficiencia, también introduce riesgos significativos. La gestión de credenciales con altos privilegios, necesarias para la automatización, se convierte en un punto crítico que, de ser comprometido, podría exponer la integridad, confidencialidad y disponibilidad de todos los activos de código de la organización.

3. Metodología de valoración de activos

3.1. Descripción

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es una metodología desarrollada por el Gobierno de España que busca identificar y gestionar los riesgos que afectan a los sistemas de información. Su propósito es proteger los activos más relevantes de una organización, garantizando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

En cuanto a la valoración de activos, MAGERIT establece que cada activo debe ser identificado y clasificado según su importancia para la organización. Esta evaluación se realiza con base en las siguientes dimensiones:

- **Confidencialidad:** ¿qué daño causaría que lo conociera quien no debe?
- **Integridad:** ¿qué perjuicio causaría que estuviera dañado o corrupto?
- **Disponibilidad:** ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?
- **Autenticidad:** ¿qué perjuicio causaría no saber exactamente quién hace o ha hecho cada cosa?
- **Trazabilidad:** ¿qué daño causaría no saber a quién hace algo y cuándo?

Adicionalmente, MAGERIT identifica los siguientes tipos de activo:

- **Datos,** que materializan la información.
- **Servicios,** que se necesitan para poder organizar el sistema.
- **Las aplicaciones informáticas (software),** que permiten manejar los datos.
- **Los equipos informáticos (hardware),** y que permiten hospedar datos, aplicaciones y servicios.
- **Los soportes de información,** que son dispositivos de almacenamiento de datos.
- **El equipamiento auxiliar,** que complementa el material informático.
- **Las redes de comunicación,** que permiten intercambiar datos.
- **Las instalaciones,** que acogen equipos informáticos y de comunicaciones.
- **Las personas,** que explotan u operan todos los elementos anteriormente citados.

3.2. Listado de activos valorados

Para el presente caso, usaremos la siguiente escala de valoración:

- **Alto (3):** Daño grave a la organización.
- **Medio (2):** Daño importante a la organización.
- **Bajo (1):** Daño menor a la organización.

1. Repositorio de código fuente
b. Descripción: Almacén centralizado donde se guarda el código fuente de las aplicaciones del banco, incluyendo configuraciones, librerías y documentación técnica.
c. Tipo de activo: Datos.

d. Criterios de valoración:

- **Confidencialidad:** Alto (contiene información sensible y propiedad intelectual).
- **Integridad:** Alto (cualquier alteración puede comprometer la seguridad y funcionalidad).
- **Disponibilidad:** Medio (una caída temporal afecta, pero existen copias y recuperación).
- **Autenticidad:** Alto (es fundamental garantizar que el código provenga de fuentes legítimas).
- **Trazabilidad:** Alto (se requiere auditar accesos y cambios).

e. Valor final del activo: Alto.

2. Credenciales privilegiadas

b. Descripción: Usuarios y sus contraseñas, que poseen acceso y permisos de administración de repositorios.

c. Tipo de activo: Datos.

d. Criterios de valoración:

- **Confidencialidad:** Alto (compromete todos los repositorios).
- **Integridad:** Alto (cualquier modificación puede cambiar el control de acceso).
- **Disponibilidad:** Alto (los usuarios autenticados deben acceder sin problemas en todo momento).
- **Autenticidad:** Alto (las credenciales deben ser legítimas).
- **Trazabilidad:** Alto (se debe registrar cualquier uso del repositorio).

e. Valor final del activo: Alto.

3. Aplicación de automatización de repositorios

b. Descripción: Plataforma que gestiona la creación estandarizada de repositorios.

c. Tipo de activo: Aplicaciones informáticas (software).

d. Criterios de valoración:

- **Confidencialidad:** Medio (maneja metadatos de los repositorios).
- **Integridad:** Medio (debe crear repositorios con parámetros correctos).
- **Disponibilidad:** Alto (si falla, no se pueden crear repositorios).
- **Autenticidad:** Alto (los repositorios que crea deben seguir los estándares definidos por la organización).
- **Trazabilidad:** Alto (se debe conocer qué repositorios fueron creados, cuándo y quién lo hizo).

e. Valor final del activo: Alto.

4. Controlador de versiones

b. Descripción: Software que permite almacenar, versionar y colaborar en el código fuente.

c. Tipo de activo: Aplicaciones informáticas (software).

d. Criterios de valoración:

- **Confidencialidad:** Medio (los repositorios privados requieren protección).
- **Integridad:** Alto (los cambios deben ser confiables y auditables).
- **Disponibilidad:** Alto (sin ella, los equipos de desarrollo quedan bloqueados).
- **Autenticidad:** Alto (el software debe ser oficial y seguro).

- **Trazabilidad:** Alto (es fundamental para el software registrar cambios de código y usuarios).

e. Valor final del activo: Alto.

5. Sistemas de respaldo
b. Descripción: Solución para generar copias de seguridad de los repositorios y configuraciones.
c. Tipo de activo: Equipamiento auxiliar.
d. Criterios de valoración:

- **Confidencialidad:** Medio (las copias deben protegerse frente a accesos no autorizados).
- **Integridad:** Alto (las copias deben ser fieles al original).
- **Disponibilidad:** Alto (se requiere acceso inmediato en caso de incidente).
- **Autenticidad:** Alto (se debe asegurar que la copia proviene del sistema original).
- **Trazabilidad:** Medio (conocer quién generó y/o restauró la copia).

e. Valor final del activo: Alto.

6. Red interna corporativa
b. Descripción: Infraestructura de comunicaciones que conecta equipos, aplicaciones y usuarios internos de la organización.
c. Tipo de activo: Redes de comunicaciones.
d. Criterios de valoración:

- **Confidencialidad:** Alto (transporta datos de los usuarios y sus acciones).
- **Integridad:** Alto (los paquetes no deben ser alterados).
- **Disponibilidad:** Alto (una interrupción paraliza las operaciones).
- **Autenticidad:** Alto (el tráfico debe provenir de fuentes legítimas).
- **Trazabilidad:** Medio (se monitorea el tráfico con logs).

e. Valor final del activo: Alto.

7. Centro de datos
b. Descripción: Instalaciones físicas que alojan servidores, redes y sistemas de almacenamiento.
c. Tipo de activo: Instalaciones.
d. Criterios de valoración:

- **Confidencialidad:** Medio (deben existir accesos físicos).
- **Integridad:** Alto (debe evitarse manipulación indebida de equipos).
- **Disponibilidad:** Alto (alberga sistemas críticos para operaciones).
- **Autenticidad:** Alto (la infraestructura debe estar certificada y soportada).
- **Trazabilidad:** Medio (se deberían registrar accesos físicos).

e. Valor final del activo: Alto.

8. Desarrolladores
b. Descripción: Colaboradores que utilizan y mantienen los repositorios con proyectos de software.
c. Tipo de activo: Personas.
d. Criterios de valoración:

- **Confidencialidad:** Alto (manejan información sensible en proyectos).
- **Integridad:** Medio (pueden cometer errores involuntarios en el desarrollo).
- **Disponibilidad:** Medio (su ausencia afecta, pero no es tan grave).
- **Autenticidad:** Alto (su identidad debe estar validada y autorizada).
- **Trazabilidad:** Bajo (sus actividades pueden ser registradas o se hace seguimiento a actividades).

e. Valor final del activo: Medio.

9. Documentación técnica en los repositorios
b. Descripción: Manuales, guías y procedimientos asociados a la configuración y uso de los repositorios.
c. Tipo de activo: Datos.
d. Criterios de valoración:

- **Confidencialidad:** Bajo (posee configuraciones internas).
- **Integridad:** Alto (debe estar actualizada y sin alteraciones).
- **Disponibilidad:** Medio (importante para referencia, pero no crítica inmediata).
- **Autenticidad:** Medio (se requiere confirmar que es oficial).
- **Trazabilidad:** Bajo (se registran cambios, pero no siempre en detalle).

e. Valor final del activo: Medio.

10. Servicio de autenticación
b. Descripción: Servicio que válida credenciales y controla accesos a repositorios y sistemas asociados.
c. Tipo de activo: Servicios.
d. Criterios de valoración:

- **Confidencialidad:** Alto (gestiona credenciales y roles).
- **Integridad:** Alto (los registros de usuarios deben ser confiables).
- **Disponibilidad:** Alto (su caída bloquea el acceso a sistemas).
- **Autenticidad:** Alto (es vital asegurar que valide usuarios legítimos).
- **Trazabilidad:** Alto (debe registrar accesos exitosos y fallidos).

e. Valor final del activo: Alto.

4. Metodología de evaluación del ciber riesgo

4.1 Recursos para Identificar Ciber-riesgos

4.1.1 Listado de Controles de Ciberseguridad

Para la identificación de ciber-riesgos en el proceso de automatización de repositorios del Banco de Bogotá, se utilizará el catálogo de amenazas de MAGERIT v3 junto con los controles del Anexo A de ISO/IEC 27001:2022. Esta combinación permite una evaluación exhaustiva de los riesgos potenciales.

Controles de ciberseguridad seleccionados según ISO 27001:2022:

A.5.1 - Políticas para la seguridad de la información
A.5.15 - Control de acceso

A.5.16 - Gestión de identidad
A.5.17 - Información de autenticación
A.5.18 - Derechos de acceso
A.8.1 - Dispositivos de usuario final
A.8.9 - Gestión de la configuración
A.8.10 - Borrado de información
A.8.12 - Prevención contra fuga de datos
A.8.16 - Actividades de monitoreo
A.8.23 - Seguridad de servicios web
A.8.24 - Uso de criptografía
A.8.28 - Codificación segura
A.8.32 - Gestión de cambios
A.8.34 - Protección de sistemas durante auditorías

4.1.2 Entrevistas/Reuniones: Listado de Preguntas

Se realizarán entrevistas estructuradas con los siguientes perfiles:

- Administradores de sistemas
- Desarrolladores senior
- Personal de seguridad informática
- Responsables del área de TI

Preguntas realizadas en la entrevista:

Sección 1: Gestión de Accesos y Credenciales

¿Cómo se gestiona actualmente el ciclo de vida de las credenciales privilegiadas para los repositorios?
¿Existe un proceso formal para la asignación y revocación de permisos en los repositorios?
¿Se implementa autenticación multifactor (MFA) para accesos privilegiados?
¿Con qué frecuencia se rotan las contraseñas de las cuentas administrativas?
¿Existe segregación de funciones en la administración de repositorios?

Sección 2: Seguridad del Código y Repositorios

6. ¿Se realizan análisis de código estático (SAST) antes de subir código al repositorio?
7. ¿Existe un proceso de revisión de código (code review) obligatorio?
8. ¿Cómo se protegen las ramas principales (master/main) contra cambios no autorizados?
9. ¿Se almacenan secretos o credenciales hardcodeadas en el código fuente?
10. ¿Existen políticas sobre el uso de librerías de terceros y su actualización?

Sección 3: Monitoreo y Auditoría

11. ¿Qué tipo de logs se generan y almacenan sobre las actividades en los repositorios?
12. ¿Existe monitoreo en tiempo real de actividades sospechosas?
13. ¿Con qué frecuencia se revisan los logs de auditoría?

14. ¿Se han detectado incidentes de seguridad relacionados con los repositorios en el último año?
15. ¿Existe un procedimiento de respuesta ante incidentes específico para los repositorios?

Sección 4: Respaldos y Continuidad

16. ¿Con qué frecuencia se realizan respaldos de los repositorios?
17. ¿Se prueban periódicamente las restauraciones de los respaldos?
18. ¿Los respaldos están cifrados y almacenados en ubicaciones seguras?
19. ¿Existe un plan de recuperación ante desastres para el servicio de repositorios?
20. ¿Cuál es el RTO (Recovery Time Objective) definido para los repositorios?

Sección 5: Automatización y Configuración

21. ¿Qué validaciones se realizan durante la creación automatizada de repositorios?
22. ¿Cómo se asegura de que las configuraciones por defecto sean seguras?
23. ¿Existe un proceso de hardening para los nuevos repositorios?
24. ¿Se realizan auditorías de configuración periódicamente?
25. ¿Qué controles existen para prevenir la creación no autorizada de repositorios?

4.2 Metodología de Valoración del Ciber-riesgo (Cualitativa)

Siguiendo las directrices de MAGERIT v3, se establece una metodología de valoración cualitativa basada en la evaluación del impacto y la probabilidad de materialización de las amenazas.

4.2.1 Escalas de Valoración del Impacto del Ciber-riesgo

Nivel	Valor	Descripción	Criterios según MAGERIT v3
Muy Alto (MA)	5	Daño extremadamente grave	- Pérdida total de la misión del servicio - Daños irreparables a la imagen institucional - Pérdidas económicas > 10% del presupuesto anual - Impacto en más del 75% de los usuarios - Sanciones regulatorias severas
Alto (A)	4	Daño grave	- Interrupción prolongada del servicio (> 24 horas) - Daño significativo a la reputación - Pérdidas económicas entre 5-10% del presupuesto - Impacto en 50-75% de usuarios - Multas regulatorias importantes

Medio (M)	3	Daño importante	- Interrupción del servicio entre 4-24 horas - Daño moderado a la imagen - Pérdidas económicas entre 1-5% del presupuesto - Impacto en 25-50% de usuarios - Requerimientos regulatorios
Bajo (B)	2	Daño menor	- Interrupción del servicio < 4 horas - Impacto limitado en la reputación - Pérdidas económicas < 1% del presupuesto - Impacto en 10-25% de usuarios - Observaciones de auditoría
Muy Bajo (MB)	1	Daño despreciable	- Degradación menor del servicio - Sin impacto en la imagen - Pérdidas económicas mínimas - Impacto en < 10% de usuarios - Sin implicaciones regulatorias

Tabla 1. *Escalas de impacto. Elaboración propia*

4.2.2 Escalas de Valoración de la Probabilidad del Ciber-riesgo

Nivel	Valor	Descripción	Frecuencia estimada según MAGERIT v3
Muy Alta (MA)	5	Casi seguro	- Ocurre varias veces al año - Probabilidad > 90% - Se espera que ocurra en circunstancias normales
Alta (A)	4	Probable	- Puede ocurrir una vez al año - Probabilidad 70-90% - Ha ocurrido en organizaciones similares
Media (M)	3	Posible	- Puede ocurrir cada 2-3 años - Probabilidad 30-70% - Podría ocurrir en algún momento
Baja (B)	2	Poco probable	- Puede ocurrir cada 5-10 años - Probabilidad 10-30% - Podría ocurrir en circunstancias excepcionales
Muy Baja (MB)	1	Raro	- Puede ocurrir cada 10+ años - Probabilidad < 10% - Solo en circunstancias excepcionales

Tabla 2. *Escalas de probablidad. Elaboración propia*

4.2.3 Escalas de Valoración Final del Ciber-riesgo (Severidad)

La valoración final del riesgo se calcula multiplicando el valor del impacto por el valor de la probabilidad:

Riesgo = Impacto × Probabilidad

Nivel de Riesgo	Rango de Valores	Descripción	Acción Requerida
Crítico	20-25	Riesgo inaceptable	Requiere acción inmediata. Implementación urgente de controles. Escalamiento a alta dirección
Alto	12-19	Riesgo importante	Requiere plan de acción prioritario. Implementación de controles en corto plazo (< 3 meses)
Medio	6-11	Riesgo moderado	Requiere plan de acción. Implementación de controles en mediano plazo (3-6 meses)
Bajo	3-5	Riesgo tolerable	Monitoreo periódico. Implementación de controles según disponibilidad de recursos
Muy Bajo	1-2	Riesgo aceptable	Aceptar el riesgo. Revisión anual de la valoración

Tabla 3. *Escalas de valoración final. Elaboración propia*

4.2.4 Mapa de Calor

Probabilidad	Impacto				
	MB (1)	**B (2)**	**M (3)**	**A (4)**	**MA (5)**
MA (5)	5	10	15	20	25
A (4)	4	8	12	16	20
M (3)	3	6	9	12	15
B (2)	2	4	6	8	10
MB (1)	1	2	3	4	5

Tabla 4. *Mapa de calor de la metodología de gestión de ciber-riesgos. Elaboración propia*

Leyenda:

Riesgo	Puntuación	Color
Crítico	20-25	
Alto	12-19	
Medio	6-11	
Bajo	3-5	
Muy Bajo	1-2	

Tabla 5. *Leyenda del mapa de calor. Elaboración propia*

5. Aplicación de la metodología

5.1. Resultados de los recursos implementados para identificar ciber-riesgos

Recurso 1 - Listado de controles (ISO/IEC 27001:2022 Anexo A) aplicado al proceso

Alcance: Controles A.5 (gobierno/identidad y acceso) y A.8 (operación/seguridad técnica) aplicados al servicio de la automatización de creación de repositorios y sus activos (credenciales privilegiadas, repositorio de código, controlador de versiones, backups, red interna, servicio de autenticación).

Evidencias /soportes:

E1. Gestión de tokens y secretos (A.5.17 / A.5.18 A.8.28)

Fecha/hora: 2025-09-12 10:34

Fuente: Auditoría de la plataforma de repositorios (registro de autenticación y eventos API)

Descripción del hallazgo: Se identificó el uso de un token de servicio (cuenta técnica svc-repo-bot) con permisos de creación y modificación de repositorios sin rotación por evento ni restricción por alcance de repositorio. Se observaron 27 invocaciones createRepository en el último mes desde el host interno 10.24.0.15. Además, el escaneo de secretos de los últimos 30 días reporta 2 hallazgos informativos de posibles claves embebidas en PRs cerrados.

Activos afectados: Credenciales privilegiadas; Repositorio de código

Controles ISO asociados: A.5.17 (Información de autenticación), A.5.18 (Derechos de acceso), A.8.28 (Codificación segura)

Conclusión: Implementación parcial de controles: faltan rotación por uso/incidente, scopes mínimos y secret-scanning bloqueante en PR.

Asociación a ciber-riesgos: CR-01 (token expuesto/abuso), CR-03 (secretos hardcodeados), CR-04 (exceso de privilegios)

E2. Gestión de cambios y trazabilidad (A.8.32 / A.8.16 / A.8.23)

Fecha/hora: 2025-09-18 16:20 (GMT-5)

Fuente: Revisión de “plantilla de repos” (IaC) y logs de auditoría de configuración

Descripción del hallazgo: La plantilla usada por la automatización permite crear repositorios públicos por defecto si no se redefine un parámetro (visibility=private ausente). Se verificó un cambio de plantilla (commit tpl-9f2a) sin RFC ni aprobación formal (solo merge de PR). Los logs de acceso se conservan 60–90 días, sin alertas por clonado masivo o *push* fuera de horario.

Activos afectados: Servicio de automatización; Controlador de versiones; Registros de auditoría

Controles ISO asociados: A.8.32 (Gestión de cambios), A.8.16 (Monitoreo), A.8.23 (Seguridad de servicios web)

Conclusión: Falta aprobación formal de cambios, retención de logs ≥180 días y detecciones de comportamiento anómalo.

Asociación a ciber-riesgos: CR-02 (supply chain/configuración), CR-05 (exposición por automatización), CR-12 (trazabilidad insuficiente)

Recurso 2 - Entrevistas estructuradas (Perfiles: Admin. Sistemas, Dev Sr., Seguridad/TI)

Entrevistas a Admins de sistemas, Devs senior, Seguridad y TI, con preguntas sobre accesos, MFA, rotación, código seguro, monitoreo y respaldos.

Evidencias /soportes:

E3. Entrevista a Administración de Sistemas (respaldo y continuidad) Anexo 1

Fecha/hora: 2025-09-09 09:15 (GMT-5) — Duración 35 min

Participantes: Líder de Infraestructura y Backups; Analista de Seguridad

Extracto relevante:

- Backups diarios de repos (snapshots incrementales) en el mismo *datacenter*; sin copia inmutable ni air-gap.
- **Última prueba de restauración:** 2025-06-20 (demoró 1 h 15 min).
- **RTO/RPO declarados:** 2 h / 24 h; no hay acuerdo formal con Desarrollo.

Conclusión: Respaldo no segregado e inmutable ausente → exposición a ransomware y fallas de recuperación.
Asociación a ciber-riesgos: CR-07 (respaldo inutilizable), CR-06 (indisponibilidad del VCS)

E4. Entrevista a Desarrollo (credenciales y código) Anexo 1

Fecha/hora: 2025-09-11 14:40 (GMT-5) — Duración 30 min

Participantes: Dev Sr. del equipo de automatización; AppSec

Extracto relevante:

- MFA obligatorio para usuarios humanos; tokens de servicio sin MFA (no aplica) y expiración a 180 días.
- Branch protection activo en repos core, inconsistente en equipos satélite.
- Dos casos en 2025 con secretos en PR detectados por *scanner*; se revocaron y se hizo *force-push*, sin post-mortem formal.

Conclusión: Buenas prácticas parciales; faltan estandarización de protecciones, revocación/rotación por incidente y post-mortems para evitar recurrencia.
Asociación a ciber-riesgos: CR-01, CR-03, CR-08 (phishing + abuso de acceso)

Recomendaciones derivadas (enlazadas a los hallazgos)

1. **Identidad y secretos:** tokens scoped y ephemerales, rotación por uso/incidente, revocación automatizada y secret-scanning bloqueante en PR.
2. **Gestión de cambios y monitoreo:** *branch protection* estandarizado en nuevas “plantillas”, retención de logs ≥180 días, alertas por clonado/push anómalo, RFC obligatorio para cambios de plantilla.
3. **Respaldo y continuidad:** backups inmutables y off-site/air-gapped, pruebas de restauración trimestrales, formalizar RTO/RPO.

5.2. Listado de ciber-riesgos valorados

Escalas usadas: Impacto y Probabilidad (1–5) y Riesgo = Impacto × Probabilidad con rangos de severidad (Muy Bajo 1–2, Bajo 3–5, Medio 6–11, Alto 12–19, Crítico 20–25).

ID	Descripción	Activo	Impacto	Prob.	Valor	Severidad
CR-01	El token de servicio expuesto y sin alcance restringido puede causar la creación o alteración masiva e incontrolada de repositorios.	Credenciales privilegiadas	5	3	15	Alto
CR-02	El uso de librerías de terceros sin control de seguridad implica el riesgo de inyección de código malicioso.	Controlador de versiones / Repos	4	4	16	Alto
CR-03	Las credenciales o secretos embebidos en el código fuente permiten el acceso no autorizado a sistemas.	Código / Credenciales	4	3	12	Alto
CR-04	Una gestión de roles deficiente en IAM puede ser explotada para lograr una elevación de privilegios.	Servicio de autenticación	4	3	12	Alto
CR-05	La configuración por defecto insegura de la automatización conlleva la exposición de información confidencial o propiedad intelectual.	Servicio de automatización	4	2	8	Medio
CR-06	Una vulnerabilidad en la infraestructura del Controlador de Versiones resultaría en la interrupción total del desarrollo.	Controlador de versiones	4	2	8	Medio
CR-07	Los sistemas de respaldo no segregados exponen a la imposibilidad de restauración tras un ataque de *ransomware*.	Sistemas de respaldo	5	2	10	Medio
CR-08	Un ataque de phishing exitoso contra un desarrollador podría	Repositorio de código	5	3	15	Alto

	permitir la exfiltración masiva de repositorios.					
CR-09	Los cambios en plantillas sin control formal generan una configuración errónea y persistente en nuevos repositorios.	Automatización / Configuración	3	3	9	Medio
CR-10	La vulnerabilidad de la red interna a la interceptación de tráfico facilita el robo de tokens o sesiones.	Red interna	4	2	8	Medio
CR-11	La asignación de permisos excesivos aumenta la probabilidad de fuga accidental de Propiedad Intelectual.	Repositorio de código	4	2	8	Medio
CR-12	La retención insuficiente de logs impide realizar auditorías completas o análisis forenses requeridos.	Repos / Autenticación	3	3	9	Medio

Tabla 6. *Listado de ciber-riesgos. Elaboración propia*

5.3. Mapa de calor

Se valoraron 12 ciber-riesgos del proceso de automatización de creación de repositorios. No hay críticos; 5 en banda Alta (I×P 12–16) y 7 en banda Media (I×P 8–10). La nube de puntos se concentra en celdas (Impacto 4–5, Probabilidad 2–3), lo que indica impactos potenciales elevados y probabilidades moderadas: un entorno con controles presentes pero aún incompletos/irregulares.

Prob\Imp	1	2	3	4	5
5					
4				CR-02	
3			CR-09, CR-12	CR-03, CR-04	CR-01, CR-08

2				CR-05, CR-06, CR-10, CR-11	CR-07
1					

Tabla 7. *Mapa de calor de los ciber-riesgos. Elaboración propia*

Leyenda

Severidad	Rango I×P	Color
Crítico	20–25	
Alto	12–19	
Medio	6–11	
Bajo	3–5	
Muy Bajo	1–2	

Tabla 8. *Leyenda del mapa de calor. Elaboración propia*

6. Estado esperado a 3 años.

6.1. Visión Estratégica a 3 Años.

El objetivo para el año 2028 es evolucionar el proceso de "Automatización en la creación de repositorios" de un estado de protección reactiva y manual a un estado de gobernanza automatizada, inmutable y predictiva. Actualmente, en 2025, el sistema se encuentra en un estado con controles parciales, una gestión de secretos manual/estática, backups in situ y un monitoreo basado en logs simples. En contraste, el estado esperado para 2028 es alcanzar la gestión de identidades efímera (Zero Trust), la inmutabilidad de la infraestructura y respaldos, y el monitoreo comportamental (UEBA).

6.2. Declaración de Aplicabilidad: Estado Esperado (3 Años).

Dominio A.5: Controles Organizacionales (Identidad y Acceso)

Control ISO 27001:2022	Estado Actual (Hallazgo Documentado)	Estado Esperado (Meta 3 Años)

A.5.15 Control de Acceso	Acceso privilegiado gestionado con tokens de larga duración (180 días) sin rotación por uso.	**Acceso Just-in-Time (JIT):** Implementación de privilegios elevados temporales que se revocan automáticamente tras completar la tarea. Integración total con RBAC granular.
A.5.17 Información de Autenticación	Uso de tokens de servicio (svc-repo-bot) con permisos amplios y sin MFA para cuentas de servicio.	**Secretos Efímeros:** Uso de bóvedas dinámicas (ej. Vault) donde las credenciales de servicio se generan al vuelo, son únicas por transacción y viven segundos (TTL corto).
A.5.18 Derechos de Acceso	Los tokens tienen permisos de creación/modificación sin restricción de alcance (scope) por repositorio.	**Least Privilege Automation:** Los tokens de automatización tendrán un alcance (scope) limitado estricta y únicamente al repositorio que están creando en ese milisegundo.

Tabla 9. *Controles organizacionales. Elaboración propia*

Dominio A.8: Controles Tecnológicos (Operación y Seguridad)

Control ISO 27001:2022	Estado Actual (Hallazgo Documentado)	Estado Esperado (Meta 3 Años)
A.8.12 Prevención de Fuga de Datos (Backups)	Backups diarios in situ (mismo datacenter), mutables y sin *air-gap*. RTO/RPO no formalizados.	**Resiliencia ante Ransomware:** Estrategia 3-2-1-1-0 implementada. Copias inmutables (WORM), una copia fuera de línea (*air-gapped*) y pruebas de restauración automatizadas mensualmente con reporte de integridad.
A.8.16 Actividades de Monitoreo	Retención de logs 60-90 días. Sin alertas para clonado masivo o comportamiento anómalo.	**Monitoreo Predictivo (UEBA):** SIEM con análisis de comportamiento de usuarios/entidades. Detección automática de exfiltración (ej. clonado de >5 repos en 1 min) con respuesta automatizada (bloqueo de usuario). Retención de 1 año.
A.8.28 Codificación Segura	Escaneo de secretos informativo (no bloqueante). Secretos *hardcodeados* encontrados en PRs cerrados.	**Prevention-First (Shift Left):** *Pre-commit hooks* obligatorios que impiden subir secretos. Si un secreto toca el repositorio, se revoca automáticamente en el proveedor de identidad en tiempo real.

A.8.32 Gestión de Cambios	Cambios en plantillas de automatización (IaC) sin aprobación formal (RFC) ni validación de seguridad previa.	**GitOps & Policy-as-Code:** Todo cambio en la infraestructura de repositorios pasa por un pipeline con validación automática de políticas (ej. OPA) que impide configuraciones inseguras (como repos públicos) antes del *merge*.
A.8.9 Gestión de la Configuración	Plantillas permiten crear repositorios públicos por defecto si no se especifica lo contrario (error humano posible).	**Configuración Segura por Diseño:** Las plantillas base tendrán "Secure Defaults" forzados. La creación de un repositorio público requerirá una doble aprobación (principio de cuatro ojos) en la plataforma.

Tabla 10. *Controles tecnológicos. Elaboración propia*

6.3. Hoja de Ruta de Implementación.

El plan de trabajo proyecta la maduración de la metodología de gestión de riesgos del proceso de automatización de repositorios del Banco de Bogotá a un modelo robusto y preventivo, pasando de un estado de controles parciales a uno de Zero Trust en un horizonte de tres años. La prioridad estratégica es mitigar los cinco riesgos identificados en la banda "Alta", junto con el riesgo CR-07 (Ransomware en respaldo), debido a su impacto crítico en la disponibilidad del servicio.

6.3.1. Año 1: Higiene Crítica y Remediación Inmediata.

El primer año se centra en el establecimiento de la higiene fundamental para "detener la sangría" de los riesgos más críticos. Una acción fundamental es resolver la vulnerabilidad de las credenciales privilegiadas que dan origen al riesgo CR-01 (Token expuesto) y CR-04 (Gestión deficiente de roles). Esto se logrará reduciendo drásticamente la vida útil de los tokens de servicio (actualmente con expiración a 180 días) e implementando la rotación automatizada por uso o incidente. Paralelamente, la seguridad del código se endurecerá mediante la implementación de Secret Scanning en modo bloqueante en los Pull Requests , previniendo que el riesgo CR-03 (Secretos hardcodeados) ingrese en el código fuente. Finalmente, la resiliencia ante un incidente de ciberseguridad se fortalecerá mediante la creación de copias de seguridad inmutables con segregación (air-gap), abordando directamente la debilidad de los backups actuales, que son mutables y se encuentran en el mismo datacenter , lo cual es vital para mitigar el riesgo CR-07.

6.3.2. Año 2: Gobernanza, Cadena de Suministro y Visibilidad.

La segunda fase se enfoca en estandarizar los procesos y establecer la trazabilidad necesaria para la auditoría y la gobernanza. Para mitigar el riesgo CR-02 (Librería de terceros vulnerable) , se implementará el análisis de composición de software (SCA) en modo bloqueante dentro del pipeline,

garantizando que no se incluyan dependencias con vulnerabilidades conocidas. La gestión de cambios será formalizada para atajar el riesgo CR-09 (Cambios sin control formal) , exigiendo la aprobación formal (RFC) del Comité de Arquitectura y un proceso de Policy-as-Code para cualquier modificación a las plantillas de automatización críticas. En términos de visibilidad, se solucionará la trazabilidad incompleta (CR-12) al centralizar todos los logs en un SIEM, extendiendo su retención más allá de los 90 días y configurando reglas de correlación específicas para detectar comportamientos anómalos, como la clonación masiva o los accesos fuera de horario.

6.3.3. Año 3: Automatización Avanzada y Ciber-resiliencia Total

El año final se dedica a la optimización y la implementación de controles avanzados que eliminan las causas raíz de los riesgos. El objetivo es evolucionar la gestión de identidades hacia un modelo de credenciales efímeras y Just-in-Time (JIT), eliminando la existencia de tokens estáticos y de larga duración. Esto reducirá a un riesgo residual la explotación de CR-01 y hará inviable el robo de sesiones por MitM interno (CR-10). Para prevenir la exfiltración de información sensible (Propiedad Intelectual) resultante de ataques de phishing (CR-08) , se implementará User and Entity Behavior Analytics (UEBA), que permitirá la detección predictiva de patrones de uso anómalos o sospechosos, incluso si un atacante utiliza credenciales legítimas. Finalmente, la capacidad de recuperación del servicio se garantizará formalmente a través de la institucionalización de pruebas de restauración trimestrales automatizadas, asegurando el cumplimiento de los objetivos RTO y RPO definidos con el negocio.

6.4. Resumen de Valor

Al completar este plan a 3 años, se espera que el Banco de Bogotá mitigue los riesgos de exposición de propiedad intelectual y credenciales privilegiadas , pasando de un nivel de riesgo "Alto" en la zona de calor actual a un nivel "Bajo" o "Muy Bajo", donde los controles son preventivos y automatizados, garantizando la gobernanza exigida en su transformación digital.

7. Conclusiones

El análisis de riesgos aplicado al proceso de automatización de repositorios del Banco de Bogotá ha permitido establecer un panorama claro de la postura de ciberseguridad actual. La valoración cualitativa, basada en la metodología MAGERIT v3, demostró que no existen riesgos críticos; sin embargo, el Mapa de Calor reveló 5 riesgos en la banda Alta y 7 riesgos en la banda Media. Esta concentración de riesgos se sitúa en las celdas de Impacto 4-5 y Probabilidad 2-3, lo cual evidencia impactos potenciales elevados con probabilidades moderadas. Esta condición es típica de un entorno donde existen controles, pero estos son incompletos, inconsistentes o se aplican de manera irregular.

Los riesgos clasificados como "Altos" convergen en cuatro vectores principales que exigen atención inmediata. Estos vectores son: (i) la gestión de identidades y secretos, manifestada en la problemática de los tokens de servicio y la necesidad de definir su alcance y rotación; (ii) la automatización y gestión de cambios, donde las plantillas de creación de repositorios carecen de puertas de control o de un Requerimiento Formal de Cambio (RFC) obligatorio; (iii) el monitoreo y la trazabilidad, que resultan insuficientes en términos de retención de logs y casos de uso para la detección de comportamiento anómalo; y, finalmente, (iv) la continuidad operativa, debido a que los backups carecen de inmutabilidad y segmentación (air-gap).

Por lo tanto, la prioridad de tratamiento debe enfocarse inmediatamente en los riesgos de nivel "Alto". Es imperativo abordar los riesgos CR-01, CR-03, CR-04 y CR-08 (relacionados con la identidad, secretos, abuso de acceso y phishing), junto con CR-02 (la cadena de suministro), con el objetivo primario de reducir su probabilidad a un valor de 2 y llevarlos de manera sostenible a la banda "Media" en el primer ciclo de mejora. Adicionalmente, el riesgo CR-07 (Ransomware en respaldo), a pesar de estar en la banda Media, requiere una acción de corto plazo por su alto impacto potencial. Las medidas deben incluir la implementación de inmutabilidad, segmentación o air-gap, formalización de los acuerdos RTO/RPO, y la realización de pruebas de restauración trimestrales para validar la capacidad real de recuperación de la organización.

8. Referencias

Amutio M, Candau J. (2012). MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado de: https://pilar.ccn-cert.cni.es/docman/documentos/1-magerit-v3-libro-i-metodo/file

González C. (2021). APLICACIÓN DE MAGERIT. Recuperado de: https://www.youtube.com/watch?v=7OGiWToXxX4

ISO 27001 annex A controls list. (2023, septiembre 26). Recuperado el 29 de septiembre de 2025, de High Table website: https://hightable.io/iso-27001-annex-a-controls-list/

Anexos.

Anexo 1. Entrevistas estructuradas — Respuestas (extractos)

Metodología: entrevistas semiestructuradas a tres perfiles clave del proceso de automatización de creación de repositorios. Duración por sesión: 25–40 min. Medio: videollamada corporativa. Formato: preguntas por dominio (identidad/credenciales, código/automatización, monitoreo/auditoría, respaldo/continuidad, gestión de cambios).

Fragmento R2-E1 — Administración de Sistemas (Backups/Continuidad)

- **Fecha/hora:** 2025-09-09 09:15 (GMT-5) — Duración: 35 min
- **Participantes:** Líder de Infra y Backups; Analista de Seguridad
- **Activos tratados:** Sistemas de respaldo; Controlador de versiones; Repositorios

Q1. Frecuencia y retención de copias de seguridad.
R: “Hacemos copias diarias con incrementales. Retención 30 días en el mismo *datacenter*. No contamos con copia inmutable ni off-site.”

Q2. Pruebas de restauración (última/tiempos).
R: “La última prueba fue el 2025-06-20; restaurar un repo de 8 GB tomó 1 h 15 min. No hay plan de pruebas trimestral.”

Q3. RTO/RPO acordados con desarrollo.
R: “Operativamente apuntamos a RTO 2 h / RPO 24 h, pero no está formalizado en acuerdo.”

Conclusión parcial: Respaldo no segregado, sin inmutabilidad ni *air-gap*; pruebas de restauración esporádicas.
Controles asociados: A.8.16, A.8.23 (monitoreo/servicios), A.8.32 (cambios).
Riesgos vinculados: CR-07 (respaldo inutilizable), CR-06 (indisponibilidad del VCS).

Fragmento R2-E2 — Desarrollo Senior (Credenciales/Código Seguro)

- **Fecha/hora:** 2025-09-11 14:40 (GMT-5) — Duración: 30 min
- **Participantes:** Dev Sr. Automatización; AppSec

- **Activos tratados:** Credenciales privilegiadas; Código fuente; Repositorios

Q1. MFA y credenciales/tokens de servicio.
R: “MFA es obligatorio para usuarios humanos. Los tokens de servicio expiran a 180 días; no se rotan por uso ni por incidente automáticamente.”

Q2. Protección de ramas y firmas.
R: “main y develop están protegidas en repos core; en equipos satélite hay inconsistencias. Firmas de commits recomendadas, no obligatorias.”

Q3. Secret-scanning/SAST/SCA en PR.
R: “Tenemos secret-scanning informativo y SAST/SCA no bloqueantes. En 2025 hubo 2 PR con secretos; se revocaron y se hizo *force-push*, sin post-mortem.”

Conclusión parcial: Buenas prácticas parciales; faltan rotación por evento, scope mínimo de tokens, checks bloqueantes y estandarización de protecciones.
Controles asociados: A.5.17, A.5.18 (identidad/acceso), A.8.28 (codificación), A.8.32.
Riesgos vinculados: CR-01, CR-03, CR-04, CR-08.

Fragmento R2-E3 — Seguridad TI / Monitoreo y Auditoría

- **Fecha/hora:** 2025-09-12 10:34 (GMT-5) — Duración: 28 min
- **Participantes:** Analista Blue Team; Responsable de Logs
- **Activos tratados:** Registros de auditoría; Servicio de autenticación; Red interna

Q1. Retención y cobertura de logs.
R: “Accesos a repos y autenticación se guardan 60–90 días. No tenemos correlación específica para ‘clonado masivo’ ni *push* fuera de horario.”

Q2. Alertas y casos de uso.
R: “Existen alertas por múltiples fallos de login y uso de IPs atípicas; no por creación masiva de repos o cambios de visibilidad.”

Q3. Detección en red (MitM/exfiltración).
R: “El tráfico hacia el VCS va por TLS. No hay inspección de payload; dependemos de telemetría del servidor y EDR en endpoints.”

Conclusión parcial: Cobertura/logs insuficiente para comportamientos anómalos relevantes del proceso; retención por debajo de mejores prácticas.

Controles asociados: A.8.16 (monitoreo), A.8.23 (servicios), A.8.32 (cambios).
Riesgos vinculados: CR-12 (trazabilidad), CR-05 (exposición por automatización), CR-10 (MitM/robo de sesiones).

Fragmento R2-E4 — Gestión de Cambios / "Plantilla de repos"

- **Fecha/hora:** 2025-09-18 16:20 (GMT-5) — Duración: 25 min
- **Participantes:** Owner plantilla IaC; Líder de Configuración
- **Activos tratados:** Servicio de automatización; Configuración como código

Q1. Flujo de cambios y aprobaciones.
R: "Los cambios a la plantilla van por PR; en un caso (commit tpl-9f2a) se fusionó sin RFC ni aprobación del CAB."

Q2. Parámetros de seguridad por defecto.
R: "El parámetro visibility no estaba fijado en private por defecto; se corrigió luego, pero la automatización no valida ese valor al crear."

Q3. Controles preventivos.
R: "No hay *policy checks* que bloqueen creación pública; confiamos en la revisión de PR y en que los equipos ajusten a mano."

Conclusión parcial: Falta control preventivo y gobierno de cambios formal para plantillas críticas.
Controles asociados: A.8.32 (cambios), A.8.16 (monitoreo).
Riesgos vinculados: CR-02, CR-05, CR-12.

Fragmento R2-E5 — Dueño del Proceso (PO) / Riesgo operativo

- **Fecha/hora:** 2025-09-19 11:05 (GMT-5) — Duración: 20 min
- **Participantes:** Product Owner; Representante de Cumplimiento
- **Activos tratados:** Repositorios; Roadmap de automatización

Q1. Criterios de aceptación y seguridad.
R: "La automatización prioriza velocidad de onboarding; seguridad se revisa en el post-merge. No hay *gates* obligatorios previos."

Q2. Conciencia de riesgos y comunicación.
R: “Conocemos el riesgo de exposición accidental; tenemos un *playbook* de reversión rápida, pero no un ejercicio programado.”

Conclusión parcial: Riesgo operativo subvalorado en la etapa previa a creación; faltan gates y simulacros.
Controles asociados: A.5.18, A.8.32.
Riesgos vinculados: CR-05, CR-11, CR-12.