

**POLÍTICA CORPORATIVA DE SEGURIDAD DEL DATO**

**PROGRAMA DE GOBIERNO DEL DATO**

13/08/2025

**Contenido**

[**1.** **INTRODUCCIÓN** 3](#_Toc208476818)

[**2.** **OBJETIVO** 3](#_Toc208476819)

[**3.** **ALCANCE** 3](#_Toc208476820)

[**4.** **PRINCIPIOS FUNDAMENTALES DE SEGURIDAD** 3](#_Toc208476821)

[**5.** **LINEAMIENTOS GENERALES** 3](#_Toc208476822)

[**6.** **ROLES Y RESPONSABILIDADES EN SEGURIDAD** 4](#_Toc208476823)

[**6.1** **Comité de Gobierno de Datos** 4](#_Toc208476824)

[**6.2** **Domain Owner** 4](#_Toc208476825)

[**6.3** **Data Owner** 4](#_Toc208476826)

[**6.4** **Data Steward (Analista de Gobierno del Dato)** 4](#_Toc208476827)

[**6.5** **Analista de Calidad y Seguridad del Dato** 4](#_Toc208476828)

[**6.6** **Analista de Diseño del Dato** 5](#_Toc208476829)

[**6.7** **Data User** 5](#_Toc208476830)

[**7.** **ESTÁNDARES Y CONTROLES DE SEGURIDAD** 5](#_Toc208476831)

[**7.1** **Clasificación y Etiquetado de Datos** 5](#_Toc208476832)

[**7.2** **Controles de Acceso** 5](#_Toc208476833)

[**7.3** **Protección de Datos** 6](#_Toc208476834)

[**7.4** **Prevención y Detección de Incidentes** 6](#_Toc208476835)

[**7.5** **Interoperabilidad Segura** 6](#_Toc208476836)

[**7.6** **Preservación y Eliminación Segura** 6](#_Toc208476837)

[**8.** **MONITOREO Y AUDITORÍA** 6](#_Toc208476838)

[**8.1** **Actividades de Monitoreo** 6](#_Toc208476839)

[**8.2** **Actividades de Auditoría** 7](#_Toc208476840)

[**8.3** **Roles y Funciones de Auditoría** 7](#_Toc208476841)

[**8.4** **Conservación de Registros** 7](#_Toc208476842)

[**9.** **REFERENCIA** 7](#_Toc208476843)

[**10.** **CONTROL DE VERSIONES** 8](#_Toc208476844)

[**11.** **APROBACIÓN** 8](#_Toc208476845)

1. **INTRODUCCIÓN**

Este documento establece los lineamientos para la gestión y gobierno de seguridad de datos en el ecosistema corporativo de datos, aplicable tanto para proyectos que incluyen una solución analítica completa como para los procesos de gestión y seguridad de datos. Esta política define los principios, responsabilidades y medidas necesarias para garantizar que los datos corporativos estén protegidos frente a accesos no autorizados, alteraciones indebidas, pérdida o divulgación inadecuada, sin importar el medio en el que se encuentren o el formato en el que se presenten.

1. **OBJETIVO**

Establecer los principios, lineamientos y responsabilidades para garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de los datos corporativos, en el marco del programa de Gobierno de Datos, asegurando su protección contra accesos no autorizados, pérdida, corrupción o divulgación indebida, independientemente de su formato, ubicación o sistema de origen.

1. **ALCANCE**

Esta política aplica a:

* Toda la información del corporativo, tanto estructurada (bases de datos, registros transaccionales, maestros, reportes) como no estructurada (documentos, imágenes, correos, planos, videos, etc.).
* Todas las áreas, filiales y operaciones del corporativo.
* Todos los roles definidos en el Gobierno de Datos (Domain Owner, Data Owner, Data Steward, Data User, entre otros).
* Todos los entornos: productivo, no productivo, nube, on-premises y dispositivos móviles.

1. **PRINCIPIOS FUNDAMENTALES DE SEGURIDAD**

* **Confidencialidad:** El acceso a los datos se concede únicamente a personas autorizadas y bajo el principio de mínimo privilegio.
* **Integridad:** Los datos deben mantenerse completos, consistentes y libres de alteraciones no autorizadas.
* **Disponibilidad:** La información debe estar accesible para los usuarios autorizados cuando sea requerida para fines de negocio.
* **Trazabilidad:** Toda acción sobre datos debe ser registrada y auditable.
* **Cumplimiento Normativo:** Toda gestión de datos debe alinearse a regulaciones locales e internacionales aplicables (como, por ejemplo: Ley de Protección de Datos Personales, ISO 27001, estándares internos).

1. **LINEAMIENTOS GENERALES**

* Todo acceso a datos debe ser gestionado a través de un proceso formal de autorización (Data User solicita acceso y la revisión funcional la realiza el Domain Owner, luego pasa por la validación de Gobierno de Datos y, por último, pasa por la validación de Seguridad de la Información).
* Los datos sensibles y estratégicos deben ser clasificados según niveles de seguridad (Confidencial, Interna, Pública).
* La transmisión y almacenamiento de datos sensibles debe utilizar cifrado y protocolos seguros.
* Se deben implementar controles de monitoreo para detectar accesos, modificaciones o transferencias inusuales.
* El ciclo de vida de la información (creación, almacenamiento, uso, archivado, destrucción) debe cumplir los estándares del Gobierno de Datos corporativo.

1. **ROLES Y RESPONSABILIDADES EN SEGURIDAD**

La gestión de la seguridad de datos requiere la coordinación de diferentes actores dentro del modelo de Gobierno de Datos Corporativo, asegurando que la confidencialidad, integridad y disponibilidad de la información se mantenga a lo largo de todo su ciclo de vida.

* 1. **Comité de Gobierno de Datos**
* **Funciones:**
  + Aprobar políticas, estándares y procedimientos de seguridad de datos.
  + Revisar y dar seguimiento a métricas e indicadores clave de seguridad.
  + Resolver incidentes de seguridad críticos o de impacto corporativo.
* **Responsabilidad:** Máxima autoridad de decisión en materia de seguridad de datos a nivel corporativo.
  1. **Domain Owner**
* **Funciones:**
  + Gobernar el dominio de datos asignado, asegurando que las políticas de seguridad y calidad se cumplan en todos los sistemas que lo manejan.
  + Coordinar la priorización de iniciativas de seguridad y calidad en su dominio.
  + Aprobar diseños, estructuras y reglas aplicables a los datos del dominio.
  + Valida si el acceso tiene sentido para el rol y las funciones del solicitante. Aprueba o rechaza desde la perspectiva del negocio.
* **Responsabilidad:** Custodia estratégica y aseguramiento de la coherencia entre datos del mismo dominio.
  1. **Data Owner**
* **Funciones:**
  + Hay que asegurar que los datos de su dominio cumplan con los estándares de seguridad establecidos.
  + Aprobar niveles de acceso y permisos para usuarios internos y externos.
  + Coordinar con el Data Steward la implementación de controles de seguridad.
* **Responsabilidad:** Custodia funcional y estratégica de la seguridad de los datos bajo su subdominio.
  1. **Data Steward (Analista de Gobierno del Dato)**
* **Funciones:**
  + Monitorear el cumplimiento de las políticas y estándares de seguridad en su dominio.
  + Identificar brechas de seguridad y proponer acciones correctivas.
  + Coordinar actividades de concientización y capacitación en seguridad de datos.
* **Responsabilidad:** Vigilancia operativa y control de cumplimiento.
  1. **Analista de Calidad y Seguridad del Dato**
* **Funciones:**
  + Validar que los datos cumplan con estándares de precisión, consistencia, integridad y actualidad.
  + Detectar errores, duplicados o datos faltantes que representen un riesgo para la seguridad o confiabilidad.
  + Trabajar en conjunto con el Analista de Seguridad para garantizar que la calidad de los datos no comprometa su protección.
  + Supervisa las funciones relacionadas con el Data Steward referente a los lineamientos de calidad y seguridad previamente establecidos.
* **Responsabilidad:** Asegurar que la calidad de los datos refuerce la seguridad y la confiabilidad de la información.
  1. **Analista de Diseño del Dato**
* **Funciones:**
  + Definir el modelo lógico y físico de datos, asegurando que cumpla estándares de seguridad y calidad desde su origen.
  + Documentar definiciones, metadatos y estructuras para facilitar la interoperabilidad.
  + Colaborar con los arquitectos de datos en la optimización y alineamiento del diseño de datos a las políticas corporativas.
* **Responsabilidad:** Diseño y definición de estructuras de datos seguras, consistentes y de alta calidad.
  1. **Data User**
* **Funciones:**
  + Utilizar la información de acuerdo con los permisos otorgados y políticas vigentes.
  + Reportar incidentes o usos indebidos de datos.
* **Responsabilidad:** Uso ético y responsable de la información.

1. **ESTÁNDARES Y CONTROLES DE SEGURIDAD**

Con el fin de garantizar la confidencialidad, integridad, disponibilidad y trazabilidad de la información corporativa, se establecen los siguientes estándares y controles aplicables a todos los datos, independientemente de su formato, ubicación o sistema de origen:

* 1. **Clasificación y Etiquetado de Datos**
* Todos los datos deben clasificarse según su nivel de sensibilidad (Público, Interno, Confidencial).
  + Dato Confidencial: dato de alta sensibilidad que debe ser protegido por su relevancia legal, financiera y estratégica.
  + Dato Interno: datos cuyo contenido debe mantenerse en el ámbito interno de la organización.
  + Dato Público: dato que ha sido preparado y aprobado para el uso público.
* De acuerdo al documento DG-GUI-IDSA-MINS-001-Guía de Checklist Integrado para Ingesta de Datos & Soluciones Analíticas v5.0, el Analista de Gobierno del Dato realiza esta clasificación del dato mediante los artefactos de Formato de Relevamiento y Mapeo para Ingesta, y el Diccionario de Datos. **Seguridad de la Información** será el encargado de validar y aprobar esta clasificación del dato de cada proyecto.
* La clasificación debe estar documentada en el Catálogo de Datos Corporativo.
  1. **Controles de Acceso**
* El acceso a los datos se otorga bajo el principio de mínimo privilegio y necesidad de conocer.
* Se debe aplicar autenticación multifactor para sistemas críticos y datos sensibles.
* El Analista de Seguridad y Calidad del Dato revisará mensualmente la vigencia y pertinencia de permisos.
  1. **Protección de Datos**
* Toda transmisión de datos sensibles debe realizarse mediante protocolos seguros (HTTPS, SFTP, VPN, TLS 1.2 o superior).
* Los datos en reposo deben cifrarse con estándares de al menos AES-256.
* Las copias de seguridad deben mantenerse cifradas y almacenadas en ubicaciones seguras.
  1. **Prevención y Detección de Incidentes**
* Se deben configurar alertas automáticas para detectar accesos no autorizados, anomalías de uso y cambios no planificados.
* Se deben definir umbrales de comportamiento normal para identificar desvíos.
  1. **Interoperabilidad Segura**
* Todo intercambio de datos con terceros debe cumplir con contratos y acuerdos de confidencialidad.
* Los procesos de integración deben pasar por validaciones de seguridad y pruebas de penetración antes de su puesta en producción.
  1. **Preservación y Eliminación Segura**
* Los datos obsoletos o sin uso deben ser eliminados de forma segura, siguiendo procedimientos certificados.
* El Analista de Diseño del Dato debe validar que la eliminación no afecte la integridad de procesos dependientes.

1. **MONITOREO Y AUDITORÍA**

El monitoreo y la auditoría son mecanismos esenciales para verificar el cumplimiento de esta política, detectar incidentes y mejorar continuamente la postura de seguridad de la organización.

Con esta sección, la política pretende:

* Garantizar que todos los accesos y manipulaciones de datos sean registrados, revisados y evaluados.
* Detectar comportamientos inusuales o no autorizados en el uso de datos.
* Asegurar la trazabilidad de las acciones sobre datos críticos y sensibles.
  1. **Actividades de Monitoreo**
* **Registro de eventos:** Todos los accesos, modificaciones, eliminaciones y descargas deben generar logs seguros e inalterables.
* **Alertas tempranas:** Configuración de sistemas que generen notificaciones ante patrones anómalos de uso.
* **Monitoreo continuo:** Herramientas y procesos automáticos que supervisen de forma permanente la seguridad y la integridad de los datos.
* **Revisión de accesos:** Validaciones periódicas de que los permisos asignados corresponden al principio de mínimo privilegio.
  1. **Actividades de Auditoría**
* **Auditorías internas:** Revisiones periódicas lideradas por el área de Gobierno de Datos y Seguridad de la Información.
* **Auditorías externas:** Evaluaciones realizadas por terceros independientes para validar el cumplimiento normativo y de buenas prácticas.
* **Evaluaciones de cumplimiento:** Contraste contra marcos regulatorios aplicables (ISO 27001, Ley de Protección de Datos Personales, SOX, etc.).
* **Informe de hallazgos y remediación:** Documentación de incumplimientos, vulnerabilidades y medidas correctivas con fechas y responsables.
  1. **Roles y Funciones de Auditoría**
* **Comité de Gobierno de Datos:** Aprobar planes de auditoría y recibir informes de hallazgos.
* **Analista de Seguridad y Calidad del Dato:** Coordinar la ejecución del monitoreo, analizar logs y generar reportes.
* **Analista de Diseño del Dato:** Validar que la arquitectura incluya trazabilidad y soporte de auditoría desde su diseño.
* **Domain Owner:** Garantizar la correcta aplicación de monitoreo y auditoría en su dominio.
* **Data Owner:** Revisar informes de acceso y aprobar cambios en permisos.
* **Data Steward:** Verificar que la metadata refleje los niveles de seguridad y controles asociados.
* **Data User:** Cumplir con las normas de uso y reportar cualquier anomalía detectada.
  1. **Conservación de Registros**
* Los logs y reportes de auditoría deberán conservarse por un período mínimo de 5 años o según lo establecido por la normativa aplicable.
* Todos los registros deberán estar protegidos contra modificaciones no autorizadas y accesibles solo para personal autorizado.

1. **REFERENCIA**

* DG-POL-PCGD-MINS-001-Política Corporativa de Gobierno de Datos.
* DG-MAN-INGS-MINS-001-Procedimiento de Ingesta con Calidad y Seguridad de Datos.
* DM-POL-TI-01.09 V-005 Política Específica de Gestión de Activos.
* DG-GUI-IDSA-MINS-001-Guía de Checklist Integrado para Ingesta de Datos & Soluciones Analíticas v5.0

1. **CONTROL DE VERSIONES**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versión** | **Fecha** | **Responsable** | **Cambios Realizados** | **Aprobado por** |
| 1.0 | 13/08/2025 | Jean Cabrera | Versión inicial | Comité Directivo |

1. **APROBACIÓN**

Esta política ha sido revisada y aprobada por el Comité Directivo y es de cumplimiento obligatorio para toda la organización.

[Nombre] Comité de Gobierno de Datos [Fecha]

**APROBACION DEL DOCUMENTO**

|  |  |  |  |
| --- | --- | --- | --- |
| **Cargo** | **Nombre** | **Firma** | **Fecha** |
| **Supervisor De Sistemas De Información** | Milagros Paico |  |  |
| **Jefe De Arquitectura Y Desarrollo Ágil** | Oscar Valencia |  |  |
| **Jefe De Seguridad De La Información** | Manuel Iturrizaga |  |  |
| **Jefe de Analytics** | Sthip Blas |  |  |
| **Jefe Data Engineering** | Luis Grados |  |  |
| **Superintendente TI Marcobre** | Marco Yacarini |  |  |
| **Supervisor de Aplicación Marcobre** | Jimmy Bendezú |  |  |
| **Superintendente de TI & OT** | Edwin Saldaña |  |  |
| **Gerente de TI & OT** | Dante Cárdenas |  |  |
| **Gerente de TD** | Piero Saravia |  |  |