# Informe Técnico – Taller 6: Checklist de Cumplimiento Normativo

## 1. Introducción

Este informe presenta los resultados de la aplicación del Checklist de Cumplimiento Normativo al caso base de referencia GobData, un portal estatal donde los ciudadanos realizan trámites digitales relacionados con identidad, salud, impuestos y derechos civiles. El objetivo es evaluar el cumplimiento de los principales marcos regulatorios aplicables, incluyendo la Ley 1581 de 2012 (Habeas Data), el Reglamento General de Protección de Datos (GDPR) y el estándar ISO/IEC 27001 de gestión de seguridad de la información.

## 2. Metodología

El equipo utilizó una plantilla de checklist que consolida controles clave de privacidad y seguridad. Cada requisito se evaluó con base en la normativa correspondiente, indicando si el sistema cumple, cumple parcialmente o no cumple. Las evidencias se obtuvieron de las políticas, funcionalidades y prácticas del sistema GobData. Se consideraron las siguientes normativas principales:

- Ley 1581 de 2012 y Decreto 1377 de 2013 (Colombia).

- ISO/IEC 27001:2022 – Controles de seguridad de la información.

- GDPR (Reglamento UE 2016/679).

- Guías de Habeas Data y Seguridad Digital de la SIC y MinTIC.

## 3. Resultados del Checklist

La evaluación del sistema GobData mostró un nivel de cumplimiento general del 70%. Se identificaron brechas principalmente en los procesos de retención de datos personales y en la implementación de controles de autenticación avanzada. A continuación se resumen los principales hallazgos:

|  |  |  |  |
| --- | --- | --- | --- |
| Área Evaluada | Brecha Detectada | Impacto | Recomendación |
| Consentimiento y Transparencia | No aplica revisión anual de políticas de privacidad. | Medio | Actualizar la política de privacidad cada año y documentar la aprobación del responsable del tratamiento. |
| Seguridad y Control de Acceso | No se implementa autenticación multifactor (MFA) para funcionarios. | Alto | Implementar MFA en los accesos administrativos y de funcionarios para reforzar la protección de credenciales. |
| Retención y Eliminación | No hay política definida de eliminación de datos personales. | Alto | Desarrollar una política formal de retención y eliminación conforme a la Ley 1581 y la ISO 27001 A.18.1.3. |
| Auditoría y Responsabilidad | No se realizan auditorías anuales documentadas. | Medio | Programar auditorías internas y externas al menos una vez al año para verificar cumplimiento. |

## 4. Recomendaciones Generales

Con base en los hallazgos, se recomienda que GobData implemente un plan de mejora continua en seguridad y privacidad, centrado en los siguientes puntos:

1. Incorporar autenticación multifactor (MFA) para accesos administrativos.

2. Definir una política formal de retención y eliminación de datos personales.

3. Realizar auditorías internas de cumplimiento anualmente.

4. Documentar y publicar actualizaciones de políticas de privacidad.

## 5. Conclusión

El caso GobData presenta un avance significativo en materia de cumplimiento normativo, con controles sólidos en las áreas de consentimiento, transparencia y trazabilidad. Sin embargo, aún existen brechas relevantes en la gestión del ciclo de vida de los datos y en la implementación de controles técnicos robustos. El cumplimiento de la Ley 1581, el GDPR y la ISO 27001 no solo protege la información de los ciudadanos, sino que refuerza la confianza pública en los servicios digitales del Estado.

## 6. Referencias

• Ley 1581 de 2012 – Protección de Datos Personales (Colombia)  
• Decreto 1377 de 2013 – Reglamentario de la Ley 1581  
• ISO/IEC 27001:2022 – Gestión de Seguridad de la Información  
• Reglamento General de Protección de Datos (GDPR – UE 2016/679)  
• Guía de Habeas Data de la Superintendencia de Industria y Comercio (SIC)  
• Guía de Seguridad y Privacidad Digital – MinTIC