

 ALCALDÍA MAYOR DE BOGOTÁ D.C. BOGOTÁ Unidad Administrativa Especial de Planeación y Mantenimiento Vial		FORMATO PLAN DE MEJORAMIENTO																		
CÓDIGO: CEI-FM-028												VERSIÓN: 1								
FECHA DE APLICACIÓN: NOVIEMBRE 2023																				
PROCESO / UNIDAD AUDITADA:				ESTRATEGIA Y GOBIERNO DE TI								AÑO:				2025				
RESPONSABLE DEL PROCESO / UNIDAD AUDITADA:				Saydee Katherine Mendivelso Montañez								FECHA DE DILIGENCIAMIENTO:				Septiembre				
ÍTEM	DESCRIPCIÓN DEL HALLAZGO DE AUDITORÍA /OPORTUNIDAD DE MEJORA/ NO CONFORMIDAD/ OBSERVACIÓN	ORIGEN (1)	CAUSA (2)	TIPO DE ACCIÓN A IMPLEMENTAR (3)	DESCRIPCIÓN DE LA ACCIÓN A IMPLEMENTAR (4)	INDICADOR (5)	FORMULA INDICADOR (6)	META DEL INDICADOR (7)	RESPONSABLE DE LA ACCIÓN A IMPLEMENTAR (8)	FECHA INICIO (9)	FECHA FIN (10)	AVANCE REPORTADO DE LA ACCIÓN A IMPLEMENTAR (11)					SEGUIMIENTO (12)			
												FECHA DE CORTE	RESULTADO DEL INDICADOR A LA FECHA DE CORTE	ESTADO	DESCRIPCIÓN DE LAS ACTIVIDADES REALIZADAS EN EL PERIODO	EVIDENCIA(S) SOPORTADA(S)	FECHA	RESULTADO DEL INDICADOR A LA FECHA DE CORTE	ESTADO	OBSERVACIONES
1	Hallazgo1: Bases de datos y Política de Tratamiento de Datos Personales desactualizadas en el RNBD.	Auditoría Interna		Corrección	1) Actualizar el procedimiento EGTI-PR-011 (armonizarlo con la Carilla 5 – Gobierno y Privacidad de la Información (Ámbito 5 - Ver anexo), corregir el error de la referencia al DUR-CIT, la referencia al numeral 2.3. de la Circular única SIC – Capítulo V y hacer notificaciones a través de la Mesa de ayuda.	Porcentaje de avance en la actualización del procedimiento en SIGESTION	(N° de cambios aprobados / Total de cambios proyectados) * (N° pasos de actualización realizados / Total pasos a realizar) * 100 Total de cambios proyectados = 4 Total de pasos a realizar = 11 según Instructivo Control de Información Documentada (DES-IN-002)	100% del Procedimiento actualizado y publicado en SIGESTION	Jefe OTI - Especialista en seguridad de la información	2025-11-24	2025-12-31									
		Auditoría Interna	Falta de institucionalización y control documental del ciclo RNBD en el SGSI. El procedimiento EGTI-PR-011 no está actualizado ni articulado (referencias normativas incorrectas, canal de notificación no trazable, instrumento no oficializado en SIGESTION) y no se integra con el mapa de riesgos (DES-FM-018) ni con la política vigente en el RNBD, lo que impide una ejecución y trazabilidad coherente.	Acción de Mejora	2) Crear el instrumento "Registro y/o Actualización BD" como formato del EGTI en el SIGESTION.	Porcentaje de implementación del formato en SIGESTION	(N° pasos de implementación realizados / Total pasos a realizar) * 100 Total de pasos a realizar = 11 según Instructivo Control de Información Documentada (DES-IN-002)	100% del Formato creado y publicado en SIGESTION	Jefe OTI - Especialista en seguridad de la información	2025-11-24	2025-12-31									
		Auditoría Interna		Acción Correctiva	3) Institucionalizar el riesgo de cumplimiento del RNBD en cada proceso (1ª línea) (Formato: DES-FM-018 - Procedimiento EGTI-PR-011 como Activo de Apoyo asociado a las BD personales tratadas en cada proceso) como parte de la actividad 2 del Plan de Tratamiento de Riesgos de Seguridad Digital de la vigencia 2025.	Porcentaje de líderes de procesos notificados del riesgo de cumplimiento del RNBD	(N° procesos notificados / Total de procesos) * 100 Total de procesos = 20	100% de líderes de procesos notificados	Jefe OTI - Especialista en seguridad de la información	2025-10-01	2025-12-31									
		Auditoría Interna		Corrección	4) Actualizar los Registros del RNBD que tienen la Versión 4 de la Política de Protección y Tratamiento de Datos Personales EGTI-DI-002 a la Versión 6, como ya aparece en el registro de la base de datos de "Bicisusuarios UMY".	Porcentaje de avance en la actualización de la versión 6 de la política en los registros del RNBD	(N° registros actualizados del RNBD / Total de registros a actualizar) * 100 Total de registros a actualizar = 28	100% de registros actualizados en el RNBD a la versión 6 de la Política de Protección y Tratamiento de Datos Personales EGTI-DI-002	Jefe OTI - Especialista en seguridad de la información	2025-11-24	2025-12-31									
2	Hallazgo2: Bases de datos registradas en el RNBD no incluidas en el Inventario de Activos de Información y viceversa	Auditoría Interna	Ausencia de un lineamiento control cruzado obligatorio que declare que toda base de datos personal es un activo de información y exija su registro sincronizado entre el RNBD (EGTI-PR-011) con el Inventario de Activos de (EGTI-PR-009).	Acción Correctiva	1) Actualizar los procedimientos de "Registro y Actualización de Bases de Datos" (EGTI-PR-011) y de "Gestión de Activos de Información" (EGTI-PR-009), para exigir un registro sincronizado en sus formatos asociados.	Procedimientos actualizados con control cruzado	(N° de procedimientos actualizados con control cruzado / 2) x 100	100% de procedimientos actualizados con control cruzado en SIGESTION	Jefe OTI - Especialista en seguridad de la información	2025-11-24	2025-12-31									
		Auditoría Interna		Acción Correctiva	2) Actualizar el Manual de Protección de Datos Personales (EGTI-MA-001) para obligar al registro de bases de datos como activos de información del SGSI.	Manual actualizado con la obligación de registro	(N° pasos de actualización realizados / Total pasos a realizar) * 100 Total de pasos a realizar = 11 según Instructivo Control de Información Documentada (DES-IN-002)	100% del manual actualizado	Jefe OTI - Especialista en seguridad de la información	2025-11-24	2025-12-31									
3	Hallazgo3: Formularios físicos y electrónicos no incluyen aviso de privacidad ni mecanismo para autorización previa	Auditoría Interna	Ausencia de un control de "privacidad por diseño", no existe en el SGSI un punto de control obligatorio para la creación/modificación y publicación de formularios físicos y electrónicos. Esto impide asegurar, antes de su uso, la inclusión del aviso de privacidad y los mecanismos de autorización previa, y dificulta el seguimiento por parte de los responsables del tratamiento.	Acción Correctiva	1) Diseñar e implementar un procedimiento interno para la revisión, aprobación y publicación de formularios que recolecten datos personales, garantizando la inclusión de avisos de privacidad completos y el mecanismo de autorización previa conforme a la normativa vigente.	Procedimiento interno diseñado e implementado	(N° pasos de implementación realizados / Total pasos a realizar) * 100 Total de pasos a realizar = 11 según Instructivo Control de Información Documentada (DES-IN-002)	Procedimiento creado y publicado en SIGESTION	Jefe OTI - Especialista en seguridad de la información	2026-01-01	2026-07-31									
		Auditoría Interna		Acción de Mejora	2) Capacitar a los responsables de cada proceso sobre la correcta implementación del aviso de privacidad y la autorización previa mediante una jornada de sensibilización del nuevo procedimiento.	Porcentaje de responsables capacitados	(N° de responsables capacitados / N° total de responsables convocados) x 100 N° total de responsables convocados = 20	100% de procesos de la UAERMV capacitados	Jefe OTI - Especialista en seguridad de la información	2026-01-01	2025-07-31									
				Corrección	3) Actualizar los formularios existentes para que cumplan con los requisitos legales y la política institucional, detallando de forma específica la finalidad del tratamiento, los derechos del titular y el canal para ejercerlos. EGTI, en su rol de primera línea corregirá el Formato bitácora de control de ingreso y salida al centro de cómputo (EGTI-M-023) y el Formato gestión de credenciales de acceso y novedades (EGTI-FM-030 -Derechos del titular)	Formularios actualizados conforme a normatividad	(N° de formularios actualizados / N° de formularios programados) x 100 N° de formularios programados EGTI = 2	100% de Formularios actualizados conforme a normatividad	Jefe OTI - Líder de Infraestructura	2025-12-01	2026-08-30									
4	Observación1: Manual de protección de datos desactualizado	Auditoría Interna	Desarticulación entre la Política de Protección y Tratamiento de Datos Personales (EGTI-DI-002) y el Manual (EGTI-MA-001)	Acción Correctiva	1) Actualizar el Manual de Protección de Datos Personales, asegurando su articulación con la Política de Protección y Tratamiento de Datos Personales (EGTI-DI-002) vigente, incorporando las modificaciones necesarias para cerrar las brechas identificadas por el equipo auditor (Tabla resumen de las principales brechas identificadas).	Manual actualizado con registro	(N° pasos de actualización realizados / Total pasos a realizar) * 100 Total de pasos a realizar = 11 según Instructivo Control de Información Documentada (DES-IN-002)	100% del manual actualizado	Jefe OTI - Especialista en seguridad de la información	2025-11-24	2025-12-31									
HALLAZGO: Registre el hallazgo (OPORTUNIDAD DE MEJORAR/NO CONFORMIDAD/ OBSERVACIÓN) completo, contenido en el informe de auditoría (1) ORIGEN: El origen pueden ser: Auditoría Interna, Auditoría Externa, Revisión por la Dirección, Tratamiento del Producto y/o Servicio No Conforme, Medición de Indicadores, Mapa de Riesgos, Autoevaluación del Proceso, Sistema de Gestión, Quejas y Reclamos, Normograma, OTRO; describa (2) CAUSAS: Registre la causa del hallazgo o riesgo materializado, que originó la situación detectada (formato: Análisis de Causas), sobre la cual se enfocará la acción. (3) TIPO DE ACCIÓN A IMPLEMENTAR: acción que subsane la causa que dio origen al hallazgo identificado, con el fin de solucionar las causas identificadas, para que no vuelvan a suceder. (4) DESCRIPCIÓN DE LA ACCIÓN A IMPLEMENTAR: Registre la(s) acción(es) que realizará descriptivamente, para corregir definitivamente la causa del hallazgo de Auditoría, Oportunidad de Mejora, No Conformidad u Observación. Inicie con un verbo en infinitivo. (5) INDICADOR: Registre el nombre del indicador a través de la cual se pueda observar el cumplimiento de la acción determinada. (Ej: informes, jornadas de capacitación, actas, etc.) (6) FORMULA INDICADOR: Determine las variables y la correspondiente fórmula del indicador que permite medir el cumplimiento de la acción determinada a implementar. (7) META DEL INDICADOR: registre la cantidad asociada a las actividades realizables y verificables de la acción correcta que se espera alcanzar en el tiempo definido, teniendo en cuenta la realidad institucional y recursos disponibles (Ej: 5 informes, 10 jornadas de capacitación, 3 actas, etc.). (8) RESPONSABLE DE LA ACCIÓN A IMPLEMENTAR: Señale el responsable Directivo o Jefe de Dependencia del proceso o unidad auditada, a la cual le corresponde ejecutar la acción correctiva a implementar. (9) FECHA DE INICIO: Indicar la fecha en que comienza cada acción a implementar registrada. El formato debe ser (AAAA/MM/DD). (10) FECHA FIN: Señale la fecha en que finaliza cada acción implementada. El formato debe ser (AAAA/MM/DD). Esta fecha NO PODRÁ SUPERAR 12 MESES contados a partir de la fecha de formulación del respectivo plan de mejoramiento. (11) AVANCE REPORTADO DE LA ACCIÓN A IMPLEMENTAR: En esta sección se deberá diligenciar los siguientes campos: Fecha de corte, Resultado del indicador a la fecha de corte, Estado, Descripción de las actividades realizadas en el periodo, Evidencia (s) soportada (s) Los procesos deben automatizarse calificando el estado de las acciones, de acuerdo al resultado del avance teniendo en cuenta los siguientes criterios: -En ejecución: Indica que la acción se está desarrollando en los plazos establecidos y se encuentra en términos. -Sin iniciar: Indica que aún no ha iniciado el plazo para realizar la implementación de la acción -Cancelada: Indica que la acción está cancelada y se adelantaron todas las acciones propuestas. -Vencida: Indica que la acción se está desarrollando fuera del plazo establecido. (12) SEGUIMIENTO: En esta sección se deberá diligenciar los siguientes campos: Fecha, resultado del indicador a la fecha de corte, estado y observaciones.																				