	INSTITUTO DE DESARROLLO URBANO			Aprobado	
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN			Enero 2023	
	ACCIONES ASOCIADAS AL PLAN DE TRATAMIENTO				
ACTIVO (Información)	**OPCIÓN Tratamiento** (Política)	**ACTIVIDADES DE TRATAMIENTO**	**SOPORTE** (evidencia de la actividad)	**RESPONSABLE**	**PLAZO**
Caja de seguridad	REDUCIR	Verificar y evaluar los controles que están operando de acuerdo con las políticas de seguridad para el manejo de las cajas de seguridad.	Informe de aplicación y seguimiento de controles.	Equipo de Seguridad de la Información	30/06/2023 31/12/2023
Carpetas y/o documentos compartidas en los servidores	REDUCIR	Verificar el cumplimiento de los procedimientos de copias de seguridad y restauración. Realizar dos (2) revisiones en el año a las políticas configuradas en el Directorio Activo	Informe de las revisiones	Equipo de Seguridad de la Información	30/05/2023 30/11/2023
Carpetas y/o documentos compartidos en Drive	REDUCIR	Identificar e implementar controles de DLP para la gestión de los documentos en Google Drive. Verificar que los controles están operando de acuerdo con las políticas de seguridad implementadas en Google Drive .	Informe de aplicación y seguimiento a controles implementados	Equipo de Seguridad de la Información	15/12/2023
Credenciales de acceso	REDUCIR	Realizar dos (2) revisiones sobre la configuración de cuentas privilegiadas y procedimientos de ingreso seguro al Directorio Activo. Realizar pruebas de ingeniería social.	Informe de Revisión Informes de las pruebas realizadas	Equipo de Seguridad de la Información	30/06/2023 30/11/2023
Servicios IDU	REDUCIR	Realizar análisis de vulnerabilidades de Hacking Ético. Seguimiento a la aplicación de actualizaciones de sistemas operativos y herramientas de capa media, incluyendo certificados SSL.	Informe de Hacking Ético Informe o evidencias de la actualización de los sistemas operativos, aplicaciones y/o certificados SSL	Equipo de Seguridad de la Información STRT	15/12/2023
Consola de administración y configuración de un sistema o software	REDUCIR	Realizar análisis de vulnerabilidades de Hacking Ético a las consolas de administración. Realizar revisiones sobre la configuración de cuentas privilegiadas y procedimientos de gestión de las cuentas de administración de las consolas.	Informe de Hacking Ético Informe de revisión a la gestión de cuentas de administración de las consolas	Equipo de Seguridad de la Información STRT	30/06/2023 30/11/2023
Código fuente + Repositorio	REDUCIR	Verificar y evaluar los controles que están operando de acuerdo con las políticas de seguridad para la protección de los códigos fuentes.	Informe de aplicación y seguimiento de controles.	Equipo de Seguridad de la Información	30/06/2022
Bases de datos	REDUCIR	Realizar análisis de vulnerabilidades de Hacking Ético a las bases de datos de los sistemas de información misional de la entidad.	Informe de Hacking Ético	Equipo de Seguridad de la Información STRT	30/06/2023 30/11/2023
Dispositivos externos de procesamiento o almacenamiento (BYOD)	REDUCIR	Identificar e implementar controles a través del MDM de Google Suite para controlar los dispositivos (BYOD) registrados. Verificar que los controles están operando de acuerdo con las políticas de seguridad implementadas para BYOD .	Informe de aplicación y seguimiento a controles implementados	Equipo de Seguridad de la Información STRT	10/08/2023 15/12/2023
Imagen Institucional	REDUCIR	Verificar controles que están operando de acuerdo con las políticas de seguridad de la entidad	Instrumento de autodiagnóstico del MSPI	Equipo de Seguridad de la Información	30/06/2023 31/12/2023