	PLAN DE ACCION DE IMPLEMENTACION SOSTENIBILIDAD O MEJORA DE SUBSISTEMAS DE GESTION			
idu	Código	FO-AC-24	Versión	2

Subsistema	Norma(s) Técnica(s) o Estándar de referencia	Fecha de Elaboración y/o Actualización			Fecha de Seguimiento			% de cumplimiento	% Esperado
SGSI	27001: 2013	20	Enero	2023				0%	30%

PLANEACIÓN									SEGUIMIENTO	
Id	OBJETIVO SUBSISTEMA	REQUISITO, COMPONENTE, DIMENSIÓN	ACTIVIDAD	FECHA DE INICIO	FECHA FIN	RESPONSABLE	PRODUCTO	RECURSOS	OBSERVACIÓN	AVANCE
1	Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos vigente	4.2 Comprensión de las necesidades y expectativas de las partes interesadas	Actualizar las necesidades y expectativas de los grupos de interés (partes interesadas) del SGSI	1-feb-23	31-mar-23	Equipo de Seguridad de la Información	Grupos de interés actualizados	Equipo de Seguridad de la Información Acompañamiento OAP		
2	Fortalecer la cultura de seguridad de la información en la Gente IDU.	5.3 Roles, responsabilidades y autoridades en la organización	Realizar seguimiento al plan estratégico del SGSI	2-ene-23	31-dic-23	Equipo de Seguridad de la Información	Presentaciones de los seguimientos estratégicos	Equipo de Seguridad de la Información Acompañamiento Jefes SGGC - DTAF - STRT		
3	Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos vigente	6. Planificación	Realizar semestralmente la actualización del Instrumento de autodiagnóstico del MSPI y el GAP de protección de datos personales	2-ene-23	31-dic-23	Equipo de Seguridad de la Información	Instrumento de autodiagnóstico del MSPI GAP de protección de datos personales	Equipo de Seguridad de la Información		
4	Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos vigente	6.1 Acciones para tratar riesgos y oportunidades 8.2 Valoración de riesgos de seguridad de la información 8.3 Tratamiento de riesgos de seguridad de la información	Actualizar y reportar los riesgos de seguridad de la información de acuerdo con los lineamientos institucionales y aquellos que se hayan materializado	2-ene-23	31-dic-23	Equipo de Seguridad de la Información	Reporte de los riesgos materializados a través de la Matriz de riesgos	Equipo de Seguridad de la Información Procesos		
5	Fortalecer la cultura de seguridad de la información en la Gente IDU.	7.2 Competencia 7.3 Toma de conciencia	Definir y elaborar el plan de capacitación y el plan de comunicación y divulgación del SGSI	2-ene-23	31-ene-23	Equipo de Seguridad de la Información	Plan de capacitación definido Plan de comunicaciones definido	Equipo de Seguridad de la Información Acompañamiento OAC		
6	Fortalecer la cultura de seguridad de la información en la Gente IDU.	7.2 Competencia 7.3 Toma de conciencia	Realizar seguimiento al plan de capacitación y al plan de comunicación y divulgación del SGSI	1-feb-23	31-dic-23	Equipo de Seguridad de la Información	Documento de seguimiento al Plan de capacitación y evidencias de su ejecución y al plan de comunicación y divulgación y evidencias de su ejecución	Equipo de Seguridad de la Información Acompañamiento STRH		

7	Fortalecer la cultura de seguridad de la información en la Gente IDU.	7.3 Toma de conciencia. A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información	Llevar a acabo el día de la Seguridad Llevar a cabo tres (3) eventos "Hablemos de Seguridad sin tapujos"	1-mar-23	30-nov-23	Equipo de Seguridad de la Información	Grabaciones de las sesiones Presentaciones Evaluaciones de la actividad	Piezas de divulgación Plataformas de conexión virtual Acompañamiento OAC		
8	Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos vigente	7.5 Información documentada	Actualizar la documentación que requiera ser ajustada de acuerdo con los lineamientos institucionales y normativos aplicables Actualizar la declaración de aplicabilidad (último trimestre)	2-ene-23	31-dic-23	Equipo de Seguridad de la Información	Documentos actualizados	Equipo de Seguridad de la Información Acompañamiento OAP		
9	Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos vigente	A.8 Gestión de activos	Gestionar la implementación de la clasificación y etiquetado de la información por parte de los colaboradores, en coordinación con el subsistema de gestión documental.	2-ene-23	31-dic-23	Equipo de Seguridad de la Información	Pieza de divulgación Capacitaciones Documentos Instructivos	Mesas de trabajo con el subsistema de gestión documental		
10	Elevar el nivel de madurez de los controles de seguridad de la información, pasando el 50% de ellos a nivel L4 y asegurando el 50% restante en L3.	A.9.4.4 Uso de programas utilitarios privilegiados A.12 Seguridad de las operaciones	Realizar dos (2) revisiones sobre la configuración de cuentas privilegiadas y procedimientos de ingreso seguro al Directorio Activo Realizar dos (2) revisiones en el año de las políticas configuradas en el Directorio Activo	2-ene-23	31-dic-23	Equipo de Seguridad de la Información	Evidencias de aplicación de controles Informes de revisiones	Usuario de dominio Herramienta de revisión del Directorio Activo		
11	Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos vigente	A.12.6 Gestión de la vulnerabilidad técnica	Realizar tres (3) pruebas de ingeniería social. Realizar dos (2) pruebas de Hacking Ético	2-ene-23	31-dic-23	Proveedor seleccionado del proceso de Hacking Ético Equipo de Seguridad de la Información	Informes Actas o grabaciones de las reuniones	Contrato de servicio de Hacking Ético		
12	Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos vigente	A.12.6.1. Gestión de las vulnerabilidades técnicas	Realizar seguimiento al plan de remediaciones de las vulnerabilidades técnicas identificadas	2-ene-23	31-dic-23	Equipo de Seguridad de la Información	Plan de remediaciones de las vulnerabilidades	Colaboradores de la STRT Recursos Tecnológicos Contrato de servicio de Hacking Ético		
13	Elevar el nivel de madurez de los controles de seguridad de la información, pasando el 50% de ellos a nivel L4 y asegurando el 50% restante en L3.	A.16 Gestión de incidentes de seguridad de la información.	Planear y realizar un simulacro de incidentes de seguridad de la información por semestre y comunicar el resultado obtenido a las personas involucradas.	2-ene-23	31-dic-23	Equipo de Seguridad de la Información	Informes Actas o grabaciones de las reuniones	Colaboradores de la STRT Recursos Tecnológicos		

14	Elevar el nivel de madurez de los controles de seguridad de la información, pasando el 50% de ellos a nivel L4 y asegurando el 50% restante en L3.	A.18 Cumplimiento	Revisar y actualizar el Normograma con los requisitos legales y/o normas aplicables al SGSI.	1-feb-23	31-dic-23	Equipo de Seguridad de la Información	Normograma actualizado	Equipo de Seguridad de la Información Acompañamiento SGJ		
15	Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos vigente	A.18.1.2 Derechos de propiedad intelectual	Realizar una revisión semestral del licenciamiento del software instalado en los equipos de usuario y programar tareas para la depuración de software no autorizado identificado	2-ene-23	31-dic-23	Equipo de Seguridad de la Información	Informes o reporte de la revisión Correos de gestión	Recursos Tecnológicos Reportes de la herramienta de gestión de equipos de usuario		
16	Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos vigente	A.12.6.1. Gestión de las vulnerabilidades técnicas	Realizar 12 análisis de vulnerabilidades técnicas controladas sobre las aplicaciones de la entidad	2-ene-23	31-dic-23	Equipo de Seguridad de la Información	Informes del análisis	Aplicaciones Equipo de Seguridad de la Información Herramientas de análisis de vulnerabilidades		
17	Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos vigente	9.1 Monitoreo, medición, análisis y evaluación	Atender la Auditoría Externa de seguimiento SGSI	2-oct-23	30-nov-23	Equipo de Seguridad de la Información	Informe de auditoría	Auditores externos Procesos del alcance Acompañamiento OAP		
18	Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos vigente	9.2 Auditoría interna	Atender la Auditoría Interna SGSI	1-may-23	30-sep-23	Equipo de Seguridad de la Información	Informe de auditoría	Auditores OCI Procesos del alcance		
19	Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos vigente	9.3 Revisión por la dirección	Realizar la revisión por la Dirección del SGSI	2-ene-23	31-dic-23	Equipo de Seguridad de la Información Alta Dirección	Acta de Comité MIPG Presentación de Comité	Equipo de Seguridad de la Información Acompañamiento OAP		
20	Elevar el nivel de madurez de los controles de seguridad de la información, pasando el 50% de ellos a nivel L4 y asegurando el 50% restante en L3.	ISO 27001:2013 Anexo A	Actualizar metodología de valoración de la madurez de controles	2-ene-23	31-mar-23	Equipo de Seguridad de la Información	Metodología de valoración de la madurez de controles actualizada	Equipo de Seguridad de la Información		

21	Elevar el nivel de madurez de los controles de seguridad de la información, pasando el 50% de ellos a nivel L4 y asegurando el 50% restante en L3.	ISO 27001:2013 Anexo A	Hacer seguimiento cuatrimestral al nivel de maduración de los controles de seguridad de la información	2-ene-23	31-dic-23	Equipo de Seguridad de la Información	Documento de valoración de madurez de controles de seguridad de la información	Equipo de Seguridad de la Información		
22	Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos vigente	ISO 27701:2018	Definir el plan de acción de la norma ISO 27701:2019 asociada con la privacidad de la información.	2-ene-23	30-jun-23	Equipo de Seguridad de la Información STRT OAP	Plan de acción de la norma ISO 27701:2018 aprobado	Equipo de Seguridad de la Información OAP		
23	Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos vigente	ISO 27701:2018	Hacer seguimiento trimestral al plan de acción de la norma ISO 27701:2019 asociada con la privacidad de la información.	3-jul-23	31-dic-23	Equipo de Seguridad de la Información	Documento de seguimiento del plan de acción de la norma ISO 27701:2018	Equipo de Seguridad de la Información Dueños de procesos		
24	Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos vigente	ISO 27001:2013 Anexo A ISO 27001:2022 Anexo A	Realizar diagnóstico del SGSI sobre la versión de la ISO 27001:2022	1-sep-23	31-dic-23	Equipo de Seguridad de la Información	Diagnóstico del SGSI sobre la versión de la ISO 27001:2022	Equipo de Seguridad de la Información Acompañamiento OAP		
25	Administrar los riesgos de seguridad de la información para mantenerlos o reducirlos hasta un nivel Moderado o Inferior, aplicando el plan de tratamiento de riesgos vigente	ISO 27001:2013 Anexo A ISO 27001:2022 Anexo A	Gestionar la capacitación de los colaboradores en la nueva la versión de la ISO 27001:2022	3-abr-23	31-dic-23	Equipo de Seguridad de la Información OAP	Colaboradores capacitados versión ISO 27001:2022	Equipo de Seguridad de la Información Acompañamiento OAP		
									% Cumplimiento	0%