CONTENIDO

1 OBJETIVO

Describir la forma en la cual el Instituto de Desarrollo Urbano aborda los controles de seguridad de la información.

2 ALCANCE

Esta Declaración de Aplicabilidad abarca todos los activos de información del Instituto, incluyendo datos, sistemas de información, el conocimiento de las personas, la plataforma informática, los servicios y cualquier otro componente relacionado con la seguridad de la información.
Además, facilita la comunicación interna y externa sobre las medidas de seguridad implementadas y es esencial para el cumplimiento con la norma ISO 27001:2022 durante el proceso de auditoría.

3 JUSTIFICACIÓN

Contar con una Declaración de Aplicabilidad permite personalizar los controles de seguridad para abordar de manera específica y eficiente los riesgos identificados.

4 RESPONSABILIDADES

Oficial de Seguridad de la Información:

- Liderar la elaboración y revisión de la Declaración de Aplicabilidad.
- Asegurar que los controles seleccionados sean apropiados y eficaces.
- Informar a la alta dirección sobre el estado de la Declaración de Aplicabilidad.

Alta Dirección

- Aprobar la Declaración de Aplicabilidad y asegurar que esté alineada con los objetivos estratégicos de la organización.
- Proporcionar los recursos necesarios para implementar y mantener los controles de seguridad.

Equipo de seguridad de la información

- Identificar y evaluar los riesgos de seguridad de la información.
- Proponer los controles a ser incluidos en la Declaración de Aplicabilidad basados en el análisis de riesgos.

Líder del Subsistema de Gestión de Seguridad de la Información

- Asegurar que la SOA cumpla con las leyes y regulaciones aplicables.
- Realizar auditorías internas para verificar la efectividad de los controles.

Equipo de la STRT

- Implementar los controles técnicos definidos en la SOA.
- Monitorear la efectividad y eficiencia de los controles implementados.

5 MARCO NORMATIVO

- Ley 23 de 1982. Ley sobre derechos de autor
- Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso, uso de los mensajes de datos, del comercio electrónico, las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 1273 de 05 de enero de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado de la protección de la información y de los datos-, preservando integralmente los sistemas utilizados en las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1450 de 2011. Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.
- Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014. Por medio de la cual se crea la ley de transparencia, como también el derecho de acceso a la información pública nacional, dictándose otras disposiciones.
- Directiva Presidencial 03 de 2021. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- Resolución 2710 DE 2017, Por la cual se establecen lineamientos para la adopción del protocolo IPv6.
- Resolución 001519 de 2020 de MINTIC. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014, definiéndose los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, así mismo los datos abiertos.
- Resolución 00500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital, adoptando el modelo de seguridad, además el de privacidad, como habilitador de la política de Gobierno Digital.
- Resolución 1126 de 2021 de MINTIC. Por la cual se modifica la Resolución 2710 de 2017.
- Resolución Distrital 305 de 2008. Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información, comunicaciones respecto a la planeación, seguridad, democratización, caridad, racionalización del gasto, conectividad, infraestructura de Datos Especiales e incluso Software Libre.
- Resolución 004 de 2017. Por la cual se modifica la Resolución 305 de 2008 de la CDS.

- Documento CONPES 3701 de 2011 - Lineamientos de Políticas sobre ciberseguridad y ciberdefensa.
- Documento CONPES 3854 de 2016 - Política Nacional de Seguridad Digital.
- Documento CONPES 3975 de 2019 - Política Nacional para la Transformación Digital e Inteligencia Artificial.
- Documento CONPES 3995 de 2020 - Política Nacional De Confianza y Seguridad Digital.
- NTC/ISO 27001:2013. Sistemas de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

Nota: Las normas de aplicación general y documentos internos (circulares, resoluciones, memorandos) que son parte de este documento, están relacionadas en el normograma del proceso Tecnologías de Información y comunicación publicado en el mapa de procesos.

6 TÉRMINOS Y DEFINICIONES

Los términos y definiciones aplicables al procedimiento pueden ser consultados en el micro sitio Diccionario de términos IDU (https://www.idu.gov.co/page/transparencia/informacion-de-interes/glosario).

- **Activos de Información**
- **Alta Dirección**
- **Amenaza**
- **Anexo A de la norma técnica NTC - ISO / IEC 27001:**
- **Autoridades**
- **Ciberseguridad**
- **Clasificación de la Información**
- **Controles de Seguridad de la Información**
- **Declaración de Aplicabilidad (SOA)**
- **Equipo de Seguridad de la Información**
- **Estado del Control**
- **Gestión de Incidentes de Seguridad de la Información**
- **Grupos de Interés Especial**
- **Información de Autenticación**

- **Inteligencia de Amenazas**
- **Marco Normativo**
- **Oficial de Seguridad de la Información**
- **Políticas de Seguridad de la Información**
- **Privacidad y Protección de Información de Identificación Personal (IIP)**
- **Proceso Disciplinario**
- **Registros**
- **Responsabilidades**
- **Revisión Independiente**
- **Riesgos de Seguridad de la Información**
- **Roles y Responsabilidades de SI**
- **Segregación de Funciones**
- **Servicios en la Nube**
- **Sistemas de Información**
- **STRT**
- **Trabajo a Distancia**
- **Transferencia de la Información**
- **Uso Aceptable de la Información y Otros Activos Asociados**
- **Vulnerabilidades Técnicas**

7 DECLARACIÓN DE APLICABILIDAD

A continuación, se presenta la Declaración de Aplicabilidad del IDU, tomando como base el Anexo A de la norma técnica NTC - ISO / IEC 27001 en su versión 2022.

Categoría	Orden	Control	Controles ISO 27001: 2022	Controles ISO 27001: 2013	Aplica	Justificación	Evidencia o registro	Responsable / Dependencia	Estado del control
ORGANIZACIONALES	1	5.1	Políticas de seguridad de la información	A.5.1.1 Políticas para la seguridad de la Información A.5.1.2 Revisión de las Políticas para la seguridad de la Información	**SI**	Se adopta este control, puesto que se debe definir un conjunto de políticas para la Seguridad de la Información, aprobadas por la Dirección, publicadas y comunicadas a los funcionarios y partes externas pertinentes.	a.MG-TI-18 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN b. Resolución 744 de 2024 - Artículo 17. Adopción de la Directriz del SGSI. c. Campañas de divulgación d. Actas de reunión del Comité MIPG-SIG, en donde se evidencia la revisión de las políticas de los Subsistemas y su debida alineación.	OAP / STRT	Implementado
	2	5.2	Roles y responsabilidades de SI	A.6.1.1 Roles y responsabilidades para la Seguridad de la Información	**SI**	Se adopta este control para estructurar la organización del SGSPI y así facilitarles a las personas la identificación de sus responsabilidades frente al subsistema	RESOLUCIÓN NÚMERO 6135 DE 2023 “Por la cual se definen los roles y las responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI”	SGGC / DTAF / STRT	Implementado
	3	5.3	Segregación de funciones	A.6.1.2 Separación de Deberes	**SI**	La entidad requiere este control para evitar conflicto de interés durante el procesamiento de la información.	a. RESOLUCIÓN NÚMERO 6135 DE 2023 b. Matriz RACI	STRT	Implementado
	4	5.4	Responsabilidades de la dirección	A.7.2.1 Responsabilidades de la Dirección	**SI**	Es necesaria la implementación de este control para que la Alta Dirección pueda exigirle a funcionarios y contratistas la aplicación de las políticas y procedimientos de seguridad de la información adoptados por la entidad.	a. MG-TI-18 Políticas de seguridad de la información b. RESOLUCIÓN NÚMERO 6135 DE 2023	OAP / STRH	Implementado
	5	5.5	Contacto con autoridades	A.6.1.3 Contacto con las autoridades	**SI**	Se adopta para mantener una comunicación asertiva con las autoridades ante cualquier amenaza o circunstancia sospechosa en el ciberespacio y tomar las medidas suficientes y necesarias para salvaguardar los activos de información de la entidad.	a. GU-TI-01 INTERCAMBIO DE información CON LAS AUTORIDADES Y GRUPOS DE interés DEL IDU V 1.0.pdf b. FOTI35 RELACION GRUPOS interés Y FUENTES información V1 c. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN - Cap. 7.2 CONTACTO CON LAS AUTORIDADES (Incidentes) d. PL-AC-01 - PLAN DE PREVENCIÓN, PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS – PPPRE e. PL-PE-05_PLAN_DE_MANEJO_DE_INCIDENTES_DE_CONTINUIDAD	STRH	Implementado
	6	5.6	Contacto con grupos de interés especial	A.6.1.4 Contacto con los grupos de interés especial	**SI**	Se incorpora este control para articularnos con las partes interesadas de tal forma que las comunicaciones y acciones ante cualquier circunstancia en la gestión del subsistema sean efectivas.	a. GU-TI-01 INTERCAMBIO DE información CON LAS AUTORIDADES Y GRUPOS DE interés DEL IDU V 1.0.pdf b. FOTI35 RELACION GRUPOS interés Y FUENTES información V1 c. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN - Cap. 7.2 CONTACTO CON LAS AUTORIDADES (Incidentes) d. PL-AC-01 - PLAN DE PREVENCIÓN, PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS – PPPRE e. Boletines de CSIRT Gobierno - Correo Electrónico f. WhatsApp Grupo "Segurinfo Distrito" g. WhatsApp Grupo "Segur_info_IDU"	STRT	Implementado
	7	5.7	Inteligencia de Amenazas	N/A	**SI**	Se adopta este control para mantener el conocimiento ante cualquier amenaza o circunstancia sospechosa en el	a. Informes de las herramientas de ciberseguridad. b. MG-TI-18 Políticas de seguridad de la información. Cap. 6.3.20 Política contra códigos maliciosos.	STRT	Implementado

Categoría	Orden	Control	Controles ISO 27001: 2022	Controles ISO 27001: 2013	Aplica	Justificación	Evidencia o registro	Responsable / Dependencia	Estado del control
						ciberespacio y tomar las medidas suficientes y necesarias para salvaguardar los activos de información de la entidad.	c. Boletines de seguridad emitidos por entes como COLCERT, SANS Institute, INCIBE, y DragonJAR. d. Boletines de seguridad remitidos a la Gente IDU. e. e. Informes de incidentes ocurridos f. Informes de análisis de seguridad realizados a las aplicaciones institucionales por el equipo de seguridad del IDU. g. Informes de las pruebas de intrusión realizadas por el proveedor del servicio. h. Informes entregados por el proveedor de SOC: "El contratista debe disponer de un servicio 7x24 para la identificación de amenazas que puedan poner en riesgo a la infraestructura del IDU en la Deep & Dark web y en fuentes abiertas".		
	8	5.8	Seguridad de la información en la gestión de proyectos	A.6.1.5 Seguridad de la Información en la Gestión de Proyectos. A.14.1.1 Análisis y especificación de requisitos de Seguridad de la Información	**SI**	Se implementa este control incorporando los lineamientos del subsistema de seguridad a la metodología de gestión de proyectos de la entidad.	1. PRTI04 DESARROLLO DE SOLUCIONES 2. PRTI15 gestión DE SISTEMAS DE información 3. FOTI06 SOLICITUD REQUERIMIENTOS APLICACIONES 4. FO-AC 56 PLANTILLA PLAN DE gestión DE CALIDAD	OAP / SGGC / STRT	Implementado
	9	5.9	Inventario de información y otros activos asociados	A.8.1.1 Inventario de activos A.8.1.2 Propiedad de los activos	**SI**	Se adopta este control en el IDU, puesto que se deben identificar la información y los activos asociados e instalaciones de procesamiento de información, elaborando y manteniendo un inventario de estos activos, así como, asignar un propietario a cada activo.	a. PR-TI-13 gestión DE ACTIVOS DE INFORMACIÓN b. IN-TI-13 Identificación de activos de información y uso del módulo de apoyo a la gestión de activos de información. c. Sistema CHIE - SGSI - https://openerp.idu.gov.co d. FO-TI-03 MATRIZ DE ACTIVOS DE información, Inventario publicado en la Intranet en cada proceso. e. Circular Interna 85 de 2020. PROPIEDAD DE LOS ACTIVOS DE INFORMACIÓN DENOMINADOS "SISTEMAS DE INFORMACIÓN".	STRT	Implementado
	10	5.10	Uso aceptable de la información y otros activos asociados	A.8.1.3 Uso aceptable de los activos. A.8.2.3 Manejo de Activos	**SI**	Se adopta este control, puesto que se deben desarrollar el procedimiento y las políticas para el manejo adecuado de la información y los activos asociados e instalaciones de procesamiento de información, de acuerdo con la circular vigente de clasificación y etiquetado.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.13 Política de uso aceptable de los activos de información. b. INTI06 USO ADECUADO DE LOS RECURSOS DE TI. c. PR-TI-13 gestión DE ACTIVOS DE INFORMACIÓN d. IN-TI-13 Identificación de activos de información y uso del módulo de apoyo a la gestión de activos de información. e. Sistema CHIE - SGSI - https://openerp.idu.gov.co	STRT	Implementado
	11	5.11	Devolución de activos	A.8.1.4 Devolución de Activos	**SI**	Se adopta este control, puesto que TODOS los funcionarios, contratistas de prestación de servicios y terceros con acceso a los activos de información DEBEN devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	a. INTI06 USO ADECUADO DE LOS RECURSOS DE TI Cap. 5.2.3 La Devolución. b. Sistema de información Chie: FaceIDU c. Paz y salvo - Módulo CHIE: Paz y Salvo - https://openerp.idu.gov.co d. PR-RF-103 ADMINISTRACIÓN DE INVENTARIO DE BIENES MUEBLES	STRT / STRF	Implementado
	12	5.12	Clasificación de la información	A.8.2.1 Clasificación de la Información	**SI**	Se implementa este control para darle un tratamiento adecuado a la información dependiendo de su clasificación, la cual está definida de acuerdo a la confidencialidad.	a. MG-TI-18 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.3.19 Política de clasificación, etiquetado y manejo de la información. b. PR-TI-13 gestión DE ACTIVOS DE INFORMACIÓN c. IN-TI-13 Identificación de activos de información y uso del módulo de apoyo a la gestión de activos de información. d. Sistema CHIE - SGSI - https://openerp.idu.gov.co e. CIRCULAR N. 216 DE 2023. CRITERIOS PARA LA CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN DEL IDU	STRF - Gestión Documental / STRT	Implementado

Categoría	Orden	Control	Controles ISO 27001: 2022	Controles ISO 27001: 2013	Aplica	Justificación	Evidencia o registro	Responsable / Dependencia	Estado del control
	13	5.13	Etiquetado de la información	A.8.2.2 Etiquetado y manejo de información	**SI**	Se implementa este control para darle un etiquetado adecuado a la información dependiendo de su clasificación, la cual está definida de acuerdo a la confidencialidad.	a. MG-TI-18 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.3.19 Política de clasificación, etiquetado y manejo de la información. b. PR-TI-13 gestión DE ACTIVOS DE INFORMACIÓN c. IN-TI-13 Identificación de activos de información y uso del módulo de apoyo a la gestión de activos de información. d. Sistema CHIE - SGSI - https://openerp.idu.gov.co e. CIRCULAR N. 216 DE 2023. CRITERIOS PARA LA CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN DEL IDU	STRF - Gestión Documental / STRT	Implementado
	14	5.14	Transferencia de la información	A.13.2.1 Políticas y procedimientos de transferencia de información A.13.2.2 Acuerdos sobre transferencia de Información A.13.2.3 Mensajería Electrónica	**SI**	Se adopta este control para garantizar la confidencialidad e integridad de la información cuando la misma está en tránsito.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.7 Política de transferencia de información b. PRTI23 gestión DE TELECOMUNICACIONES c. INTI08 PROTECCION DE LA información DIGITAL d. INTI19 aplicación DE CIFRADO e. INTI11 USO DE MENSAJERIA INSTANTANEA Y COMUNICACION ELECTRONICA f. INTI20 INTERCAMBIO DE información g. INTI22 USO ADECUADO DE LAS CARPETAS COMPARTIDAS h. INTI12 USO DEL SERVICIO DE CORREO ELECTRONICO INSTITUCIONAL i. FO-PE-20 COMPROMISO DE INTEGRIDAD, TRANSPARENCIA, CONFIDENCIALIDAD Y CONFLICTO DE INTERESES.	STRT	Implementado
	15	5.15	Control de acceso	A.9.1.1 Política de Control de Acceso A.9.1.2 Acceso a redes y a servicios de red	**SI**	Se incorpora este control para garantizar que solamente tengan acceso a los servicios de TI, los usuarios que hayan sido autorizados específicamente.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.4 Política de control de acceso a los servicios tecnológicos. b. IN-TI-16 REVISION DERECHOS ACCESO RECURSOS c. IN-TI-04 INGRESO AL_CENTRO DE COMPUTO Y A LOS CENTROS DE CABLEADO d. MGRF03 MANUAL SEGURIDAD Y VIGILANCIA	STRT / STRF	Implementado
	16	5.16	Gestión de la identidad	A.9.2.1 Registro y cancelación del registro de usuarios	**SI**	Se adopta este control para establecer el registro, modificación y cancelación de derechos de acceso para los usuarios.	a. PRTI02 GESTIONAR USUARIOS TECNOLOGICOS b. Se cuenta con un sistema de apoyo para facilitar el registro y cancelación del registro de usuarios. Ver Sistema de Información CHIE módulo Gestión TIC (https://openerp.idu.gov.co/documentacion/chie/gestión usuario tic/manual facilitador.html) c. Registro y cancelación de cuentas mediante Directorio Activo	STRT	Implementado
	17	5.17	Información de autenticación	A.9.2.4 Gestión de información de autenticación secreta de usuarios A.9.3.1 Uso de información de autenticación secreta A.9.4.3 Sistema de Gestión de Contraseñas	**SI**	Se adopta este control para garantizar el manejo adecuado de la información de autenticación.	a. PRTI02 GESTIONAR USUARIOS TECNOLOGICOS b. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.3 Política de control de acceso a los servicios tecnológicos c. Se cuenta con un sistema de apoyo para facilitar el registro y cancelación del registro de usuarios. Ver Sistema de Información CHIE módulo Gestión TIC (https://openerp.idu.gov.co/documentacion/chie/gestión usuario tic/manual facilitador.html). d. Registro y cancelación de cuentas mediante Directorio Activo e. Restricciones de ingreso seguro mediante Directorio Activo y políticas GPO para terminación de sesiones. f. IN-TI-07 ADMINISTRACION DEL DIRECTORIO ACTIVO g. GU-TI-02 PARA EL MANEJO DE CREDENCIALES TIC EN CONTINGENCIA h. Módulo para el cambio remoto y seguro de contraseñas del Directorio Activo	STRT	Implementado
	18	5.18	Derechos de acceso	A.9.2.2 Suministro de Acceso a Usuarios A.9.2.5 Revisión de los	**SI**	Se adopta este control, puesto que se debe implementar un proceso de suministro de acceso a los usuarios y	a. PRTI02 GESTIONAR USUARIOS TECNOLOGICOS b. Se cuenta con un sistema de apoyo para facilitar el registro y cancelación del registro de usuarios. Ver Sistema de Información CHIE módulo Gestión TIC	STRT	Implementado

Categoría	Orden	Control	Controles ISO 27001: 2022	Controles ISO 27001: 2013	Aplica	Justificación	Evidencia o registro	Responsable / Dependencia	Estado del control
				derechos de Acceso de Usuarios A.9.2.6 Retiro o ajuste de derechos de acceso		asignar o revocar los derechos sobre todos los sistemas y servicios de TI.	(https://openerp.idu.gov.co/documentacion/chie/gestión usuario tic/manual facilitador.html) c. Registro y cancelación de cuentas mediante Directorio Activo d. IN-TI-16 REVISION DE LOS DERECHOS DE ACCESO A LOS RECURSOS (Se ejecuta por cambios significativos en las plataformas)" e. Paz y salvo - Módulo CHIE: Paz y Salvo - https://openerp.idu.gov.co		
	19	5.19	Seguridad de la información en la relación con proveedores	A.15.1.1 Política de Seguridad de la Información para las relaciones con proveedores	**SI**	Se implementa este control, para mantener un nivel de seguridad de la información adecuado y mitigar los riesgos asociados con el acceso de proveedores a los activos de la entidad.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.9 Política de seguridad de la información para la relación con proveedores b. PRTI21 gestión DE COMPRAS DE PRODUCTOS Y/O SERVICIOS DE TECNOLOGIA DE información c. FO-PE-20 COMPROMISO DE INTEGRIDAD, TRANSPARENCIA, CONFIDENCIALIDAD Y CONFLICTO DE INTERESES.	STRT	Implementado
	20	5.20	Abordar la seguridad de la información en los acuerdos con los proveedores	A.15.1.2 Tratamiento de la Seguridad dentro de los acuerdos con proveedores	**SI**	Se implementa este control, para mantener un nivel de seguridad de la información adecuado y mitigar los riesgos asociados con el acceso de proveedores a los activos de la entidad.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.9 Política de seguridad de la información para la relación con proveedores b. PRTI21 gestión DE COMPRAS DE PRODUCTOS Y O SERVICIOS DE TECNOLOGIA DE información c. FO-PE-20 COMPROMISO DE INTEGRIDAD, TRANSPARENCIA, CONFIDENCIALIDAD Y CONFLICTO DE INTERESES.	STRT	Implementado
	21	5.21	Gestión de la seguridad de la información en la cadena de suministro	A.15.1.3 Cadena de Suministro de Tecnología de Información y Comunicación	**SI**	Se implementa este control, para mantener un nivel de seguridad de la información adecuado y mitigar los riesgos asociados con el acceso de proveedores a los activos de la entidad.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.9 Política de seguridad de la información para la relación con proveedores b. PRTI21 gestión DE COMPRAS DE PRODUCTOS Y O SERVICIOS DE TECNOLOGIA DE información c. FO-PE-20 COMPROMISO DE INTEGRIDAD, TRANSPARENCIA, CONFIDENCIALIDAD Y CONFLICTO DE INTERESES.	STRT	Implementado
	22	5.22	Seguimiento, revisión y gestión de cambios de servicios de proveedores	A.15.2.1 Seguimiento y revisión de los servicios de los proveedores A.15.2.2 Gestión de Cambios en los Servicios de los Proveedores	**SI**	Se incorpora este control para gestionar la continuidad de los servicios prestados por los proveedores de la entidad.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.9 Política de seguridad de la información para la relación con proveedores b. PRTI21 gestión DE COMPRAS DE PRODUCTOS Y O SERVICIOS DE TECNOLOGIA DE información c. PRTI08 gestión DE CAMBIOS d. Contratos. e. Procedimientos PRGC01 Mínima cuantía contratación hasta el 10% de la menor cuantía PRGC03 Selección abreviada menor cuantía PRGC04 Concurso de méritos abierto o con precalificación PRGC05 Suscripción de contratos derivados de procesos de selección producto convocatoria pública	STRT	Implementado
	23	5.23	Seguridad de la información para el uso de servicios en la nube	N/A	**SI**	Se adopta este control para definir los requerimientos adecuados para los servicios en la nube, de acuerdo a las necesidades de la entidad.	a. MG-TI-18 Políticas de seguridad de la información. b. PR-TI-23 gestión de telecomunicaciones. c. PL-TI-01 PLAN DE RECUPERACIÓN ANTE DESASTRES. d, Contrato de servicios de nube con Oracle. (ANS)	STRT	Implementado
	24	5.24	Planificación y preparación de la gestión de incidentes de SI.	A.16.1.1 Gestión de Incidentes / Responsabilidades y Procedimientos	**SI**	Se implementa este control para facilitar una respuesta adecuada y oportuna ante un incidente de seguridad de la información.	a. RESOLUCIÓN NÚMERO 6135 DE 2023 "Por la cual se definen los roles y las responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI" b. PRTI22 gestión DE INCIDENTES DE SEGURIDAD DE LA información c. GU-TI-03 GUÍA ANALISIS FORENSE PARA INCIDENTES SEGURIDAD DE LA información d. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	STRT	Implementado

Categoría	Orden	Control	Controles ISO 27001: 2022	Controles ISO 27001: 2013	Aplica	Justificación	Evidencia o registro	Responsable / Dependencia	Estado del control
	25	5.25	Evaluación y decisión sobre los eventos de SI.	A.16.1.4 Evaluación de Eventos de Seguridad de la Información y decisiones sobre ellos	**SI**	Se adopta este control para definir la forma de evaluar y clasificar de los eventos de seguridad de la información.	a. PRTI22 gestión DE INCIDENTES DE SEGURIDAD DE LA información b. GU-TI-03 GUÍA ANALISIS FORENSE PARA INCIDENTES SEGURIDAD DE LA información c. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN d. Módulo Aranda USDK para el reporte de requerimientos e incidentes. e. FOTI42 INFORME DE INCIDENTES DE SEGURIDAD DE LA información	STRT	Implementado
	26	5.26	Respuesta a incidentes de SI.	A.16.1.5 Respuesta a incidentes de seguridad de la información	**SI**	Se implementa este control para facilitar una respuesta adecuada y oportuna ante un incidente de seguridad de la información.	a. PRTI22 gestión DE INCIDENTES DE SEGURIDAD DE LA información b. GU-TI-03 GUÍA ANALISIS FORENSE PARA INCIDENTES SEGURIDAD DE LA información c. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN d. FOTI42 INFORME DE INCIDENTES DE SEGURIDAD DE LA información	STRT	Implementado
	27	5.27	Aprendiendo de los incidentes de SI	A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información	**SI**	Se incorpora este control para reducir el impacto de incidentes de seguridad de la información a través de la identificación de lecciones aprendidas.	a. PRTI22 gestión DE INCIDENTES DE SEGURIDAD DE LA información b. GU-TI-03 GUÍA ANALISIS FORENSE PARA INCIDENTES SEGURIDAD DE LA información c. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN d. Módulo Aranda USDK para el reporte de requerimientos e incidentes. e. FOTI42 INFORME DE INCIDENTES DE SEGURIDAD DE LA información	STRT	Implementado
	28	5.28	Recopilación de pruebas	A.16.1.7 Recolección de Evidencia	**SI**	Se adopta este control para aplicar los procedimientos que permitan la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia en un proceso disciplinario o judicial.	a. PRTI22 gestión DE INCIDENTES DE SEGURIDAD DE LA información b. GU-TI-03 GUÍA ANALISIS FORENSE PARA INCIDENTES SEGURIDAD DE LA información c. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN d. Módulo Aranda USDK para el reporte de requerimientos e incidentes. e. FOTI42 INFORME DE INCIDENTES DE SEGURIDAD DE LA información f. FOTI43 EVIDENCIA DIGITAL	STRT	Implementado
	29	5.29	Sistemas de información durante la interrupción	A.17.1.1 Planificación de la continuidad de la Seguridad de la Información. A.17.1.2 Implementación de la continuidad de la seguridad de la información. A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**SI**	Se incorpora este control para establecer, documentar, implementar y mantener procesos y procedimientos para mantener la seguridad de la información requerida por la entidad durante una situación adversa.	a. PRTI20 gestión DE CONTINUIDAD DE SERVICIOS b. PLTI01 PLAN RECUPERACION ANTE DESASTRES c. FOTI38 PLAN DE PRUEBAS PARA DRP d. FOTI39 GUIÓN PARA PRUEBAS DE DRP e. FOTI40 MINUTOGRAMA PARA PRUEBAS DRP f. INTI03 RESTAURACION DE LA aplicación VALORICEMOS g. INTI23 RESTAURACION BOTON AZUL h. INTI24 RESTAURACION SISTEMAS BASADOS EN ODOO i. INTI26 RESTAURACION SISTEMA KACTUS j. INTI27 RESTAURACION SISTEMA STONE k. FOTI26 ARBOL DE LLAMADAS PARA CONTINUIDAD DEL NEGOCIO l. PLPE05 PLAN DE MANEJO DE INCIDENTES DE CONTINUIDAD m. INFORMES DE LAS PRUEBAS REALIZADAS	STRT	Implementado

Categoría	Orden	Control	Controles ISO 27001: 2022	Controles ISO 27001: 2013	Aplica	Justificación	Evidencia o registro	Responsable / Dependencia	Estado del control
	30	5.30	Preparación de las TIC para continuidad del negocio.	N/A	**SI**	Se incorpora este control para establecer la estrategia necesaria para gestionar la seguridad de la información requerida por la entidad durante una situación adversa.	a. Subsistema de Gestión de Continuidad de Negocio. b. PL-TI-01 Plan de Recuperación ante Desastres. C. DU-TI-07 Gestión de redes IDU	STRT	Implementado
	31	5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	A.18.1.1 Identificación de la legislación aplicable y los requisitos contractuales A.18.1.5 Reglamentación de Controles Criptográficos	**SI**	Se adopta este control puesto que la entidad debe cumplir con los requisitos legales de orden local y nacional, así como con las circulares y resoluciones internas.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.4 Política de controles criptográficos b. El normograma está publicado en la web institucional, por procesos, en la siguiente URL: https://www.idu.gov.co/page/transparencia/normatividad/normograma c. IN-TI-08 PROTECCION DE LA información DIGITAL, Cap. 8.5 Controles criptográficos para el sistema administrativo y financiero STONE d. IN-TI-19 aplicación DE CIFRADO e. En la Intranet - mapa de procesos.	DTGC / STRT	Implementado
	32	5.32	Derechos de la propiedad intelectual	A.18.1.2 Derechos de propiedad intelectual (DPI)	**SI**	Se adopta este control, puesto que se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos propietarios.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.12 Política de instalación y uso de software b. MG-TI-19 DESARROLLO SEGURO DE SOFTWARE c. PRTI14 gestión DE LICENCIAMIENTO DE SW d. FOTI25 INVENTARIO APLICACIONES e. Informe Anual sobre Derechos de Autor en materia de software.	STRT	Implementado
	33	5.33	Protección de registros	A.18.1.3 Protección de registros	**SI**	Se adopta este control, puesto que se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con la protección de los registros o logs.	MGDO01 gestión DOCUMENTAL	STRF / STRT / OAP	Implementado
	34	5.34	Privacidad y protección de IIP	A.18.1.4 Privacidad y Protección de información de datos personales	**SI**	Se adopta este control, puesto que se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con la protección de la información de identificación personal.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.14 Política de Privacidad y protección de datos personales b. MGTI17 PROTECCION DE DATOS PERSONALES	OAC / OTC / STRT	Implementado
	35	5.35	Revisión independiente	A.18.2.1 Revisión Independiente de la Seguridad de Información	**SI**	Se incorpora este control para permitir la validación independiente del SGSPI por parte de un tercero idóneo.	a. PRTI18 REVISION A LA PLATAFORMA DE TECNOLOGIA DE información b. Programa de Auditoría c. PREC01 EVALUACION INDEPENDIENTE Y AUDITORIAS INTERNAS d. Auditorías externas	OAP / OCI / STRT	Implementado
	36	5.36	Cumplimiento de políticas, normas y estándares de seguridad	A.18.2.2 Cumplimiento con las políticas y normas de seguridad A.18.2.3 Revisión del cumplimiento técnico	**SI**	Se adopta este control puesto que la entidad debe cumplir con los requisitos legales de orden local y nacional, así como con los convenios internacionales que el Estado Colombiano haya suscrito y las circulares y resoluciones internas relacionados con los estándares de seguridad de la información.	a. Resolución 2330 de 2023. b. PRTI18 REVISION A LA PLATAFORMA DE TECNOLOGIA DE información c. PRTI24 gestión OPTIMIZACION DEL PROCESO d. PRMC03 REVISION POR LA Dirección e. Informe de Análisis de vulnerabilidades y hacking ético f. PREC01 EVALUACION INDEPENDIENTE Y AUDITORIAS INTERNAS	STRT	Implementado
	37	5.37	Procedimientos operativos documentados	A.12.1.1 Procedimientos de Operación Documentados	**SI**	Se adopta este control, puesto que los procedimientos que orientan la operación se deben documentar y poner	Intranet IDU - Documentación SIG	OAP / STRT	Implementado

Categoría	Orden	Control	Controles ISO 27001: 2022	Controles ISO 27001: 2013	Aplica	Justificación	Evidencia o registro	Responsable / Dependencia	Estado del control
						a disposición de todos los usuarios que los necesitan.			
PERSONAS	38	6.1	Selección	A.7.1.1 Seguridad de los Recursos humanos / Selección	**SI**	Se adopta este control puesto que la entidad desarrolla los procedimientos de selección y contratación a partir de las leyes vigentes, lineamientos de la CNSC y definiciones establecidas por el IDU.	a. RESOLUCIÓN NÚMERO 6135 DE 2023 b. Para el personal de planta la verificación de antecedentes se realiza de acuerdo a lo establecido por la Comisión Nacional del Servicio Civil (CNSC). Además, la STRH realiza una verificación de los antecedentes y de ser necesario se devuelve la lista de elegibles. c. Para los contratistas se realiza de acuerdo con el procedimiento PR-GC-12 CONTRATACION PSPAG PERSONAS NATURALES y según lo indicado en la ley.	DTGC / STRH	Implementado
	39	6.2	Términos y condiciones del empleo	A.7.1.2 Términos y condiciones del empleo	**SI**	Se adopta este control puesto que la entidad desarrolla los procedimientos de selección y contratación a partir de las leyes vigentes, lineamientos de la CNSC y definiciones establecidas por el IDU.	a. RESOLUCIÓN NÚMERO 6135 DE 2023 b. FO-PE-20 COMPROMISO DE INTEGRIDAD, TRANSPARENCIA, CONFIDENCIALIDAD Y CONFLICTO DE INTERESES.	DTGC / STRH	Implementado
	40	6.3	Concienciación, educación y capacitación en seguridad de la información	A.7.2.2 Toma de Conciencia, Educación y Formación en la Seguridad de la Información	**SI**	La entidad implementa este control en el proceso de incorporación de funcionarios a la entidad y con la coordinación de talento humano y el equipo de seguridad de la información.	PL-CO-02 Plan de comunicaciones Ruta de Posesión, Inducciones, reinducciones, Campañas con OAC, Correos, Hablemos de Seguridad Sin Tapujos, etc.	OAC / STRT	Implementado
	41	6.4	Proceso disciplinario	A.7.2.3 Proceso Disciplinario	**SI**	La entidad adopta este control porque los procesos disciplinarios en el IDU son un componente esencial para garantizar la integridad y la ética en el servicio público cumpliendo con las normas y regulaciones establecidas	a. 2310430-PR-126 PRIMERA INSTANCIA ETAPA INSTRUCCIÓN b. 2310430-PR-123 PROCEDIMIENTO SEGUNDA INSTANCIA c. 2310430-PR-124 PRIMERA INSTANCIA-ETAPA DE JUZGAMIENTO JUICIO VERBAL d. 2310430-PR-125 PROCEDIMIENTO PRIMERA INSTANCIA ETAPA JUZGAMIENTO ORDINARIO e. PREC02 EJECUCION DE LA SANCION DISCIPLINARIA f. PRTI22 gestión DE INCIDENTES DE SEGURIDAD DE LA información	OCID / STRT	Implementado
	42	6.5	Responsabilidades después de terminar el empleo	A.7.3.1 Terminación o cambio de responsabilidades de empleo	**SI**	Se adopta este control puesto que la entidad desarrolla los procedimientos de selección y contratación a partir de las leyes vigentes, lineamientos de la CNSC y definiciones establecidas por el IDU que permitan establecer responsabilidades después de terminar el vínculo con la entidad.	a. Suscripción de cláusulas de confidencialidad y no divulgación de la información del Instituto, por un periodo de mínimo de 2 años de la desvinculación o terminación del contrato. b. Circular 7 de 2019 - LINEAMIENTOS PARA LA FINALIZACIÓN DEL VÍNCULO LABORAL O CONTRACTUAL CON EL IDU c. Módulo CHIE: Gestión TIC - https://openerp.idu.gov.co	STRH / DTGC	Implementado
	43	6.6	Acuerdos de confidencialidad y no divulgación	A.13.2.4 Acuerdos de Confidencialidad o de NO divulgación	**SI**	En la incorporación de este control la entidad ha desarrollado instrumentos que permiten registrar los compromisos, acuerdos de confidencialidad, no divulgación y conflicto de intereses en cumplimiento de las definiciones de ley y las directrices de la entidad de acuerdo al sistema integrado de gestión.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.7 Política de transferencia de información b. FO-PE-20 COMPROMISO DE INTEGRIDAD, TRANSPARENCIA, CONFIDENCIALIDAD Y CONFLICTO DE INTERESES.	STRT	Implementado
	44	6.7	Trabajo a distancia	A.6.2.2 Teletrabajo	**SI**	La entidad adopta este control a través de las definiciones del libro blanco de teletrabajo del IDU el cual contempla todas las definiciones de ley para realizar teletrabajo formal y actividades de trabajo remoto o a distancia.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.2 Política para teletrabajo o trabajo remoto. b. GU-TH- 01 LIBRO BLANCO DE TELETRABAJO IDU	STRT - STRH	Implementado
	45	6.8	Reporte de eventos de seguridad de la información	A.16.1.2 Reporte de Eventos de Seguridad de la Información.	**SI**	Se adopta este control, para que la entidad pueda asegurar sus plataformas de registro de eventos y coordinar la reacción con sus equipos de trabajo	a. PRTI22 gestión DE INCIDENTES DE SEGURIDAD DE LA información b. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	STRT	Implementado

Categoría	Orden	Control	Controles ISO 27001: 2022	Controles ISO 27001: 2013	Aplica	Justificación	Evidencia o registro	Responsable / Dependencia	Estado del control
				A.16.1.3 Reporte de debilidades de seguridad de la información.		tecnológico ante eventos de seguridad de la información que se constituyan un riesgo a la información del IDU.	c. FOTI28 CONDICIONES PARA VALIDACION DE EVENTOS DE SEGURIDAD DE LA información d. Módulo Aranda USDK para el reporte de requerimientos e incidentes.		
FÍSICOS	46	7.1	Perímetro de seguridad física	A.11.1.1 Perímetro de seguridad física	**SI**	La entidad incorpora este control con la definición de su anillo físico perimetral, áreas seguras y la gestión de los puntos de acceso con personal e infraestructura dedicada a la vigilancia, validación y registro.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.10 Política de seguridad física y del entorno b. MG-RF-03 MANUAL SEGURIDAD Y VIGILANCIA, cap. 7 Sistema de control de acceso c. Existe un control de acceso a las áreas seguras. d. FORF06 Planilla de control de personas que ingresan a áreas restringidas IDU	STRF / STRT	Implementado
	47	7.2	Entrada física	A.11.1.2 Controles de acceso físico A.11.1.6 Áreas de despacho y carga	**SI**	La entidad incorpora este control con la definición de su anillo físico perimetral, áreas seguras y la gestión de los puntos de acceso con personal e infraestructura dedicada a la vigilancia, validación y registro.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.10 Política de seguridad física y del entorno b. MG-RF-03 MANUAL SEGURIDAD Y VIGILANCIA, cap. 7 Sistema de control de acceso c. FORF06 Planilla de control de personas que ingresan a áreas restringidas IDU d. Acceso mediante biométrico y tarjetas de proximidad	STRF / STRT	Implementado
	48	7.3	Aseguramiento de oficinas, salas e instalaciones	A.11.1.3 Seguridad de oficinas, recintos e instalaciones	**SI**	La entidad incorpora este control con la definición de su anillo físico perimetral, áreas seguras y la gestión de los puntos de acceso con personal e infraestructura dedicada a la vigilancia, validación y registro.	a. MG-TI-18 Políticas de seguridad de la información . Cap.6.3.10 Política de seguridad física y del entorno b. MG-RF-03 MANUAL SEGURIDAD Y VIGILANCIA, cap. 7 Sistema de control de acceso c. Acceso mediante control biométrico y tarjetas de proximidad a las áreas seguras d. FORF06 Planilla de control de personas que ingresan a áreas restringidas IDU	STRF / STRT	Implementado
	49	7.4	Supervisión de seguridad física	N/A	**SI**	La entidad incorpora este control con la definición de su anillo físico perimetral, áreas seguras y la gestión de los puntos de acceso con personal e infraestructura dedicada a la vigilancia, validación y registro.	a. MG-TI-18 Políticas de seguridad de la información . Cap.6.3.10 Política de seguridad física y del entorno b. MG-RF-03 MANUAL SEGURIDAD Y VIGILANCIA, cap. 7 Sistema de control de acceso c. Acceso mediante control biométrico y tarjetas de proximidad a las áreas seguras d. FORF06 Planilla de control de personas que ingresan a áreas restringidas IDU. e. Contrato de vigilancia. Presta el servicio de monitoreo de la sede mediante CCTV.	STRF / STRT	Implementado
	50	7.5	Protección contra amenazas físicas y ambientales	A.11.1.4 Protección contra amenazas externas y ambientales	**SI**	La entidad incorpora este control con la definición de su anillo físico perimetral, áreas seguras y la gestión de los puntos de acceso con personal e infraestructura dedicada a la vigilancia, validación y registro.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.10 Política de seguridad física y del entorno b. MG-RF-03 MANUAL SEGURIDAD Y VIGILANCIA, cap. 7 Sistema de control de acceso c. IN-TI-04 INGRESO AL CENTRO DE COMPUTO Y A LOS CENTROS DE CABLEADO. Cap. 5 condiciones para el ingreso. d. El centro de cómputo tiene un sistema de detección y extinción de incendios. e. La Entidad cuenta con extintores distribuidos de manera estratégica. g. La Entidad tiene un Plan Institucional de Respuesta a Emergencias, enlazado con el Sistema Distrital de Atención de Emergencias. h. La Entidad cuenta con una brigada para la atención de emergencias. i. PL-AC-01 - PLAN DE PREVENCIÓN, PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS – PPPRE	STRH / STRF / STRT	Implementado
	51	7.6	Trabajo en áreas seguras	A.11.1.5 Trabajo en áreas seguras	**SI**	La entidad incorpora este control con la definición de su anillo físico perimetral, áreas seguras y la gestión de los puntos	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.10 Política de seguridad física y del entorno b. MG-RF-03 MANUAL SEGURIDAD Y VIGILANCIA, cap. 7 Sistema	STRF / STRT	Implementado

Categoría	Orden	Control	Controles ISO 27001: 2022	Controles ISO 27001: 2013	Aplica	Justificación	Evidencia o registro	Responsable / Dependencia	Estado del control
						de acceso con personal e infraestructura dedicada a la vigilancia, validación y registro.	de control de acceso c. IN-TI-04 INGRESO AL CENTRO DE COMPUTO Y A LOS CENTROS DE CABLEADO. Cap. 5 condiciones para el ingreso		
	52	7.7	Escritorio despejado y pantalla despejada	A.11.2.9 Política de Escritorio Limpio y pantalla limpia	**SI**	Se adopta este control atendiendo los riesgos a los que se ve expuesta la información física y electrónica de la entidad en los puestos de trabajo y puntos de atención ciudadana.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.6 Política de escritorio y pantalla limpia b. Política para la gestión de pantalla limpia implementada en Directorio Activo.	STRT	Implementado
	53	7.8	Ubicación y protección del equipo	A.11.2.1 Ubicación y protección de los equipos	**SI**	Se adopta este control atendiendo los riesgos a los que se ve expuesta la información física y electrónica de la entidad en los equipos, puestos de trabajo y puntos de atención ciudadana.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.11 Política de uso aceptable de los activos b. INTI04 INGRESO AL CENTRO DE COMPUTO Y A LOS CENTROS DE CABLEADO c. INTI06 USO ADECUADO DE LOS RECURSOS DE TI d. Contratos de mantenimiento plantas eléctricas y UPS	STRF / STRT	Implementado
	54	7.9	Seguridad de los activos fuera de las instalaciones	A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	**SI**	Se adopta este control, para proteger los activos de información fuera de las instalaciones de la entidad en cumplimiento de las actividades y procesos propios del IDU .	a. MG-TI-18 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Cap. 6.3.2 Política para teletrabajo o trabajo remoto b. MGRF02 ADMINISTRACION DE BIENES MUEBLES E INMUEBLES DEL IDU c. MGRF03 MANUAL SEGURIDAD Y VIGILANCIA Cap. Seguridad en movimientos de bienes muebles del IDU.	STRF / STRT	Implementado
	55	7.10	Medios de almacenamiento	A.8.3.1 Gestión de Medios Removibles. A.8.3.2 Disposición de los Medios. A.8.3.3 Transferencia de Medios Físicos	**SI**	Se adopta este control, mediante la definición de procedimientos desde la STRT para la gestión de medios removibles y gestionar su disposición en forma segura de los medios cuando ya no se requieran, asegurando el acceso no autorizado, uso indebido o corrupción durante el transporte.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.7 Política de transferencia de información b. PR-RF- 103 ADMINISTRACION DE INVENTARIO DE BIENES MUEBLES c. IN-TI-15 BORRADO SEGURO FORMATEO FINAL EQUIPOS d. Control de dispositivos a través del antivirus Bitdefender	STRT / STRF	Implementado
	56	7.11	Servicios públicos de respaldo	A.11.2.2 Servicios de suministro	**SI**	Se adopta este control, en donde el IDU establece directrices para asegurar que los servicios públicos requeridos para la operación de TI, tales como energía y canales de comunicación, entre otros, estén siempre disponibles.	a. INTI04 INGRESO AL CENTRO DE COMPUTO Y A LOS CENTROS DE CABLEADO b. Se cuenta con servicios de respaldo, por ejemplo UPS, plantas eléctricas, aire acondicionado redundante.	STRF / STRT	Implementado
	57	7.12	Seguridad del cableado	A.11.2.3 Seguridad del cableado	**SI**	Se adopta este control con objetivo de proteger la infraestructura de información del IDU para prevenir accesos no autorizados y asegurar la integridad y confidencialidad (que aplique) de la información.	1. PRTI23 gestión DE TELECOMUNICACIONES cap. 1.1 Gestión de telecomunicaciones. 2. La entidad cuenta con cable UTP categoría 6.	STRT	Implementado
	58	7.13	Mantenimiento de equipos	A.11.2.4 Mantenimiento de los equipos	**SI**	Se adopta este control, en donde el IDU establece directrices para asegurar que los servicios de soporte, mantenimiento y gestión de instalaciones, se realicen de manera que no comprometan la seguridad de sus activos de información.	a. Contratos de mantenimiento preventivo y bolsa de repuestos (Datacenter -Servidores - Computadores.)	STRF / STRT	Implementado
	59	7.14	Eliminación segura o reutilización de equipos	A.11.2.7 Disposición Segura o Reutilización de equipos	**SI**	La implementación de este control en la entidad se centra en la disposición segura o reutilización de equipos. Este control es relevante para prevenir el acceso no autorizado a información sensible que pueda estar almacenada en equipos que se van a desechar o reutilizar en el IDU.	a. PR-RF- 103 ADMINISTRACION DE INVENTARIO DE BIENES MUEBLES b. MGRF02 ADMINISTRACION DE BIENES MUEBLES E INMUEBLES DEL IDU c. IN-TI-15 BORRADO SEGURO FORMATEO FINAL EQUIPOS d. Resolución y/o actas de bajas	STRT / STRF	Implementado

Categoría	Orden	Control	Controles ISO 27001: 2022	Controles ISO 27001: 2013	Aplica	Justificación	Evidencia o registro	Responsable / Dependencia	Estado del control
TECNOLÓGICOS	60	8.1	Dispositivos finales del usuario	A.6.2.1 Política para dispositivos móviles. A.11.2.8 Equipos de Usuario Desatendidos	**SI**	Se adopta este control en el IDU para realizar la planificación y control operacional dentro del Sistema de Gestión de Seguridad de la Información (SGSI) para proteger la información institucional que es procesada en equipo de usuario final.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.1 Política para dispositivos móviles b. IN-TI-20 INTERCAMBIO DE información MEDIOS EXTRAIBLES Cap. 5.5 intercambio de información mediante dispositivo móviles. c. Módulo MDM de GOOGLE para dispositivos móviles. d. INTI07 ADMINISTRACION DEL DIRECTORIO ACTIVO e. Políticas de directorio activo sobre cierre de sesiones y se han realizado campañas de sensibilización respecto a la importancia del cierre de la sesión y bloqueo de la estación de trabajo.	STRT	Implementado
	61	8.2	Derechos de acceso privilegiado	A.9.2.3 Gestión de Derechos de Acceso Privilegiado	**SI**	El IDU implementa este control para asegurar que los accesos privilegiados que se entregan sean controlados, asignados y revocados cuando corresponda.	a. PRTI02 GESTIONAR USUARIOS TECNOLOGICOS b. MG-TI-18 Políticas de seguridad de la información. Cap. 6.3.5.2 Gestión de derechos de acceso privilegiado. c. Se cuenta con un sistema de apoyo para facilitar el registro y cancelación del registro de usuarios. Ver Sistema de Información CHIE módulo Gestión TIC (https://openerp.idu.gov.co/documentacion/chie/gestión usuario tic/manual facilitador.html). d. Registro y cancelación de cuentas mediante Directorio Activo	STRT	Implementado
	62	8.3	Restricción de acceso a la información	A.9.4.1 Restricción de Acceso a la Información	**SI**	Se adopta este control para asegurar el acceso a la información, garantizando que solo las personas autorizadas puedan acceder a datos sensibles y críticos dentro del IDU.	a. MG-TI-18 Políticas de seguridad de la información. Cap. 6.3.3 Política de control de acceso a los servicios tecnológicos b. IN-TI-22 USO ADECUADO DE LAS CARPETAS COMPARTIDAS Cap. 5.4 ASIGNACIÓN Y REVOCACIÓN DE PERMISOS DE ACCESO. c. Módulo CHIE: Gestión TIC - https://openerp.idu.gov.co. Los directivos definen el nivel de acceso a cada aplicación de sus subalternos.	STRT	Implementado
	63	8.4	Acceso al código fuente	A.9.4.5 Control de Acceso a Códigos Fuente de Programas	**SI**	Se implementa este control para que la STRT administre el acceso al código fuente protegiendo la integridad, confidencialidad y disponibilidad de este, que es absolutamente relevante para el funcionamiento de aplicaciones y sistemas dentro de la entidad.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.3 Política de control de acceso a los servicios tecnológicos b. PRTI04 DESARROLLO DE SOLUCIONES c. INTI29 AMBIENTES-TRABAJO PARA DESARROLLO SOFTWARE d. Software para control de versiones (GIT) e. INTI08 PROTECCION DE LA información DIGITAL, Cap. 8.4 Método usado para la gestión de versionamiento. f. INTI30 UTILIZACIÓN DEL REPOSITORIO DE DOCUMENTOS Y CÓDIGO FUENTE	STRT	Implementado
	64	8.5	Autenticación segura	A.9.4.2 Procedimiento de Ingreso Seguro	**SI**	Se adopta este control en el IDU como un componente relevante en la protección de los activos de información y los sistemas de información de la entidad, estableciendo las directrices para garantizar que tanto los usuarios humanos, como los no humanos puedan acceder a los recursos de tecnología de la información de manera segura.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.3 Política de control de acceso a los servicios tecnológicos b. PRTI02 GESTIONAR USUARIOS TECNOLOGICOS c. Restricciones de ingreso seguro mediante Directorio Activo y políticas GPO para terminación de sesiones. d. IN-TI-07 ADMINISTRACION DEL DIRECTORIO ACTIVO	STRT	Implementado
	65	8.6	Gestión de la capacidad	A.12.1.3 Gestión de Capacidad	**SI**	Se adopta este control, puesto que en la gestión de la STRT se debe hacer seguimiento al uso de los recursos, hacer los ajustes y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido de los sistemas de información de la entidad.	a. PRTI16 gestión DE LA CAPACIDAD b. FOTI30 CONTROL DE CAPACIDAD DE LOS RECURSOS DE TI	STRT	Implementado
	66	8.7	Protección contra malware	A.12.2.1 Controles contra códigos maliciosos	**SI**	Se implementa en el IDU este control para contar con la detección, prevención y recuperación ante eventos de código	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.20 Política contra códigos maliciosos b. INTI21 USO ANTIVIRUS EN LOS EQUIPOS DE USUARIO FINAL	STRT	Implementado

Categoría	Orden	Control	Controles ISO 27001: 2022	Controles ISO 27001: 2013	Aplica	Justificación	Evidencia o registro	Responsable / Dependencia	Estado del control
						malicioso, combinados con la toma de conciencia adecuada, por parte de los funcionarios y contratistas de prestación de servicios.	c. Software de Antivirus Corporativo, Sandbox y WAF. d. Bloqueo de puertos USB, a través del sistema antivirus. e. Restricción de instalación de software no autorizada mediante política de directorio Activo.		
	67	8.8	Gestión de vulnerabilidades técnicas	A.12.6.1 Gestión de las Vulnerabilidades Técnicas. A.18.2.3 Revisión del cumplimiento técnico	**SI**	Se adopta este control para que la STRT en la gestión de la infraestructura tecnológica obtenga oportunamente información acerca de las vulnerabilidades técnicas de la plataforma en operación; evaluando la exposición de los activos de información a vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	a. PRTI24 gestión OPTIMIZACION DEL PROCESO b. PRTI18 REVISION A LA PLATAFORMA DE TECNOLOGIA DE información c.. PREC01 EVALUACION INDEPENDIENTE Y AUDITORIAS INTERNAS d. FOTI23 LISTA DE VULNERABILIDADES Y AMENAZAS e. Informe de Análisis de vulnerabilidades y hacking ético. f. Plan de remediación	STRT	Implementado
	68	8.9	Gestión de la configuración	N/A	**SI**	Se adopta este control, puesto que se deben prevenir cambios no autorizados y asegurar que las configuraciones gestionadas por la STRT sean documentadas, implementadas, monitoreadas y revisadas periódicamente.	a. PRTI08 gestión DE CAMBIOS b. FOTI29 CONTROL DE CAMBIOS DETECNOLOGIAS c. FOTI33 ACTIVIDADES DE CAMBIOS TECNOLOGICOS PRESENTADAS A LA MESA DE TRABAJO d. Base de datos de gestión de la configuración en el sistema Aranda - CMDB	STRT	Implementado
	69	8.10	Eliminación de la información	N/A	**SI**	Se adopta este control en el IDU, puesto que se debe asegurar que la información sea eliminada cuando ya no sea necesaria y prevenir la exposición innecesaria de activos de información etiquetados como clasificados o reservados y cumplir con las definiciones ley.	a. IN-TI-15 Borrado seguro de datos y formateo final de equipos	STRT	Implementado
	70	8.11	Enmascaramiento de datos	N/A	**SI**	Se adopta este control en el IDU en cumplimiento de la protección de datos sensibles, incluyendo los datos personales (IIP), la entidad en cumplimiento de su misión procesa o da tratamiento a información de carácter personal a través de sus sistemas de información.	a. MG-TI-18 Políticas de seguridad de la información Cap. 6.3.6 Política de controles criptográficos	STRT	En implementación
	71	8.12	Prevención de la fuga de datos	N/A	**SI**	Se adopta este control, puesto que se debe proteger la información gestionada por el IDU, contra la extracción o exposición de activos de información de forma no autorizada.	a. MG-TI-18 Políticas de seguridad de la información	STRT	Implementado
	72	8.13	Copias de seguridad de la información	A.12.3.1 Respaldo de la Información	**SI**	Se implementa el control, puesto que la STRT realiza copias de respaldo de la información, software e imágenes de los sistemas, y las pone a prueba regularmente de acuerdo con una política de copias de respaldo acordadas con las áreas.	a. MG-TI-18 Políticas de seguridad de la información Cap. 6.3.13 Política de copias de respaldo b. MGTI16 MANUAL COPIAS SEGURIDAD c. PRTI11 GENERACION DE COPIAS DE SEGURIDAD d. PRTI12 RESTAURACION DE COPIAS DE SEGURIDAD e. Solución de copias de seguridad - Backup EXEC y Veeam Backup	STRT	Implementado
	73	8.14	Redundancia de las instalaciones de procesamiento de datos	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	**SI**	Se incorpora este control en la entidad contratando instalaciones alternas de procesamiento de datos, dichas instalaciones cuentan con las certificaciones de buenas prácticas y	a. Póliza de seguro para la infraestructura física. b. Contrato de Colocation. (Datacenter TIER 3) c.PRTI20 gestión DE CONTINUIDAD DE SERVICIOS d. Se cuenta con infraestructura de procesamiento en la nube, DRP.	STRT	Implementado

Categoría	Orden	Control	Controles ISO 27001: 2022	Controles ISO 27001: 2013	Aplica	Justificación	Evidencia o registro	Responsable / Dependencia	Estado del control
						redundancias para soportar los servicios tecnológicos del IDU.			
	74	8.15	Registros	A.12.4.1 Registro de Eventos A.12.4.2 Protección de la información del registro A.12.4.3 Registros del Administrador y del Operador	**SI**	Se adopta este control, puesto que se deben elaborar, conservar y revisar regularmente los registros acerca de actividades de los usuarios, excepciones, fallas y eventos de seguridad de la información. También, en la entidad las instalaciones y la información de registro se deben proteger contra la alteración y acceso no autorizado.	a. MG-TI-18 Políticas de seguridad de la información Cap. 6.3.21 Registros de eventos automáticos de los elementos de TI b. Sistema de correlación de eventos SIEM	STRT	Implementado
	75	8.16	Actividades de seguimiento	N/A	**SI**	Se adopta este control, puesto que la STRT debe supervisar las actividades en las redes y sistemas de información para detectar comportamientos anómalos a través de monitoreo continuo, los registro de eventos y la documentación de soporte.	a. MG-TI-18 Políticas de seguridad de la información Cap. 6.3.4 Política de control de acceso a los servicios tecnológicos. b. 6.3.21 Registros de eventos automáticos de los elementos de TI. c. PR-TI-17 Gestión de servidores d. PR-TI-23 gestión de telecomunicaciones e. Contrato del servicio de SOC	STRT	Implementado
	76	8.17	Sincronización de relojes	A.12.4.4 Sincronización de Relojes	**SI**	Se implementa este control en la entidad, puesto que los relojes de todos los sistemas de procesamiento de información deben cumplir con las definiciones de la hora legal de Colombia. horalegal.inm.gov.co	a. INTI28 CONFIGURACION HORA LEGAL COLOMBIANA b. Los relojes de los sistemas del IDU se sincronizan por un servicio de NTP, desde el controlador de dominio con una fuente principal y una alterna.	STRT	Implementado
	77	8.18	Uso de programas de utilidad privilegiados	A.9.4.4 Uso de programas utilitarios privilegiados	**SI**	Se adopta este control, considerando el riesgo en donde estos programas pueden proporcionar a los usuarios, privilegios elevados que, si se utilizan de manera inapropiada, pueden comprometer la seguridad de la información del IDU.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.12 Política de instalación y uso de software y 6.3.15 Política de instalación y uso de software. b. INTI14 PREPARACION DE UN EQUIPO DE COMPUTO PARA USUARIO FINAL. Cap. 5.1 Instalación y configuración del sistema operativo	STRT	Implementado
	78	8.19	Instalación de software para sistemas operativos	A.12.5.1 Instalación de Software en Sistemas Operativos A.12.6.2 Restricciones sobre la instalación de Software	**SI**	Se adopta este control, para prevenir la instalación de software en sistemas operativos, además se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios, salvaguardando la integridad de los sistemas operativos y así evitar la explotación de las vulnerabilidades técnicas.	a. MG-TI-18 Políticas de seguridad de la información Cap. 6.3.15 Política de instalación y uso de software b. INTI07 ADMINISTRACION DEL DIRECTORIO ACTIVO c. INTI14 PREPARACION DE UN EQUIPO DE COMPUTO PARA USUARIO FINAL d. Inventario de aplicaciones FO-TI-25 e. Inventario de software en Aranda Metrix f. Repositorio de software autorizado. g. Por Directorio Activo se restringe la instalación de software en los equipos de usuario final.	STRT	Implementado
	79	8.20	Seguridad de redes	A.13.1.1 Controles de Redes	**SI**	La entidad adopta este control para establecer las directrices y asegurar que las redes sean diseñadas, implementadas y mantenidas de manera que se minimicen los riesgos asociados con la seguridad de la información.	a. MG-TI-18 Políticas de seguridad de la información Cap. 6.3.18 Política de redes y servicios de red. b. PRTI23 gestión DE TELECOMUNICACIONES c. INTI08 PROTECCION DE LA información DIGITAL d. Mapas de red	STRT	Implementado
	80	8.21	Seguridad de los servicios de red	A.13.1.2 Seguridad en los servicios de red	**SI**	Se implementa este control, puesto que es importante proteger la información que se transmite a través de redes y asegurar que los servicios de red se gestionen de manera segura, minimizando riesgos asociados con	a. MG-TI-18 Políticas de seguridad de la información Cap. 6.3.18 Política de redes y servicios de red. b. PRTI23 gestión DE TELECOMUNICACIONES c. INTI08 PROTECCION DE LA información DIGITAL d. DUTI01 CATALOGO DE SERVICIOS DE TECNOLOGIAS DE LA información Y LA COMUNICACION Cap. 5.9 SERVICIO ACCESO	STRT	Implementado

Categoría	Orden	Control	Controles ISO 27001: 2022	Controles ISO 27001: 2013	Aplica	Justificación	Evidencia o registro	Responsable / Dependencia	Estado del control
						accesos no autorizados y ciber amenazas.	SEGURO A LA RED INSTITUCIONAL e. Contratos con proveedores de servicios de Internet f. Topología de red		
	81	8.22	Segregación de redes	A.14.2.1 Política de Desarrollo Seguro	**SI**	Se adopta este control, para permitir a la STRT dividir sus redes informáticas en subredes basadas en el nivel de sensibilidad y criticidad, restringiendo el flujo de tráfico entre estas diferentes subredes y evitar así la propagación de malware o virus desde redes comprometidas hacia otras que almacenan información sensible, asegurando así que se mantenga la confidencialidad e integridad de los activos críticos.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.8 Política de desarrollo y mantenimiento seguro de software y Cap. 6.3.18 Política de redes y servicios de red. b. MG-TI-19 MANUAL DESARROLLO SEGURO DE SOFTWARE c. PRTI04 DESARROLLO DE SOLUCIONES d. INTI29 AMBIENTES DE TRABAJO PARA DESARROLLO SOFTWARE	STRT	Implementado
	82	8.23	Filtrado web	N/A	**SI**	Se implementa este control, puesto que la STRT debe prevenir el acceso a sitios web que puedan comprometer la seguridad de la información de la entidad valiéndose de la distribución de código malicioso.	a. MG-TI-18 Políticas de seguridad de la información Cap. 6.3.18 Política de redes y servicios de red. b. Módulo UTM para el filtrado web y definición de grupos de navegación.	STRT	Implementado
	83	8.24	Uso de criptografía	A.10.1.1 Política sobre el uso de controles criptográficos A.10.1.2 Gestión de Llaves	**SI**	Se adopta este control para asegurar la confidencialidad, integridad y autenticidad de los activos de información mediante el uso adecuado de técnicas criptográficas desarrollando e implementando una política sobre el uso de controles criptográficos para la protección de la información.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.4 Política de controles criptográficos b. IN-TI-08 PROTECCION DE LA información DIGITAL, Cap. 8.5 Controles criptográficos para el sistema administrativo y financiero STONE c. IN-TI-19 aplicación DE CIFRADO	STRT	Implementado
	84	8.25	Ciclo de vida de desarrollo seguro	A.14.2.1 Política de Desarrollo Seguro	**SI**	Se adopta este control en la entidad, para garantizar que los procesos de desarrollo de software en el IDU, se realicen de manera segura; minimizando los riesgos asociados con vulnerabilidades y amenazas a la seguridad, facilitando que la seguridad se integre en todas las fases del ciclo de vida del desarrollo de software, desde la planificación hasta el despliegue y mantenimiento.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.8 Política de desarrollo y mantenimiento seguro de software b. MG-TI-19 MANUAL DESARROLLO SEGURO DE SOFTWARE c. PRTI04 DESARROLLO DE SOLUCIONES d. INTI29 AMBIENTES DE TRABAJO PARA DESARROLLO SOFTWARE	STRT	Implementado
	85	8.26	Requisitos de seguridad de la aplicación	A.14.2.5 Principios de construcción de sistemas seguros	**SI**	Se implementa este control, puesto que se deben establecer, documentar y mantener principios para la construcción de sistemas de información seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información y garantizar que las aplicaciones desarrolladas y utilizadas por la entidad cumplan con los estándares de seguridad que protejan la información.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.8 Política de desarrollo y mantenimiento seguro de software b. PRTI04 DESARROLLO DE SOLUCIONES c. INTI29 AMBIENTES DE TRABAJO PARA DESARROLLO SOFTWARE d. MG-TI-19 MANUAL DESARROLLLO DE SOFTWARE SEGURO	STRT	Implementado
	86	8.27	Arquitectura del sistema y principios de ingeniería	A.14.2.5 Principios de construcción de sistemas seguros	**SI**	Se adopta este control, para establecer un marco seguro en el diseño, implementación y gestión de sistemas de información, asegurando que se	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.8 Política de desarrollo y mantenimiento seguro de software b. PRTI04 DESARROLLO DE SOLUCIONES c. INTI29 AMBIENTES DE TRABAJO PARA DESARROLLO	STRT	Implementado

Categoría	Orden	Control	Controles ISO 27001: 2022	Controles ISO 27001: 2013	Aplica	Justificación	Evidencia o registro	Responsable / Dependencia	Estado del control
						alineen con los requisitos de seguridad de la entidad.	SOFTWARE d. MG-TI-19 MANUAL DESARROLLLO DE SOFTWARE SEGURO		
	87	8.28	Codificación segura	A.14.2.7 Desarrollo contratado externamente	**SI**	Se implementa este control para garantizar la seguridad del software desarrollado, estableciendo directrices para minimizar las vulnerabilidades que pueden surgir de prácticas de codificación inadecuadas.	a. PRTI04 DESARROLLO DE SOLUCIONES b. PRTI15 gestión DE SISTEMAS DE información c. PRTI21 gestión DE COMPRAS DE PRODUCTOS Y/O SERVICIOS DE TECNOLOGIA DE información d. MG-TI-19 DESARROLLO SEGURO DE SOFTWARE d. En los contratos se incluyen cláusulas de confidencialidad y de sesión de código y derecho de propiedad.	STRT	Implementado
	88	8.29	Pruebas de seguridad en el desarrollo y aceptación	A.14.2.8 Pruebas de seguridad de sistemas	**SI**	Se adopta este control, puesto que durante el desarrollo se deben llevar a cabo pruebas de seguridad, verificando que estas sean adecuadas para identificar y corregir vulnerabilidades en el software durante las fases de desarrollo y aceptación, confirmando que los sistemas del IDU cumplen con los requisitos de seguridad definidos, asegurando su robustez frente a amenazas.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.8 Política de desarrollo y mantenimiento seguro de software b. PRTI04 DESARROLLO DE SOLUCIONES c. INTI10 REALIZACION DE PRUEBAS A LOS DESARROLLOS DE SOFTWARE d. FOTI16 ACEPTACION DE PRUEBAS REALIZADAS A LAS APLICACIONES DESARROLLADAS. e. Revisiones internas del equipo de seguridad a los sistemas de información IDU.	STRT	Implementado
	89	8.30	Desarrollo subcontratado	A.14.2.7 Desarrollo contratado externamente	**SI**	Se adopta este control, para establecer que los requisitos de seguridad de la información se mantengan incluso cuando el desarrollo de software se contrata con terceros.	a. PRTI04 DESARROLLO DE SOLUCIONES b. PRTI15 gestión DE SISTEMAS DE información c. PRTI21 gestión DE COMPRAS DE PRODUCTOS Y/O SERVICIOS DE TECNOLOGIA DE información d. En los contratos se incluyen cláusulas de confidencialidad y de sesión de código y derecho de propiedad.	STRT	Implementado
	90	8.31	Separación de los entornos de desarrollo, prueba y producción.	12.1.4Separación de los ambientes de desarrollo, ensayo y operación 14.2.6 Ambiente de desarrollo seguro	**SI**	Se implementa este control, para proteger la confidencialidad, integridad y disponibilidad de los activos de información del IDU, evitando que las actividades de desarrollo y prueba comprometan el entorno de producción, reduciendo el riesgo de errores o accesos no autorizados que puedan afectar los datos gestionados por las aplicaciones institucionales.	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.8 Política de desarrollo y mantenimiento seguro de software y Cap. 6.3.18 Política de redes y servicios de red. b. INTI10 REALIZACION DE PRUEBAS A LOS DESARROLLOS DE SOFTWARE c. FOTI16 ACEPTACION DE PRUEBAS REALIZADAS A LAS APLICACIONES DESARROLLADAS d. FO-PE-20 COMPROMISO DE INTEGRIDAD, TRANSPARENCIA, CONFIDENCIALIDAD Y CONFLICTO DE INTERESES.	STRT	Implementado
	91	8.32	Gestión de cambios	A.14.2.2 Procedimiento de Control de Cambios en sistemas A.14.2.3 Revisión Técnica de las Aplicaciones después de los cambios en la plataforma de operación A.14.2.4 Restricciones en los cambios a los paquetes de software	**SI**	Se implementa este control en la STRT, puesto que los cambios a la plataforma se deben controlar mediante el uso de procedimientos formales de control de cambios. Asimismo, se deben revisar las aplicaciones críticas de la entidad, y someter a pruebas para asegurar que no haya impacto adverso en las operaciones. Además, se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios.	a. PRTI08 gestión DE CAMBIOS b. PRTI04 DESARROLLO DE SOLUCIONES c. PRTI15 gestión DE SISTEMAS DE información d. FOTI29 CONTROL DE CAMBIOS DETECNOLOGIAS e. FOTI33 ACTIVIDADES DE CAMBIOS TECNOLOGICOS PRESENTADAS A LA MESA DE TRABAJO f. INTI10 REALIZACION DE PRUEBAS A LOS DESARROLLOS DE SOFTWARE g. INTI17 USO SERVICIO WINDOWS SERVER UPDATE	STRT	Implementado
	92	8.33	Información de prueba	A.14.3.1 Protección de datos de prueba	**SI**	Se adopta este control en la STRT para proteger los datos sensibles, asegurando que la información clasificada o reservada, protegida por la ley de datos personales al ser utilizada en pruebas no comprometa la seguridad de los activos de información de la	a. MG-TI-18 Políticas de seguridad de la información . Cap. 6.3.10 Política para los sistemas de información. b. INTI10 REALIZACION DE PRUEBAS A LOS DESARROLLOS DE SOFTWARE c. FOTI16 ACEPTACION DE PRUEBAS REALIZADAS A LAS APLICACIONES DESARROLLADAS	STRT	Implementado

Categoría	Orden	Control	Controles ISO 27001: 2022	Controles ISO 27001: 2013	Aplica	Justificación	Evidencia o registro	Responsable / Dependencia	Estado del control
						organización, manteniendo la confidencialidad e integridad a través de medidas adecuadas.	d. FO-PE-20 COMPROMISO DE INTEGRIDAD, TRANSPARENCIA, CONFIDENCIALIDAD Y CONFLICTO DE INTERESES.		
	93	8.34	Protección de los sistemas de información durante las pruebas de auditoría	A.12.7.1 Controles de auditorías de sistemas de información	**SI**	Se adopta este control, para que las actividades de auditoría no comprometan la seguridad de la información de la entidad.	a PRTI18 REVISION A LA PLATAFORMA DE TECNOLOGIA DE información b. Revisiones internas del equipo de seguridad a los sistemas de información IDU.	STRT	Implementado

8 CONTROL DE VERSIONES

Versión	Fecha	Descripción Modificación	Folios
1	2025-04-01	Cambio de tipo documental de formato a documento para facilitar su aprobación en SUE. La nueva versión recoge los controles de la última versión de las normas ISO 27001 e ISO 27701.	20

El documento original ha sido aprobado mediante el SID (Sistema Información Documentada del IDU). La autenticidad puede ser verificada a través del código

Participaron en la elaboración[1]	**Angel Antonio Diaz Vega, STRT / Carlos Fernando Campos Sosa, OAP / Hector Andres Mafla Trujillo, STRT /**
Validado por	**Liliana Pulido Villamil, OAP Validado el 2025-03-19**
Revisado por	**Jose Alfredo Ruiz Peralta, STRT Revisado el 2025-03-21 Maryid Betty Castaneda Romero, DTAF Revisado el 2025-03-25**
Aprobado por	**Gisele Manrique Vaca, SGGC Aprobado el 2025-04-01**

[1]El alcance de participación en la elaboración de este documento corresponde a las funciones del área que representan