| FORMATO | | |
|---|---|---|
| DECLARACIÓN DE APLICABILIDAD | | |
| **CÓDIGO** | **PROCESO** | **VERSIÓN** |
| FO-TI-41 | Tecnologias de Información y Comunicación | 1 |

| | Dia | Mes | Año |
|---|---|---|---|
| **Fecha de Actualización** | 21 | Diciembre | 2023 |

| Dominio | Objetivo de Control | # Ctrl | Código Control | Control | Aplica | Justificación | Selección del control | | | | Evidencia o registro | Responsable / Dependencia | Estado del control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Por valoración del riesgo | Por mejora / buena práctica | Por ser requisito legal | Cód Riesgo / Norma | | | |
| A.5. POLITICAS DE LA SEGURIDAD DE LA INFORMACION | A.5.1. ORIENTACION DE LA DIRECCION PARA LA GESTION DE LA SEGURIDAD DE LA INFORMACION | 1 | A.5.1.1 | 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 empleados y partes externas pertinentes. | X | | | I.TI.01 I.PE.03 G.IC.01 I.IC.01 I.IC.03 I.IN.01 I.IN.02 I.IN.03 G.CO.02 I.CO.02 I.CO.03 I.CO.04 I.GI.01 I.FP.01 I.FP.02 I.FP.03 I.DP.01 I.DP.02 I.DP.03 G.GP.08 I.GP.01 I.GP.02 I.GP.03 I.EO.01 I.EO.02 I.EO.03 I.CI.01 I.CI.02 I.CI.03 I.CI.04 I.RF.01 I.RF.02 I.RF.03 I.GC.01 I.GC.04 I.GC.05 I.GL.01 I.AC.04 I.GF.01 I.TH.02 I.TH.05 I.DO.01 I.DO.03 I.DO.05 G.EC.07 I.EC.01 I.EC.02 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN<br>c. Resolución 2330 de 2023 - Artículo 17. Adopción de la Directriz del SGSI.<br>d. Campañas de divulgación | STRT | Implementado |
| | | 2 | A.5.1.2 | Revisión de las Políticas para la seguridad de la Información | **SI** | Se adopta este control, puesto que las políticas se deben revisar a intervalos planificados, o sí ocurren cambios significativos para asegurar su conveniencia, adecuación y eficacias continuas. | | X | | | 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 |
| A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | A.6.1. ORGANIZACIÓN INTERNA | 3 | A.6.1.1 | Roles y responsabilidades para la Seguridad de la Información | **SI** | Se adopta este control, puesto que se deben definir y asignar todas las responsabilidades de la Seguridad de la Información. | X | X | | R.TI.07 I.CO.01 G.RF.01 I.EC.01 I.EC.02 | RESOLUCIÓN NÚMERO 6135 DE 2023<br>"Por la cual se definen los roles y las responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI" | SGGC / DTAF / STRT | Implementado |
| | | 4 | A.6.1.2 | Separación de Deberes | **SI** | Se adopta este control, puesto que los deberes y áreas de responsabilidad en conflicto se deben separar, para reducir las posibilidades de modificación no autorizada, o no intencional, o el uso indebido de los activos de la organización. | X | X | | I.TI.04 R.TI.13 I.CO.01 I.EC.01 I.EC.03 | a. RESOLUCIÓN NÚMERO 6135 DE 2023<br>b. Matriz RACI | STRT | Implementado |
| | | 5 | A.6.1.3 | Contacto con las autoridades | **SI** | Se adopta este control, puesto que se deben mantener contactos apropiados con las autoridades pertinentes. | X | | | I.TI.04 R.TI.11 | a. GU-TI-01 INTERCAMBIO DE INFORMACION CON LAS AUTORIDADES Y GRUPOS DE INTERES DEL IDU V 1.0.pdf<br>b. FOTI35 RELACION GRUPOS INTERES Y FUENTES INFORMACION V1<br>c. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN - Cap. 7.2 CONTACTO CON LAS AUTORIDADES (Incidentes)<br>d. PL-AC-01 - PLAN DE PREVENCIÓN, PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS – PPPRE<br>e. PL-PE-05 PLAN DE MANEJO DE INCIDENTES DE CONTINUIDAD | STRH | Implementado |
| | | 6 | A.6.1.4 | Contacto con los grupos de interés especial | **SI** | Se adopta este control, puesto que se deben mantener contactos apropiados con los grupos de interés especial, o foros, o asociaciones profesionales especializadas en seguridad. | X | | | I.TI.04 R.TI.11 | a. GU-TI-01 INTERCAMBIO DE INFORMACION CON LAS AUTORIDADES Y GRUPOS DE INTERES DEL IDU V 1.0.pdf<br>b. FOTI35 RELACION GRUPOS INTERES Y FUENTES INFORMACION V1<br>c. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN - Cap. 7.2 CONTACTO CON LAS AUTORIDADES (Incidentes)<br>d. PL-AC-01 - PLAN DE PREVENCIÓN, PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS – PPPRE<br>e. Boletines de CSIRT Gobierno - Correo Electrónico<br>f. WhatsApp Grupo "Segurinfo Distrito"<br>g. WhatsApp Grupo "Segur. info. IDU" | STRT | Implementado |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 7 | A.6.1.5 | Seguridad de la Información en la Gestión de Proyectos | **SI** | Se adopta este control, puesto que la seguridad de la Información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto. | X | X | | G.GI.01<br>G.GI.02 | FO-AC 56 PLANTILLA PLAN DE GESTION DE CALIDAD | OAP / SGGC | Implementado |
| | A.6.2. DISPOSITIVOS MÓVILES Y TELETRABAJO | 8 | A.6.2.1 | Política para dispositivos móviles | **SI** | Se adopta este control, puesto que se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles. | X | | | I.TI.01<br>I.TI.03<br>I.PE.03<br>I.CO.04<br>I.DP.02 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.1 Política para dispositivos móviles<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.2.3. Uso de los dispositivos móviles.<br>c. IN-TI-20 INTERCAMBIO DE INFORMACION MEDIOS EXTRAIBLES Cap. 5.5 intercambio de información mediante dispositivo móviles.<br>d. Política de APP GOOGLE en dispositivos móviles | STRT | En implementación |
| | | 9 | A.6.2.2 | Teletrabajo | **SI** | Se adopta este control, puesto que se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza el teletrabajo. | X | | | I.TI.01<br>I.TI.03<br>R.TI.16<br>I.CO.04<br>I.GP.03 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.2 Política para conexión remota a los servicios tecnológicos<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.4.4.1. Conexión de Usuarios.<br>c. GU-TH- 01 LIBRO BLANCO DE TELETRABAJO IDU | STRT - STRH | Implementado |
| A.7. SEGURIDAD DE LOS RECURSOS HUMANOS | A.7.1. ANTES DE ASUMIR EL EMPLEO | 10 | A.7.1.1 | Seguridad de los Recursos humanos / Selección | **SI** | Se adopta este control, puesto que las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos del negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos. | | | X | | a. RESOLUCIÓN NÚMERO 6135 DE 2023<br>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.<br>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 |
| | | 11 | A.7.1.2 | Términos y condiciones del empleo | **SI** | Se adopta este control, puesto que los acuerdos contractuales con los empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información. | | | X | Resolución | a. RESOLUCIÓN NÚMERO 6135 DE 2023<br>b. FO-PE-20 COMPROMISO DE INTEGRIDAD, TRANSPARENCIA, CONFIDENCIALIDAD Y CONFLICTO DE INTERESES. | DTGC / STRH | Implementado |
| | A.7.2. DURANTE LA EJECUCION DEL EMPLEO | 12 | A.7.2.1 | Responsabilidades de la Dirección | **SI** | Se adopta este control, puesto que la dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización. | X | | | I.TI.01<br>I.CO.04 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION<br>b. RESOLUCIÓN NÚMERO 6135 DE 2023 | OAP / STRH | Implementado |
| | | 13 | A.7.2.2 | Toma de Conciencia, Educación y Formación en la Seguridad de la Información | **SI** | Se adopta este control, puesto que todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo. | X | | | I.TI.01 I.TI.02 R.TI.11 I.TI.04 I.TI.05 R.TI.16 I.TI.07 I.IC.01 I.GS.01 I.IN.01 I.IN.02 I.IN.03 I.CO.03 I.CO.04 I.FP.01 I.FP.02 I.FP.03 I.DP.01 I.DP.02 I.DP.03 I.GP.01 I.GP.02 I.EO.01 I.EO.02 I.EO.03 I.CI.01 I.CI.02 I.CI.03 G.RF.01 I.RF.01 I.RF.02 I.RF.03 I.RF.05 I.RF.07 I.GC.01 I.GC.02 I.GC.03 I.GL.01 I.AC.04 G.GF.09 G.GF.10 I.GF.01 I.GF.02 I.GF.04 G.TH.06 I.TH.03 I.TH.05 | PL-CO-02 Plan de comunicaciones<br>Ruta de Posesión, Inducciones, reinducciones, Campañas con OAC, Correos, Hablemos de Seguridad Sin Tapujos, etc. | OAC / STRT | Implementado |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 14 | A.7.2.3 | Proceso Disciplinario | **SI** | Se adopta este control, puesto que se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información. | X | | | R.TI.11<br>G.EC.07 | a. 2310430-PR-126 PRIMERA INSTANCIA ETAPA INSTRUCCION<br>b. 2310430-PR-123 PROCEDIMIENTO SEGUNDA INSTANCIA<br>c. 2310430-PR-124 PRIMERA INSTANCIA-ETAPA DE JUZGAMIENTO JUICIO VERBAL<br>d. 2310430-PR-125 PROCEDIMIENTO PRIMERA INSTANCIA ETAPA JUZGAMIENTO ORDINARIO<br>e. PREC02 EJECUCION DE LA SANCION DISCIPLINARIA<br>f. PRTI22 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION | OCID / STRT | Implementado |
| | A.7.3. TERMINACION Y CAMBIO DE EMPLEO | 15 | A.7.3.1 | Terminación o cambio de responsabilidades de empleo | **SI** | Se adopta este control, puesto que las responsabilidades y los deberes de Seguridad de la Información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir. | | | X | Resolución | 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.<br>b. Circular 7 de 2019 - LINEAMIENTOS PARA LA FINALIZACIÓN DEL VÍNCULO LABORAL O CONTRACTUAL CON EL IDU<br>c. Módulo CHIE: Gestión TIC - https://openerp.idu.gov.co | STRH / DTGC | Implementado |
| A.8. GESTION DE ACTIVOS | A.8.1. RESPONSABILIDAD POR LOS ACTIVOS | 16 | A.8.1.1 | Inventario de activos | **SI** | Se adopta este control, puesto que se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos. | X | | | I.TI.02<br>I.GS.04<br>I.IN.01<br>I.RF.07<br>I.GC.01<br>G.DO.04 | a. PR-TI-13 GESTION DE ACTIVOS DE INFORMACION<br>b. IN-TI-13 Identificación de activos de información y uso del módulo de apoyo a la gestión de activos de información.<br>c. Sistema CHIE - SGSI - https://openerp.idu.gov.co<br>d. FO-TI-03 MATRIZ DE ACTIVOS DE INFORMACION, Inventario publicado en la Intranet en cada proceso | STRT | Implementado |
| | | 17 | A.8.1.2 | Propiedad de los activos | **SI** | Se adopta este control, puesto que los activos mantenidos en el inventario deben tener un propietario. | X | | | I.TI.02<br>I.IN.01<br>I.RF.07<br>I.GC.01<br>G.DO.04 | a. PR-TI-13 GESTION DE ACTIVOS DE INFORMACION<br>b. IN-TI-13 Identificación de activos de información y uso del módulo de apoyo a la gestión de activos de información.<br>c. Sistema CHIE - SGSI - https://openerp.idu.gov.co<br>d. FO-TI-03 MATRIZ DE ACTIVOS DE INFORMACION, Inventario publicado en la Intranet en cada proceso<br>e. Circular Interna 85 de 2020. PROPIEDAD DE LOS ACTIVOS DE INFORMACIÓN DENOMINADOS "SISTEMAS DE INFORMACIÓN" | STRT | Implementado |
| | | 18 | A.8.1.3 | Uso aceptable de los activos | **SI** | Se adopta este control, puesto que se deben identificar, documentar e implementar reglas para el uso aceptable de la información y de los activos asociados con información e instalaciones de procesamiento de información. | X | | | I.IN.01<br>I.CO.01<br>I.CO.03<br>I.RF.07<br>I.GC.01<br>I.GC.02<br>I.GI.01 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.11 Política de uso aceptable de los activos<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.14. Responsabilidad de los activos de información.<br>c. INTI06 USO ADECUADO DE LOS RECURSOS DE TI | STRT | Implementado |
| | | 19 | A.8.1.4 | Devolución de Activos | **SI** | Se adopta este control, puesto que TODOS los empleados y usuarios de partes externas DEBEN devolver todos los activos de la organización que se encuentren a su cargo. Al terminar su empleo, contrato o acuerdo. | X | | | I.GS.01<br>I.IN.01<br>I.CI.01<br>I.RF.01<br>I.GC.01<br>I.DO.01 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.2.6. Devolución de equipos tecnológicos.<br>b. INTI06 USO ADECUADO DE LOS RECURSOS DE TI Cap. 5.2.3 Devolución recursos TI<br>c. Paz y salvo - Módulo CHIE: Paz y Salvo - https://openerp.idu.gov.co<br>d. PR-RF-103 ADMINISTRACIÓN DE INVENTARIO DE BIENES MUEBLES | STRT / STRF | Implementado |
| | A.8.2. CLASIFICACION DE LA INFORMACION | 20 | A.8.2.1 | Clasificación de la Información | **SI** | Se adopta este control, puesto que la información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o modificación no autorizada. | X | | | I.GS.01<br>I.IN.01<br>I.FP.01<br>I.DP.01<br>I.RF.01<br>I.GF.01<br>I.DO.01 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.15. Clasificación y etiquetado de información.<br>b. PR-TI-13 GESTION DE ACTIVOS DE INFORMACIÓN<br>c. IN-TI-13 Identificación de activos de información y uso del módulo de apoyo a la gestión de activos de información.<br>d. Sistema CHIE - SGSI - https://openerp.idu.gov.co<br>e. CIRCULAR N. 216 DE 2023. CRITERIOS PARA LA CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN DEL IDU | STRF - Gestión Documental / STRT | Implementado |
| | | 21 | A.8.2.2 | Etiquetado y manejo de información | **SI** | Se adopta este control, puesto que se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización. | X | | | I.GS.01<br>I.IN.01<br>I.FP.01<br>I.DP.01<br>I.RF.01<br>I.GF.01<br>I.DO.01<br>I.DO.05 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.15. Clasificación y etiquetado de información.<br>b. PR-TI-13 GESTION DE ACTIVOS DE INFORMACIÓN<br>c. IN-TI-13 Identificación de activos de información y uso del módulo de apoyo a la gestión de activos de información.<br>d. Sistema CHIE - SGSI - https://openerp.idu.gov.co<br>e. CIRCULAR N. 216 DE 2023. CRITERIOS PARA LA CLASIFICACIÓN Y ETIQUETADO DE LA INFORMACIÓN DEL IDU | STRF - Gestión Documental / STRT | Implementado |
| | | 22 | A.8.2.3 | Manejo de Activos | **SI** | Se adopta este control, puesto que se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación adoptado por la organización. | X | | | I.GS.01<br>I.IN.01<br>I.CO.01<br>I.DP. 01<br>I.EC.01 | a. PR-TI-13 GESTION DE ACTIVOS DE INFORMACION<br>b. IN-TI-13 Identificación de activos de información y uso del módulo de apoyo a la gestión de activos de información.<br>c. Sistema CHIE - SGSI - https://openerp.idu.gov.co<br>d. FO-TI-03 MATRIZ DE ACTIVOS DE INFORMACION, Inventario publicado en la Intranet en cada proceso y en la sección Transparencia en la web. | STRT | Implementado |
| | A.8.3. MANEJO DE MEDIOS | 23 | A.8.3.1 | Gestión de Medios Removibles | **SI** | Se adopta este control, puesto que se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización. | X | X | | I.TI.03 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.2.2. Uso de los dispositivos de almacenamiento extraíbles.<br>b. Control de dispositivos a través del antivirus Bitdefender | STRT | Implementado |
| | | 24 | A.8.3.2 | Disposición de los Medios | **SI** | Se adopta este control, puesto que se debe disponer en forma segura de los medios cuando ya no se requieran, usando procedimientos formales. | X | | | I.TI.01<br>I.TI.07<br>I.MC.01 | a. PR-RF- 103 ADMINISTRACION DE INVENTARIO DE BIENES MUEBLES<br>b. IN-TI-15 BORRADO SEGURO FORMATEO FINAL EQUIPOS | STRT / STRF | Implementado |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 25 | A.8.3.3 | Transferencia de Medios Físicos | **SI** | Se adopta este control, puesto que Los medios que contienen información, se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte. | X | | | I.TI.03<br>G.GP.08<br>I.DO.06 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.7<br>Política de transferencia de información | STRT | Implementado |
| A.9. CONTROL DE ACCESO | A.9.1. REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO. | 26 | A.9.1.1 | Política de Control de Acceso | **SI** | Se adopta este control, puesto que se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. | X | | | I.TI.01<br>I.PE.03<br>I.CO.04<br>I.DP.02 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.3<br>Política de control de acceso a los servicios tecnológicos<br>b. IN-TI-16 REVISION DERECHOS ACCESO RECURSOS<br>c. IN-TI-04 INGRESO AL_CENTRO DE COMPUTO Y A LOS CENTROS DE CABLEADO<br>d. MGRF03 MANUAL SEGURIDAD Y VIGILANCIA | STRT / STRF | Implementado |
| | | 27 | A.9.1.2 | Acceso a redes y a servicios de red | **SI** | Se adopta este control, puesto que se debe permitir acceso de los usuarios a la red para los que hayan sido autorizados específicamente. | X | | | G.TI.03<br>I.TI.04<br>R.TI.14<br>I.MC.02 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.4. Servicios de red. | STRT | Implementado |
| | A.9.2. GESTIÓN DE ACCESO A USUARIOS. | 28 | A.9.2.1 | Registro y cancelación del registro de usuarios | **SI** | Se adopta este control, puesto que se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso. | X | | | R.TI.07 | a. PRTI02 GESTIONAR USUARIOS TECNOLOGICOS<br>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/gestion usuario tic/manual facilitador.html)<br>c. Registro y cancelación de cuentas mediante Directorio Activo | STRT | Implementado |
| | | 29 | A.9.2.2 | Suministro de Acceso a Usuarios | **SI** | Se adopta este control, puesto que se debe implementar un proceso de suministro de acceso formal de usuario para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios. | X | | | R.TI.07 | a. PRTI02 GESTIONAR USUARIOS TECNOLOGICOS<br>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/gestion usuario tic/manual facilitador.html)<br>c. Registro y cancelación de cuentas mediante Directorio Activo | STRT | Implementado |
| | | 30 | A.9.2.3 | Gestión de Derechos de Acceso Privilegiado | **SI** | Se adopta este control, puesto que se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. | X | | | R.TI.07<br>I.EC.02 | a. PRTI02 GESTIONAR USUARIOS TECNOLOGICOS<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.1.2. Usuarios con derechos de acceso privilegiado.<br>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/gestion usuario tic/manual facilitador.html).<br>d. Registro y cancelación de cuentas mediante Directorio Activo | STRT | Implementado |
| | | 31 | A.9.2.4 | Gestión de información de autenticación secreta de usuarios | **SI** | Se adopta este control, puesto que la asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal. | X | | | R.TI.07<br>I.CI.01 | a. PRTI02 GESTIONAR USUARIOS TECNOLOGICOS<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN.<br>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/gestion usuario tic/manual facilitador.html).<br>d. Registro y cancelación de cuentas mediante Directorio Activo | STRT | Implementado |
| | | 32 | A.9.2.5 | Revisión de los derechos de Acceso de Usuarios | **SI** | Se adopta este control, puesto que los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares. | X | | | R.TI.07 | a. PRTI02 GESTIONAR USUARIOS TECNOLOGICOS<br>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/gestion usuario tic/manual facilitador.html)<br>c. Registro y cancelación de cuentas mediante Directorio Activo<br>d. IN-TI-16 REVISION DE LOS DERECHOS DE ACCESO A LOS RECURSOS (Se ejecuta por cambios significativos en las plataformas) | STRT | Implementado |
| | | 33 | A.9.2.6 | Retiro o ajuste de derechos de acceso | **SI** | Se adopta este control, puesto que los derechos de acceso de todos los empleados y de los usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios. | X | | | R.TI.07 | a. PRTI02 GESTIONAR USUARIOS TECNOLOGICOS<br>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/gestion usuario tic/manual facilitador.html)<br>c. Registro y cancelación de cuentas mediante Directorio Activo.<br>d. Paz y salvo - Módulo CHIE: Paz y Salvo - https://openerp.idu.gov.co | STRT | Implementado |
| | A.9.3. RESPONSABILIDADES DE LOS USUARIOS. | 34 | A.9.3.1 | Uso de información de autenticación secreta | **SI** | Se adopta este control, puesto que se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta. | X | | | G.TI.03 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.1. Autenticación de las cuentas de usuario<br>b. PRTI02 GESTIONAR USUARIOS TECNOLOGICOS<br>c. Registro y cancelación de cuentas mediante Directorio Activo. | STRT | Implementado |
| | | 35 | A.9.4.1 | Restricción de Acceso a la Información | **SI** | Se adopta este control, puesto que el acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso. | X | | | I.TI.03<br>R.TI.10<br>I.TI.07 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.3<br>Política de control de acceso a los servicios tecnológicos<br>b. IN-TI-22 USO ADECUADO DE LAS CARPETAS COMPARTIDAS Cap. 5.4 ASIGNACIÓN Y REVOCACIÓN DE PERMISOS DE ACCESO.<br>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 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | A.9.4. CONTROL DE ACCESO A SISTEMAS Y APLICACIONES. | 36 | A.9.4.2 | Procedimiento de Ingreso Seguro | **SI** | Se adopta este control, puesto que cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro. | X | | | G.TI.03<br>I.DP.01 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.3 Política de control de acceso a los servicios tecnológicos<br>b. PRTI02 GESTIONAR USUARIOS TECNOLOGICOS<br>c. Restricciones de ingreso seguro mediante Directorio Activo y políticas GPO para terminación de sesiones.<br>d. IN-TI-07 ADMINISTRACION DEL DIRECTORIO ACTIVO | STRT | Implementado |
| | | 37 | A.9.4.3 | Sistema de Gestión de Contraseñas | **SI** | Se adopta este control, puesto que los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas | X | | | G.TI.03<br>I.TI.01<br>R.TI.11<br>I.TI.04<br>R.TI.14<br>I.TI.05<br>I.GS.01<br>I.IN.01<br>I.DP.01<br>I.EC.02<br>I.MC.01 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.3 Política de control de acceso a los servicios tecnológicos<br>b. PRTI02 GESTIONAR USUARIOS TECNOLOGICOS<br>c. Restricciones de ingreso seguro mediante Directorio Activo y políticas GPO para terminación de sesiones.<br>d. IN-TI-07 ADMINISTRACION DEL DIRECTORIO ACTIVO<br>e. GU-TI-02 PARA EL MANEJO DE CREDENCIALES TIC EN CONTINGENCIA<br>f. Módulo para el cambio remoto y seguro de contraseñas del Directorio Activo | STRT | Implementado |
| | | 38 | A.9.4.4 | Uso de programas utilitarios privilegiados | **SI** | Se adopta este control, puesto que se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones. | X | | | I.TI.01<br>I.TI.04 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.12 Política de instalación y uso de software<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.6.4. Instalación de aplicaciones de software y 6.6.5. Utilitarios de administración.<br>c. INTI14 PREPARACION DE UN EQUIPO DE COMPUTO PARA USUARIO FINAL. Cap. 5.1 Instalación y configuración del sistema operativo | STRT | Implementado |
| | | 39 | A.9.4.5 | Control de Acceso a Códigos Fuente de Programas | **SI** | Se adopta este control, puesto que se debe restringir el acceso a los códigos fuente de los programas. | X | | | I.TI.01 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.3 Política de control de acceso a los servicios tecnológicos<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.6.1. Protección del código fuente, desarrollo seguro y realización de pruebas de calidad.<br>c. PRTI04 DESARROLLO DE SOLUCIONES<br>d. INTI29 AMBIENTES-TRABAJO PARA DESARROLLO SOFTWARE<br>e. Software para control de versiones (GIT)<br>f. INTI08 PROTECCION DE LA INFORMACION DIGITAL, Cap. 8.4 Método usado para la gestión de versionamiento.<br>g. INTI30 UTILIZACIÓN DEL REPOSITORIO DE DOCUMENTOS Y CÓDIGO FUENTE | STRT | Implementado |
| A.10. CRIPTOGRAFIA | A.10.1. CONTROLES CRIPTOGRAFICOS | 40 | A.10.1.1 | Política sobre el uso de controles criptográficos | **SI** | Se adopta este control, puesto que se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. | X | | | I.TI.01<br>R.TI.11<br>I.PE.03 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.4 Política de controles criptográficos<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.5.3. Cifrado de archivos locales.<br>c. IN-TI-08 PROTECCION DE LA INFORMACION DIGITAL, Cap. 8.5 Controles criptográficos para el sistema administrativo y financiero STONE<br>d. IN-TI-19 APLICACION DE CIFRADO | STRT | Implementado |
| | | 41 | A.10.1.2 | Gestión de Llaves | **SI** | Se adopta este control, puesto que se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida. | X | | | R.TI.11<br>I.PE.03<br>G.GF.08 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.5 Política de gestión de llaves<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.5.3. Cifrado de archivos locales.<br>c. IN-TI-08 PROTECCION DE LA INFORMACION DIGITAL, Cap. 6. Controles de seguridad perimetral (SSL/TLS) y 8.5 Controles criptográficos para el sistema administrativo y financiero STONE<br>d. IN-TI-19 APLICACION DE CIFRADO | STRT | Implementado |
| | | 42 | A.11.1.1 | Perímetro de seguridad física | **SI** | Se adopta este control, puesto que se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información. | X | | | I.TI.06<br>A.11.1.1<br>G.EC.07<br>I.EC.01<br>I.EC.04<br>I.MC.01 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.10 Política de seguridad física y del entorno<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.17. Áreas seguras<br>c. MG-RF-03 MANUAL SEGURIDAD Y VIGILANCIA, cap. 7 Sistema de control de acceso<br>d. Existe un control de acceso a las áreas seguras.<br>e. FORF06 Planilla de control de personas que ingresan a áreas restringidas IDU | STRF / STRT | Implementado |
| | | 43 | A.11.1.2 | Controles de acceso físico | **SI** | Se adopta este control, puesto que las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado. | X | | | R.TI.10<br>I.TI.06<br>G.EC.07<br>I.EC.01<br>I.EC.04<br>I.MC.01<br>I.MC.02<br>I.MC.04 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.10 Política de seguridad física y del entorno<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.17. Áreas seguras<br>c. MG-RF-03 MANUAL SEGURIDAD Y VIGILANCIA, cap. 7 Sistema de control de acceso<br>d. Acceso mediante biométrico y tarjetas de proximidad<br>e. FORF06 Planilla de control de personas que ingresan a áreas restringidas IDU | STRF / STRT | Implementado |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A.11. SEGURIDAD FÍSICA Y DEL ENTORNO | A.11.1. AREAS SEGURAS. | 44 | A.11.1.3 | Seguridad de oficinas, recintos e instalaciones | **SI** | Se adopta este control, puesto que Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones. | X | | | R.TI.10 I.TI.06<br>I.IN.01 I.CI.01<br>I.GC.01 G.EC.07<br>I.EC.01 I.EC.04<br>I.MC.01 I.MC.02 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap.6.3.10 Política de seguridad física y del entorno<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.17. Áreas seguras<br>c. MG-RF-03 MANUAL SEGURIDAD Y VIGILANCIA, cap. 7 Sistema de control de acceso<br>d. Acceso mediante control biométrico y tarjetas de proximidad a las áreas seguras<br>e. FORF06 Planilla de control de personas que ingresan a áreas restringidas IDU | STRF / STRT | Implementado |
| | | 45 | A.11.1.4 | Protección contra amenazas externas y ambientales | **SI** | Se adopta este control, puesto que se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. | X | | | I.TI.06<br>I.RF.08<br>I.DO.06 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.10 Política de seguridad física y del entorno<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.17. Áreas seguras<br>c. MG-RF-03 MANUAL SEGURIDAD Y VIGILANCIA, cap. 7 Sistema de control de acceso<br>d. IN-TI-04 INGRESO AL CENTRO DE COMPUTO Y A LOS CENTROS DE CABLEADO. Cap. 5 condiciones para el ingreso.<br>e. El centro de cómputo tiene un sistema de detección y extinción de incendios.<br>f. La Entidad cuenta con extintores distribuidos de manera estratégica.<br>g. La Entidad tiene un Plan Institucional de Respuesta a Emergencias, enlazado con el Sistema Distrital de Atención de Emergencias.<br>h. La Entidad cuenta con una brigada para la atención de emergencias.<br>i. PL-AC-01 - PLAN DE PREVENCIÓN, PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS – PPPRE | STRH / STRF / STRT | Implementado |
| | | 46 | A.11.1.5 | Trabajo en áreas seguras | **SI** | Se adopta este control, puesto que se debe diseñar y aplicar procedimientos para trabajo en áreas seguras. | X | | | I.TI.06 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.10 Política de seguridad física y del entorno<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.17. Áreas seguras<br>c. MG-RF-03 MANUAL SEGURIDAD Y VIGILANCIA, cap. 7 Sistema de control de acceso<br>d. IN-TI-04 INGRESO AL CENTRO DE COMPUTO Y A LOS CENTROS DE CABLEADO. Cap. 5 condiciones para el ingreso | STRF / STRT | Implementado |
| | | 47 | A.11.1.6 | Áreas de despacho y carga | **SI** | Se adopta este control, puesto que se deben controlar puntos de acceso tales como áreas de despacho y de carga y otros puntos donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado. | X | | | I.RF.08 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.10 Política de seguridad física y del entorno<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.17. Áreas seguras<br>c. MG-RF-03 MANUAL SEGURIDAD Y VIGILANCIA | STRF / STRT | Implementado |
| | | 48 | A.11.2.1 | Ubicación y protección de los equipos | **SI** | Se adopta este control, puesto que los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado. | X | | | G.TI.03 I.TI.03<br>R.TI.11 I.TI.04<br>R.TI.16 I.IN.01<br>I.CO.01 I.CO.03<br>I.GP.02 I.DO.07<br>I.EC.01 I.MC.01<br>I.MC.02 I.MC.04 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.11 Política de uso aceptable de los activos<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.2. Uso adecuado de elementos y recursos de tecnología.<br>c. INTI04 INGRESO AL CENTRO DE COMPUTO Y A LOS CENTROS DE CABLEADO<br>d. INTI06 USO ADECUADO DE LOS RECURSOS DE TI<br>e. Contratos de mantenimiento plantas eléctricas y UPS | STRT | Implementado |
| | | 49 | A.11.2.2 | Servicios de suministro | **SI** | Se adopta este control, puesto que Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | x | | | I.CO.04<br>I.EC.04<br>I.MC.04 | a. INTI04 INGRESO AL CENTRO DE COMPUTO Y A LOS CENTROS DE CABLEADO<br>b. Se cuenta con servicios de respaldo, por ejemplo UPS, plantas eléctricas, aire acondicionado redundante. | STRF / STRT | Implementado |
| | | 50 | A.11.2.3 | Seguridad del cableado | **SI** | Se adopta este control, puesto que el cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño. | X | X | | G.TI.03<br>I.TI.04 | 1. PRTI23 GESTION DE TELECOMUNICACIONES cap. 1.1 Gestión de telecomunicaciones.<br>2. La entidad cuenta con cable UTP categoría 6. | STRT | Implementado |
| | | 51 | A.11.2.4 | Mantenimiento de los equipos | **SI** | Se adopta este control, puesto que los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas. | X | | | G.TI.03 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.3.2. Mantenimiento y operación<br>b. Contratos de mantenimiento preventivo y bolsa de repuestos (Datacenter - Servidores - Computadores.) | STRF / STRT | Implementado |
| | | 52 | A.11.2.5 | Retiro de Activos | **SI** | Se adopta este control, puesto que Los equipos, información o software no se deben retirar de su sitio sin autorización previa. | X | | | G.RF.07 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.2.4. Uso de los equipos de cómputo del Instituto fuera de las instalaciones.<br>b. MGRF03 MANUAL SEGURIDAD Y VIGILANCIA. Cap. Entrada y salida de bienes. | STRF / STRT | Implementado |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | A.11.2. EQUIPOS. | 53 | A.11.2.6 | Seguridad de los equipos y activos fuera de las instalaciones | **SI** | Se adopta este control, puesto que se deben aplicar medidas se seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones. | X | | | I.TI.03<br>R.TI.16<br>I.CO.01 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.2.4. Uso de los equipos de cómputo del Instituto fuera de las instalaciones<br>b. MGRF02 ADMINISTRACION DE BIENES MUEBLES E INMUEBLES DEL IDU<br>c. MGRF03 MANUAL SEGURIDAD Y VIGILANCIA Cap. Seguridad en movimientos de bienes muebles del IDU. | STRF / STRT | Implementado |
| | | 54 | A.11.2.7 | Disposición Segura o Reutilización de equipos | **SI** | Se adopta este control, puesto que se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier datos confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso. | X | | | I.TI.01<br>I.TI.07<br>I.EC.01<br>I.MC.01 | a. PR-RF- 103 ADMINISTRACION DE INVENTARIO DE BIENES MUEBLES<br>b. MGRF02 ADMINISTRACION DE BIENES MUEBLES E INMUEBLES DEL IDU<br>c. IN-TI-15 BORRADO SEGURO FORMATEO FINAL EQUIPOS<br>d. Resolución y/o actas de bajas | STRT / STRF | Implementado |
| | | 55 | A.11.2.8 | Equipos de Usuario Desatendidos | **SI** | Se adopta este control, puesto que los usuarios deben asegurarse de que a los equipos desatendidos se les da protección adecuada. | X | | | G.TI.03 I.TI.01<br>I.TI.04 I.TI.05<br>I.IC.01 I.GS.01<br>I.IN.01 I.CO.01<br>I.FP.01 I.RF.02<br>I.GC.01 I.GC.03<br>I.GF.01 I.TH.02<br>I.DO.01 I.DO.03<br>G.EC.07 I.EC.01<br>I.EC.02 I.MC.01<br>I.MC.02 I.MC.05 | a. INTI07 ADMINISTRACION DEL DIRECTORIO ACTIVO<br>b. 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 |
| | | 56 | A.11.2.9 | Política de Escritorio Limpio y pantalla limpia | **SI** | Se adopta este control, puesto que se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información. | X | | | I.TI.01 I.PE.03<br>I.IC.01 I.GS.01<br>I.IN.01 I.IN.02<br>I.IN.03 I.CO.01<br>I.CO.02 I.GI.01<br>I.FP.01 I.DP.01<br>I.EO.01 I.CI.01<br>I.CI.02<br>I.CI.03<br>I.RF.01 I.RF.02<br>I.GC.01 I.GC.03<br>I.GF.01 I.TH.02<br>I.DO.01 I.DO.03<br>G.EC.07 I.EC.01<br>I.EC.02 I.MC.01<br>I.MC.02 I.MC.05 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.6 Política de escritorio y pantalla limpia<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.9. Escritorio limpio y pantalla limpia.<br>c. Política para la gestión de pantalla limpia implementada en Directorio Activo. | STRT | Implementado |
| | A.12.1. PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES | 57 | A.12.1.1 | Procedimientos de Operación Documentados | **SI** | Se adopta este control, puesto que Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan. | X | | | I.GI.01<br>I.AC.04<br>G.GF.12<br>I.GF.02<br>I.DO.03 | Intranet IDU - Documentación SIG | OAP / STRT | Implementado |
| | | 58 | A.12.1.2 | Gestión de Cambios | **SI** | Se adopta este control, puesto que se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamientos de información que afectan la seguridad de la información. | X | | | R.TI.07<br>I.TI.03 | a. PRTI08 GESTION DE CAMBIOS<br>b. FOTI29 CONTROL DE CAMBIOS DETECNOLOGIAS<br>c. FOTI33 ACTIVIDADES DE CAMBIOS TECNOLOGICOS PRESENTADAS A LA MESA DE TRABAJO | STRT | Implementado |
| | | 59 | A.12.1.3 | Gestión de Capacidad | **SI** | Se adopta este control, puesto que 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 del sistema. | X | | | G.TI.02<br>I.DP.03<br>G.GP.08<br>I.EC.03<br>I.MC.03 | a. PRTI16 GESTION DE LA CAPACIDAD<br>b. FOTI30 CONTROL DE CAPACIDAD DE LOS RECURSOS DE TI | STRT | Implementado |
| | | 60 | A.12.1.4 | Separación de los ambientes de desarrollo, ensayo y operación | **SI** | Se adopta este control, puesto que se deben separar los ambientes de desarrollo, pruebas y operación (producción), para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación. | X | | | G.TI.01 | a. INTI29 AMBIENTES DE TRABAJO PARA DESARROLLO SOFTWARE.<br>b. Servidores de desarrollo, pruebas y producción | STRT | Implementado |
| | A.12.2. PROTECCION CONTRA CODIGO MALICIOSO | 61 | A.12.2.1 | Controles contra códigos maliciosos | **SI** | Se adopta este control, puesto que Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. | X | | | I.TI.01<br>I.TI.02<br>I.TI.03<br>I.TI.04<br>R.TI.14<br>I.CO.02<br>I.CO.03<br>I.EC.02<br>I.MC.02<br>A.12.1.3 | a.DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.1. Uso adecuado de elementos y recursos de tecnología.<br>b. INTI21 USO ANTIVIRUS EN LOS EQUIPOS DE USUARIO FINAL<br>c. Software de Antivirus Corporativo, Sandbox y WAF.<br>d. Bloqueo de puertos USB, a través del sistema antivirus.<br>e. Restricción de instalación de software no autorizada mediante política de directorio Activo. | STRT | Implementado |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A.12. SEGURIDAD DE LAS OPERACIONES | A.12.3. COPIAS DE RESPALDO | 62 | A.12.3.1 | Respaldo de la Información | **SI** | Se adopta este control, puesto que se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas. | X | | | G.TI.03 I.TI.03 R.TI.10 R.TI.16 I.GI.01 I.FP.02 I.DP.01 I.DP.02 I.DP.03 G.GP.08 I.GP.03 I.EO.01 I.CI.01 I.CI.02 I.RF.02 I.GC.02 I.AC.04 I.GF.01 I.TH.02 G.DO.02 G.DO.03 I.DO.02 G.EC.07 I.EC.04 I.MC.03 I.MC.04 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.13 Política de copias de respaldo<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.4.2. Copias de Seguridad.<br>c. MGTI16 MANUAL COPIAS SEGURIDAD<br>d. PRTI11 GENERACION DE COPIAS DE SEGURIDAD<br>e. PRTI12 RESTAURACION DE COPIAS DE SEGURIDAD<br>f. Solución de copias de seguridad - Backup EXEC y Veeam Backup | STRT | Implementado |
| | A.12.4. REGISTRO Y SEGUIMIENTO | 63 | A.12.4.1 | Registro de Eventos | **SI** | Se adopta este control, puesto que se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información. | X | | | I.TI.01 I.FP.02 I.DP.02 I.RF.02 I.EC.03 I.MC.03 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.5.4. Registros de Eventos Automáticos de los elementos de TIC<br>b. Sistema de correlación de eventos SIEM | STRT | Implementado |
| | | 64 | A.12.4.2 | Protección de la información del registro | **SI** | Se adopta este control, puesto que Las instalaciones y la información de registro se deben proteger contra la alteración y acceso no autorizado. | x | | | I.TI.01 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.5.4. Registros de Eventos Automáticos de los elementos de TIC<br>b. Sistema de correlación de eventos SIEM | STRT | Implementado |
| | | 65 | A.12.4.3 | Registros del Administrador y del Operador | **SI** | Se adopta este control, puesto que las actividades del administrador y del operador del sistema se deben registrar, los registros se deben proteger y revisar con regularidad. | X | | | R.TI.07 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.5.4. Registros de Eventos Automáticos de los elementos de TIC<br>b. Sistema de correlación de eventos SIEM | STRT | Implementado |
| | | 66 | A.12.4.4 | Sincronización de Relojes | **SI** | Se adopta este control, puesto que los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo | X | | | R.TI.07 | a. INTI28 CONFIGURACION HORA LEGAL COLOMBIANA<br>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 |
| | A.12.5. CONTROL DE SOFTWARE OPERACIONAL | 67 | A.12.5.1 | Instalación de Software en Sistemas Operativos | **SI** | Se adopta este control, puesto que se deben implementar procedimientos para controlar la instalación de software en sistemas operativos. | X | | | G.TI.03 I.TI.01 I.TI.02 I.TI.03 I.TI.05 R.TI.16 I.RF.02 I.GC.02 I.DO.02 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.12 Política de instalación y uso de software<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.6.4. Instalación de aplicaciones de software.<br>c. INTI07 ADMINISTRACION DEL DIRECTORIO ACTIVO<br>d. INTI14 PREPARACION DE UN EQUIPO DE COMPUTO PARA USUARIO FINAL<br>e. Inventario de aplicaciones FO-TI-25<br>f. Inventario de software en Aranda Metrix<br>g. Repositorio de software autorizado.<br>h. Por Directorio Activo se restringe la instalación de software en los equipos de usuario final. | STRT | Implementado |
| | A.12.6. GESTION DE LA VULNERABILIDAD TECNICA | 68 | A.12.6.1 | Gestión de las Vulnerabilidades Técnicas | **SI** | Se adopta este control, puesto que se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a esas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. | X | X | | I.TI.01 G.TI.03 | a. FOTI23 LISTA DE VULNERABILIDADES Y AMENAZAS<br>b. Informe de Análisis de vulnerabilidades y hacking ético.<br>c. Plan de remediación | STRT | Implementado |
| | | 69 | A.12.6.2 | Restricciones sobre la instalación de Software | **SI** | Se adopta este control, puesto que se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios. | X | | | G.TI.03 I.TI.01 R.TI.11 I.TI.04 R.TI.14 I.TI.05 I.IN.01 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.12 Política de instalación y uso de software<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.6.4. Instalación de aplicaciones de software.<br>c. PRTI14 GESTION DE LICENCIAMIENTO DE SW<br>d. INTI07 ADMINISTRACION DEL DIRECTORIO ACTIVO<br>e. INTI14 PREPARACION DE UN EQUIPO DE COMPUTO PARA USUARIO FINAL<br>f. Inventario de aplicaciones FO-TI-25<br>g. Inventario de software en Aranda Metrix<br>h. Repositorio de software autorizado | STRT | Implementado |
| | A.12.7. CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS DE INFORMACION | 70 | A.12.7.1 | Controles de auditorias de sistemas de información | **SI** | Se adopta este control, puesto que los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos de negocio. | X | | | I.TI.01 I.TI.03 | a PRTI18 REVISION A LA PLATAFORMA DE TECNOLOGIA DE INFORMACION<br>b. Revisiones internas del equipo de seguridad a los sistemas de información IDU. | STRT | Implementado |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A.13. SEGURIDAD DE LAS COMUNICACIONES | A.13.1 GESTION DE LA SEGURIDAD DE LAS REDES | 71 | A.13.1.1 | Controles de Redes | **SI** | Se adopta este control, puesto que las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones. | X | | | G.TI.03<br>R.TI.14<br>I.CO.02 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.4. Servicios de red.<br>b. PRTI23 GESTION DE TELECOMUNICACIONES<br>c. INTI08 PROTECCION DE LA INFORMACION DIGITAL<br>d. Mapas de red | STRT | Implementado |
| | | 72 | A.13.1.2 | Seguridad en los servicios de red | **SI** | Se adopta este control, puesto que se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten. | X | | | G.TI.03<br>G.GF.02<br>G.GF.08<br>I.EC.01<br>I.EC.03<br>I.MC.03<br>I.MC.04 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.3. Servicios de red.<br>b. PRTI23 GESTION DE TELECOMUNICACIONES<br>c. INTI08 PROTECCION DE LA INFORMACION DIGITAL<br>d. DUTI01 CATALOGO DE SERVICIOS DE TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACION Cap. 5.9 SERVICIO ACCESO SEGURO A LA RED INSTITUCIONAL<br>e. Contratos con proveedores de servicios de Internet<br>f. Topología de red | STRT | Implementado |
| | | 73 | A.13.1.3 | Separación en las Redes | **SI** | Se adopta este control, puesto que los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes. | X | | | R.TI.14 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.3. Servicios de red.<br>b. PRTI23 GESTION DE TELECOMUNICACIONES<br>c. Las redes de datos de la entidad separadas lógicamente - Topología de red | STRT | Implementado |
| | A.13.2 TRANSFERENCIA DE INFORMACION | 74 | A.13.2.1 | Políticas y procedimientos de transferencia de información | **SI** | Se adopta este control, puesto que se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones. | X | | | G.TI.03<br>I.TI.03<br>R.TI.14<br>R.TI.16<br>I.FP.03 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.7 Política de transferencia de información<br>b. PRTI23 GESTION DE TELECOMUNICACIONES<br>c. INTI08 PROTECCION DE LA INFORMACION DIGITAL<br>d. INTI11 USO DE MENSAJERIA INSTANTANEA Y COMUNICACION ELECTRONICA<br>e. INTI20 INTERCAMBIO DE INFORMACION<br>f. INTI22 USO ADECUADO DE LAS CARPETAS COMPARTIDAS | STRT | Implementado |
| | | 75 | A.13.2.2 | Acuerdos sobre transferencia de Información | **SI** | Se adopta este control, puesto que los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas. | X | | | G.TI.03<br>G.GF.02 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.7 Política de transferencia de información<br>b. PRTI23 GESTION DE TELECOMUNICACIONES<br>c. INTI19 APLICACION DE CIFRADO<br>d. INTI20 INTERCAMBIO DE INFORMACION<br>e. FO-PE-20 COMPROMISO DE INTEGRIDAD, TRANSPARENCIA, CONFIDENCIALIDAD Y CONFLICTO DE INTERESES. | STRT | Implementado |
| | | 76 | A.13.2.3 | Mensajería Electrónica | **SI** | Se adopta este control, puesto que se debe proteger adecuadamente la información incluida en la mensajería electrónica. | X | | | I.TI.05 I.GS.01<br>I.IN.01 I.DP.03<br>I.CI.01 I.CI.03<br>I.RF.01 G.GC.03<br>I.GC.03 I.DO.01<br>I.DO.03 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.4.4. Uso del correo electrónico.<br>b. INTI12 USO DEL SERVICIO DE CORREO ELECTRONICO INSTITUCIONAL<br>c. INTI11 USO DE MENSAJERIA INSTANTANEA Y COMUNICACION ELECTRONICA | STRT | Implementado |
| | | 77 | A.13.2.4 | Acuerdos de Confidencialidad o de NO divulgación | **SI** | Se adopta este control, puesto que se debe identificar, revisar y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información. | X | | | I.GS.04 I.IN.02<br>I.IN.03 I.CI.03<br>I.RF.01 I.RF.05<br>I.GC.01 I.GC.03<br>I.GC.05 I.DO.03<br>I.DO.05 G.EC.07<br>I.EC.05 I.MC.03 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.7 Política de transferencia de información<br>b. FO-PE-20 COMPROMISO DE INTEGRIDAD, TRANSPARENCIA, CONFIDENCIALIDAD Y CONFLICTO DE INTERESES. | STRT | Implementado |
| | A.14.1. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN. | 78 | A.14.1.1 | Análisis y especificación de requisitos de Seguridad de la Información | **SI** | Se adopta este control, puesto que los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras de sistemas de información existentes | X | | | G.TI.01<br>G.RF.01 | 1. PRTI04 DESARROLLO DE SOLUCIONES<br>2. PRTI15 GESTION DE SISTEMAS DE INFORMACION<br>3. FOTI06 SOLICITUD REQUERIMIENTOS APLICACIONES | STRT | Implementado |
| | | 79 | A.14.1.2 | Seguridad en los servicios de las aplicaciones en redes públicas | **SI** | Se adopta este control, puesto que la información involucrada en los servicios de las aplicaciones que pasan por las redes públicas se debe proteger de actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizadas. | X | | | G.TI.01 | a. PRTI23 GESTION DE TELECOMUNICACIONES<br>b. INTI08 PROTECCION DE LA INFORMACION DIGITAL<br>c. Banca electrónica segura en el proceso Gestión Financiera. | STRT | Implementado |
| | | 80 | A.14.1.3 | Protección de transacciones de los servicios de las aplicaciones | **SI** | Se adopta este control, puesto que la información involucrada en los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada | X | | | G.TI.01<br>G.GF.05 | a. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.16. Uso de firmas electrónicas y medios técnicos de autenticación (tokens)<br>b. INTI08 PROTECCION DE LA INFORMACION DIGITAL<br>c. Banca electrónica segura en el proceso Gestión Financiera. | STRT | Implementado |
| | | 81 | A.14.2.1 | Política de Desarrollo Seguro | **SI** | Se adopta este control, puesto que se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro del organización | X | X | | G.TI.01<br>I.TI.01<br>I.PE.03 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.8 Política de desarrollo y mantenimiento seguro de software<br>b. MG-TI-19 MANUAL DESARROLLO SEGURO DE SOFTWARE<br>c. PRTI04 DESARROLLO DE SOLUCIONES<br>d. INTI29 AMBIENTES DE TRABAJO PARA DESARROLLO SOFTWARE | STRT | Implementado |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS. | A.14.2. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE. | 82 | A.14.2.2 | Procedimiento de Control de Cambios en sistemas | **SI** | Se adopta este control, puesto que los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios. | X | | | G.TI.01 | a. PRTI08 GESTION DE CAMBIOS<br>b. PRTI04 DESARROLLO DE SOLUCIONES<br>c. PRTI15 GESTION DE SISTEMAS DE INFORMACION<br>d. FOTI29 CONTROL DE CAMBIOS DETECNOLOGIAS<br>e. FOTI33 ACTIVIDADES DE CAMBIOS TECNOLOGICOS PRESENTADAS A LA MESA DE TRABAJO | STRT | Implementado |
| | | 83 | A.14.2.3 | Revisión Técnica de las Aplicaciones después de los cambios en la plataforma de operación | **SI** | Se adopta este control, puesto que cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas de negocio, y someter a pruebas para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización. | X | X | | R.TI.07<br>I.TI.03 | a. PRTI08 GESTION DE CAMBIOS<br>b. PRTI04 DESARROLLO DE SOLUCIONES<br>c. PRTI15 GESTION DE SISTEMAS DE INFORMACION<br>d. FOTI29 CONTROL DE CAMBIOS DETECNOLOGIAS<br>e. FOTI33 ACTIVIDADES DE CAMBIOS TECNOLOGICOS PRESENTADAS A LA MESA DE TRABAJO<br>f. INTI10 REALIZACION DE PRUEBAS A LOS DESARROLLOS DE SOFTWARE<br>g. INTI17 USO SERVICIO WINDOWS SERVER UPDATE | STRT | Implementado |
| | | 84 | A.14.2.4 | Restricciones en los cambios a los paquetes de software | **SI** | Se adopta este control, puesto que se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente. | X | | | R.TI.07 | a. PRTI08 GESTION DE CAMBIOS<br>b. PRTI04 DESARROLLO DE SOLUCIONES<br>c. PRTI15 GESTION DE SISTEMAS DE INFORMACION<br>d. FOTI29 CONTROL DE CAMBIOS DETECNOLOGIAS<br>e. FOTI33 ACTIVIDADES DE CAMBIOS TECNOLOGICOS PRESENTADAS A LA MESA DE TRABAJO<br>f. INTI10 REALIZACION DE PRUEBAS A LOS DESARROLLOS DE SOFTWARE<br>g. INTI17 USO SERVICIO WINDOWS SERVER UPDATE | STRT | Implementado |
| | | 85 | A.14.2.5 | Principios de construcción de sistemas seguros | **SI** | Se adopta este control, puesto que se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información. | X | X | | G.TI.01 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.8 Política de desarrollo y mantenimiento seguro de software<br>b. PRTI04 DESARROLLO DE SOLUCIONES<br>c. INTI29 AMBIENTES DE TRABAJO PARA DESARROLLO SOFTWARE<br>d. MG-TI-19 MANUAL DESARROLLLO DE SOFTWARE SEGURO | STRT | Implementado |
| | | 86 | A.14.2.6 | Ambiente de desarrollo seguro | **SI** | Se adopta este control, puesto que las organizaciones se deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de software. | X | | | I.TI.04 | a. PRTI04 DESARROLLO DE SOLUCIONES<br>b. INTI29 AMBIENTES-TRABAJO PARA DESARROLLO SOFTWARE<br>c. Servidores de desarrollo, pruebas y producción<br>d. MG-TI-19 MANUAL DESARROLLLO DE SOFTWARE SEGURO | STRT | Implementado |
| | | 87 | A.14.2.7 | Desarrollo contratado externamente | **SI** | Se adopta este control, puesto que la organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente. | X | | | I.TI.08 | a. PRTI04 DESARROLLO DE SOLUCIONES<br>b. PRTI15 GESTION DE SISTEMAS DE INFORMACION<br>c. PRTI21 GESTION DE COMPRAS DE PRODUCTOS Y/O SERVICIOS DE TECNOLOGIA DE INFORMACION<br>d. En los contratos se incluyen cláusulas de confidencialidad y de sesión de código y derecho de propiedad. | STRT | Implementado |
| | | 88 | 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 funcionalidad | | X | | G.TI.01<br>I.TI.01 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.8 Política de desarrollo y mantenimiento seguro de software<br>b. PRTI04 DESARROLLO DE SOLUCIONES<br>c. INTI10 REALIZACION DE PRUEBAS A LOS DESARROLLOS DE SOFTWARE<br>d. FOTI16 ACEPTACION DE PRUEBAS REALIZADAS A LAS APLICACIONES DESARROLLADAS.<br>e. Revisiones internas del equipo de seguridad a los sistemas de información IDU. | STRT | Implementado |
| | | 89 | A.14.2.9 | Pruebas de aceptación de sistemas | **SI** | Se adopta este control, puesto que para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados | X | X | | G.TI.01<br>I.TI.01 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.8 Política de desarrollo y mantenimiento seguro de software<br>b. PRTI04 DESARROLLO DE SOLUCIONES<br>c. INTI10 REALIZACION DE PRUEBAS A LOS DESARROLLOS DE SOFTWARE<br>d. FOTI16 ACEPTACION DE PRUEBAS REALIZADAS A LAS APLICACIONES DESARROLLADAS | STRT | Implementado |
| | A.14.3. DATOS DE PRUEBA. | 90 | A.14.3.1 | Protección de datos de prueba | **SI** | Se adopta este control, puesto que los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente. | | X | | G.TI.01<br>I.TI.01 | a. DU-TI-06 POLITICAS OPERACIONALES DE TECNOLOGIAS DE INFORMACION Y COMUNICACIÓN. Cap. 6.6.2. Datos de prueba.<br>b. INTI10 REALIZACION DE PRUEBAS A LOS DESARROLLOS DE SOFTWARE<br>c. FOTI16 ACEPTACION DE PRUEBAS REALIZADAS A LAS APLICACIONES DESARROLLADAS<br>d. FO-PE-20 COMPROMISO DE INTEGRIDAD, TRANSPARENCIA, CONFIDENCIALIDAD Y CONFLICTO DE INTERESES. | STRT | Implementado |
| | A.15.1. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES. | 91 | A.15.1.1 | Política de Seguridad de la Información para las relaciones con proveedores | **SI** | Se adopta este control, puesto que los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar y documentar. | X | | | I.TI.01<br>I.PE.03 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.9 Política de seguridad de la información para la relación con proveedores<br>b. PRTI21 GESTION DE COMPRAS DE PRODUCTOS Y/O SERVICIOS DE TECNOLOGIA DE INFORMACION<br>c. FO-PE-20 COMPROMISO DE INTEGRIDAD, TRANSPARENCIA, CONFIDENCIALIDAD Y CONFLICTO DE INTERESES. | STRT | Implementado |
| | | 92 | A.15.1.2 | Tratamiento de la Seguridad dentro de los acuerdos con proveedores | **SI** | Se adopta este control, puesto que se deben establecer y acordar todos los requisitos de seguridad pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para información de la organización. | X | | | I.TI.08<br>I.RF.08 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.9 Política de seguridad de la información para la relación con proveedores<br>b. PRTI21 GESTION DE COMPRAS DE PRODUCTOS Y O SERVICIOS DE TECNOLOGIA DE INFORMACION<br>c. FO-PE-20 COMPROMISO DE INTEGRIDAD, TRANSPARENCIA, CONFIDENCIALIDAD Y CONFLICTO DE INTERESES. | STRT | Implementado |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A.15. RELACIONES CON LOS PROVEEDORES | | 93 | A.15.1.3 | Cadena de Suministro de Tecnología de Información y Comunicación | **SI** | Se adopta este control, puesto que los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos o servicios de tecnología de la información y comunicación | X | | | I.TI.04<br>I.TI.08 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.9 Política de seguridad de la información para la relación con proveedores<br>b. PRTI21 GESTION DE COMPRAS DE PRODUCTOS Y O SERVICIOS DE TECNOLOGIA DE INFORMACION<br>c. FO-PE-20 COMPROMISO DE INTEGRIDAD, TRANSPARENCIA, CONFIDENCIALIDAD Y CONFLICTO DE INTERESES. | STRT | Implementado |
| | A.15.2. GESTIÓN DE LA PRESTACIÓN DE LOS SERVICIOS DE PROVEEDORES. | 94 | A.15.2.1 | Seguimiento y revisión de los servicios de los proveedores | **SI** | Se adopta este control, puesto que las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores. | X | | | I.TI.08 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.9 Política de seguridad de la información para la relación con proveedores<br>b. PRTI21 GESTION DE COMPRAS DE PRODUCTOS Y O SERVICIOS DE TECNOLOGIA DE INFORMACION<br>c. Contratos.<br>d. Procedimientos<br>PRGC01 Mínima cuantía contratación hasta el 10% de la menor cuantía<br>PRGC03 Selección abreviada menor cuantía<br>PRGC04 Concurso de méritos abierto o con precalificación<br>PRGC05 Suscripción de contratos derivados de procesos de selección producto convocatoria pública | STRT | Implementado |
| | | 95 | A.15.2.2 | Gestión de Cambios en los Servicios de los Proveedores | **SI** | Se adopta este control, puesto que se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de la seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, la reevaluación de los riesgos. | X | | | R.TI.07<br>I.TI.03<br>I.TI.08<br>G.GL.06 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.9 Política de seguridad de la información para la relación con proveedores<br>b. PRTI21 GESTION DE COMPRAS DE PRODUCTOS Y O SERVICIOS DE TECNOLOGIA DE INFORMACION<br>c. PRTI08 GESTION DE CAMBIOS | STRT | Implementado |
| A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | A.16.1. GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN. | 96 | A.16.1.1 | Gestión de Incidentes / Responsabilidades y Procedimientos | **SI** | Se adopta este control, puesto que se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. | X | | | R.TI.11<br>R.TI.13<br>I.EC.03 | a. RESOLUCIÓN NUMERO 6135 DE 2023 "Por la cual se definen los roles y las responsabilidades del Subsistema de Gestión de Seguridad de la Información - SGSI"<br>b. PRTI22 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION<br>c. GU-TI-03 GUÍA ANALISIS FORENSE PARA INCIDENTES SEGURIDAD DE LA INFORMACION<br>d. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | STRT | Implementado |
| | | 97 | A.16.1.2 | Reporte de Eventos de Seguridad de la Información | **SI** | Se adopta este control, puesto que los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible. | X | | | R.TI.11<br>R.TI.13 | a. PRTI22 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION<br>b. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN<br>c. FOTI28 CONDICIONES PARA VALIDACION DE EVENTOS DE SEGURIDAD DE LA INFORMACION<br>d. Módulo Aranda USDK para el reporte de requerimientos e incidentes. | STRT | Implementado |
| | | 98 | A.16.1.3 | Reporte de debilidades de seguridad de la información | **SI** | Se adopta este control, puesto que se debe exigir a los todos los empleados y contratistas que usan servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. | X | | | R.TI.11<br>R.TI.13<br>G.GL.06<br>G.GF.01<br>G.GF.02<br>G.GF.07 | a. PRTI22 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION<br>b. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN<br>c. FOTI28 CONDICIONES PARA VALIDACION DE EVENTOS DE SEGURIDAD DE LA INFORMACION<br>d. Módulo Aranda USDK para el reporte de requerimientos e incidentes. | STRT | Implementado |
| | | 99 | A.16.1.4 | Evaluación de Eventos de Seguridad de la Información y decisiones sobre ellos | **SI** | Se adopta este control, puesto que los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información. | X | | | R.TI.11<br>I.TI.04<br>R.TI.13 | a. PRTI22 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION<br>b. GU-TI-03 GUÍA ANALISIS FORENSE PARA INCIDENTES SEGURIDAD DE LA INFORMACION<br>c. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN<br>d. Módulo Aranda USDK para el reporte de requerimientos e incidentes.<br>e. FOTI42 INFORME DE INCIDENTES DE SEGURIDAD DE LA INFORMACION | STRT | Implementado |
| | | 100 | A.16.1.5 | Respuesta a incidentes de seguridad de la información | **SI** | Se adopta este control, puesto que se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados. | X | | | R.TI.11<br>I.TI.04<br>R.TI.13 | a. PRTI22 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION<br>b. GU-TI-03 GUÍA ANALISIS FORENSE PARA INCIDENTES SEGURIDAD DE LA INFORMACION<br>c. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN<br>d. FOTI42 INFORME DE INCIDENTES DE SEGURIDAD DE LA INFORMACION | STRT | Implementado |
| | | 101 | A.16.1.6 | Aprendizaje obtenido de los incidentes de seguridad de la información | **SI** | Se adopta este control, puesto que el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros. | X | | | R.TI.11<br>I.TI.04<br>R.TI.13 | a. PRTI22 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION<br>b. GU-TI-03 GUÍA ANALISIS FORENSE PARA INCIDENTES SEGURIDAD DE LA INFORMACION<br>c. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN<br>d. Módulo Aranda USDK para el reporte de requerimientos e incidentes.<br>e. FOTI42 INFORME DE INCIDENTES DE SEGURIDAD DE LA INFORMACION | STRT | Implementado |
| | | 102 | A.16.1.7 | Recolección de Evidencia | **SI** | Se adopta este control, puesto que la organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia. | X | | | R.TI.11<br>I.TI.04<br>R.TI.13 | a. PRTI22 GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION<br>b. GU-TI-03 GUÍA ANALISIS FORENSE PARA INCIDENTES SEGURIDAD DE LA INFORMACION<br>c. GU-TI-04 GUÍA DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN<br>d. Módulo Aranda USDK para el reporte de requerimientos e incidentes.<br>e. FOTI42 INFORME DE INCIDENTES DE SEGURIDAD DE LA INFORMACION<br>f. FOTI43 EVIDENCIA DIGITAL | STRT | Implementado |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A.17.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACION | A.17.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN | 103 | A.17.1.1 | Planificación de la continuidad de la Seguridad de la Información | **SI** | Se adopta este control, puesto que la organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre. | X | | | I.TI.06 I.TI.07 I.GP.03 I.CI.04 I.RF.04 I.RF.06 I.RF.08 G.GC.03 I.GC.04 I.GF.01 I.GF.02 I.GF.03 I.DO.04 I.EC.04 I.MC.04 | a. PRTI20 GESTION DE CONTINUIDAD DE SERVICIOS<br>b. PLTI01 PLAN RECUPERACION ANTE DESASTRES<br>c. FOTI38 PLAN DE PRUEBAS PARA DRP<br>d. FOTI39 GUIÓN PARA PRUEBAS DE DRP<br>e. FOTI40 MINUTOGRAMA PARA PRUEBAS DRP | STRT | Implementado |
| | | 104 | A.17.1.2 | Implementación de la continuidad de la seguridad de la información | **SI** | Se adopta este control, puesto que la organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa. | X | | | I.TI.06 I.TI.07 I.GP.03 I.CI.04 I.RF.04 I.RF.06 I.RF.08 G.GC.03 I.GC.04 I.GF.01 I.GF.02 I.GF.03 I.DO.04 I.EC.04 | a. PRTI20 GESTION DE CONTINUIDAD DE SERVICIOS<br>b. PLTI01 PLAN RECUPERACION ANTE DESASTRES<br>c. INTI03 RESTAURACION DE LA APLICACION VALORICEMOS<br>d. INTI23 RESTAURACION BOTON AZUL<br>e. INTI24 RESTAURACION SISTEMAS BASADOS EN ODOO<br>f. INTI26 RESTAURACION SISTEMA KACTUS<br>g. INTI27 RESTAURACION SISTEMA STONE<br>h. FOTI26 ARBOL DE LLAMADAS PARA CONTINUIDAD DEL NEGOCIO<br>i. PLPE05 PLAN DE MANEJO DE INCIDENTES DE CONTINUIDAD | STRT | Implementado |
| | | 105 | A.17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | **SI** | Se adopta este control, puesto que la organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas. | X | | | I.GF.03 | a. PRTI20 GESTION DE CONTINUIDAD DE SERVICIOS<br>b. PLPE05 PLAN DE MANEJO DE INCIDENTES DE CONTINUIDAD<br>c. PLTI01 PLAN RECUPERACION ANTE DESASTRES<br>d. Informes de las pruebas realizadas | STRT | Implementado |
| | A.17.2. REDUNDANCIAS | 106 | A.17.2.1 | Disponibilidad de instalaciones de procesamiento de información | **SI** | Se adopta este control, puesto que las instalaciones de procesamiento de la información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad. | X | | | I.TI.06 I.TI.07 G.GC.03 I.GF.03 I.EC.04 | a. Póliza de seguro para la infraestructura física.<br>b. Contrato de Colocation. (Datacenter TIER 3)<br>c.PRTI20 GESTION DE CONTINUIDAD DE SERVICIOS<br>d. Se cuenta con infraestructura de procesamiento en la nube, DRP. | STRT | Implementado |
| A.18. CUMPLIMIENTO | A.18.1. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES | 107 | A.18.1.1 | Identificación de la legislación aplicable y los requisitos contractuales | **SI** | Se adopta este control, puesto que todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información de la organización. | X | | X | G.TH.06 G.TH.07 G.DO.01 | a. El normograma está publicado en la web institucional, por procesos, en la siguiente URL:<br>https://www.idu.gov.co/page/transparencia/normatividad/normograma<br>b. En la Intranet - mapa de procesos. | DTGC / STRT | Implementado |
| | | 108 | 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 de software patentados. | X | | X | I.DO.07 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.12 Política de instalación y uso de software<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.6.1. Protección del código fuente, desarrollo seguro y realización de pruebas de calidad.<br>c. PRTI14 GESTION DE LICENCIAMIENTO DE SW<br>d. FOTI25 INVENTARIO APLICACIONES<br>e. Informe Anual sobre Derechos de Autor en materia de software. | STRT | Implementado |
| | | 109 | A.18.1.3 | Protección de registros | **SI** | Se adopta este control, puesto que los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación contractuales y de negocio. | X | | | R.TI.07 I.DO.02 | MGDO01 GESTION DOCUMENTAL | STRF / STRT / OAP | Implementado |
| | | 110 | A.18.1.4 | Privacidad y Protección de información de datos personales | **SI** | Se adopta este control, puesto que Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y en la reglamentación pertinentes, cuando sea aplicable. | X | | X | I.GS.04 I.CI.02 I.RF.05 I.GC.05 I.AC.04 I.GF.04 I.TH.05 I.EC.05 I.MC.05 Ley 1581 de 2012 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.14 Política de Privacidad y protección de datos personales<br>b. MGTI17 PROTECCION DE DATOS PERSONALES | OAC / OTC / STRT | Implementado |
| | | 111 | A.18.1.5 | Reglamentación de Controles Criptográficos | **SI** | Se adopta este control, puesto que se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes. | X | | | R.TI.11 I.TI.04 | a. MG-TI-18 POLITICAS DE SEGURIDAD DE LA INFORMACION . Cap. 6.3.4 Política de controles criptográficos<br>b. DU-TI-06 POLÍTICAS OPERACIONALES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Cap. 6.5.3. Cifrado de archivos locales.<br>c. IN-TI-08 PROTECCION DE LA INFORMACION DIGITAL, Cap. 8.5 Controles criptográficos para el sistema administrativo y financiero STONE<br>d. IN-TI-19 APLICACION DE CIFRADO | STRT | Implementado |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | A.18.2. REVISIONES DE SEGURIDAD DE LA INFORMACION | 112 | A.18.2.1 | Revisión Independiente de la Seguridad de Información | **SI** | Se adopta este control, puesto que El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para la seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos. | X | | | I.TI.01<br>I.TI.03<br>I.TI.04 | a. PRTI18 REVISION A LA PLATAFORMA DE TECNOLOGIA DE INFORMACION<br>b. Programa de Auditoría<br>c. PREC01 EVALUACION INDEPENDIENTE Y AUDITORIAS INTERNAS<br>d. Auditorías externas | OAP / OCI / STRT | Implementado |
| | | 113 | A.18.2.2 | Cumplimiento con las políticas y normas de seguridad | **SI** | Se adopta este control, puesto que los Directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad. | X | | | I.TI.06<br>G.EC.07<br>I.EC.02 | a. Resolución 2330 de 2023.<br>b. PRTI18 REVISION A LA PLATAFORMA DE TECNOLOGIA DE INFORMACION<br>c. PRTI24 GESTION OPTIMIZACION DEL PROCESO<br>d. PRMC03 REVISION POR LA DIRECCION | STRT | Implementado |
| | | 114 | A.18.2.3 | Revisión del cumplimiento técnico | **SI** | Se adopta este control, puesto que los Sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información. | X | | | G.TI.03<br>R.TI.07<br>R.TI.11<br>I.TI.04 | a. PRTI24 GESTION OPTIMIZACION DEL PROCESO<br>b. PRTI18 REVISION A LA PLATAFORMA DE TECNOLOGIA DE INFORMACION<br>c. Informe de Análisis de vulnerabilidades y hacking ético<br>d. PREC01 EVALUACION INDEPENDIENTE Y AUDITORIAS INTERNAS | STRT | Implementado |

| | |
|---|---|
| Total controles adoptados | **114** |
| Total controles SIN adoptar | **0** |

| **Preparado por:** | **Preparado por:** | **Revisado por:** | **Aprobado por:** | **Aprobado por:** |
|---|---|---|---|---|
| **Erika Tatiana Quintero Quintero** | **Hector Andres Mafla Trujillo** | **Arleth Patricia Saurith Contreras** | **Mercy Yasmín Parra Rodríguez** | **Rosita Esther Barrios Figueroa** |
| Oficial de Seguridad de la Información | Profesional Especializado<br>Equipo de Seguridad de la Información | Subdirectora Técnica de Recursos Tecnológicos | Dirección Técnica Administrativa y Financiera | Subdirectora General de Gestión Corporativa<br>Líder del Subsistema de Gestión de Seguridad de la Información |