| FORMATO<br>DECLARACIÓN DE APLICABILIDAD (DDA) PARA SEGURIDAD DE LA INFORMACIÓN | | | ALCALDÍA MAYOR DE BOGOTÁ D.C.<br>Instituto Desarrollo Urbano |
|---|---|---|---|
| CODIGO | PROCESO | VERSIÓN | |
| FO-TI-27 | GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN | 1.0 | |

La declaración de aplicabilidad de controles para el Sistema de Gestión de Seguridad de la Información - SGSI es una documento base para determinar los resultados de la identificación y valoración de riesgos de seguridad de la información, así como para formular actividades de tratamiento de riesgos, que cada líder operativo de proceso ha estimado convenientes, para mitigarlos y operar de forma segura y conforme los requisitos de los servicios ofrecidos por la entidad.

Los controles aplicables para la operación del Sistema de Gestión de Seguridad de la Información, son los numerales que se relacionan a continuación en el "Detalle de la Declaración de Aplicabilidad", tramitado con base en las recomendaciones de la norma NTC/ISO 27001:2013.

La presente declaración de aplicabilidad será revisada conjuntamente con los resultados de cada nuevo proceso de valoración de riesgos y/o ante cambios significativos de los elementos de la plataforma tecnológica y/o de personal. Esta información, será material de comparación en los procesos de revisión por la dirección del SGSI, en los periodos convenidos para su actualización.

Se firma la presente Declaración de Aplicabilidad,

| Carlos Humberto Moreno Bermúdez | Gustavo Adolfo Vélez Achury | Isauro Cabrera Vega |
|---|---|---|
| Subdirector General de Gestión Corporativa | Subdirector Técnico de Recursos Tecnológicos | Jefe Oficina Asesora de Planeación |

A continuación, se presenta el detalle de la Declaración de Aplicabilidad de los controles necesarios para gestionar los riesgos que afectan a la Seguridad de la Información, que fueron identificados y valorados en el Instituto de Desarrollo Urbano - IDU.

| Dominio | Subdominio | Control Actual | Objetivos de Control | Aplica | Justificación | Declaración de Aplicabilidad |
|---|---|---|---|---|---|---|
| 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 | 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. | Publicación de la Resolución 34217 de 2015. |
| | | 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 si ocurren cambios significativos para asegurar su conveniencia, adecuación y eficacias continuas. | Acta de reunión del Comité SIG, en donde se evidencia la revisión de las políticas de los Subsistemas y su debida alineación. |
| | A.6.1. ORGANIZACIÓN INTERNA | A.6.1.1 | Roles y responsabilidades para la Seguridad de la Información | SI | | Documento Responsabilidades ante el SGSI (en construcción). Este documento pretende explicar las exigencias desde y hacia los colaboradores del Instituto, frente a la seguridad de la Información, haciendo un recorrido, punto a punto de la norma de referencia NTC-ISO 27001 |
| | | 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. | Documento SERVICIOS TI VS GRUPOS DE TRABAJO. Es un documento similar a la matriz RACI. |
| | | A.6.1.3 | Contacto con las autoridades | SI | Se adopta este control, puesto que se deben mantener contactos apropiados con las autoridades pertinentes. | Documento "Guía de contactos con las autoridades y grupos de interés del IDU" |

| | | | | | | |
|---|---|---|---|---|---|---|
| A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | | A.6.1.4 | Contacto con las 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. | Documento "Guía de contactos con las autoridades y grupos de interés del IDU" |
| | | 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. | Formato Lista de chequeo - Seguridad de la Información en los Proyectos |
| | A.6.2. DISPOSITIVOS MÓVILES Y TELETRABAJO | 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. | Resolución 34217 de 2015.<br>Instructivo de uso adecuado de los dispositivos de almacenamiento de información (IN-TI-05) |
| | | 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. | Resolución 34217 de 2015.<br>Libro Blanco de Teletrabajo IDU (GU-TH-01) |
| A.7. SEGURIDAD DE LOS RECURSOS HUMANOS | A.7.1. ANTES DE ASUMIR EL EMPLEO | 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. | Consideraciones en la definición de las requisiciones de personal de planta, o requisitos para contratación de prestación de servicios profesionales. (Se debe procurar la inclusión de elementos de seguridad de la información en la definición de perfiles de cargo. – En revisión con Gestión del Talento Humano y Gestión Contractual). |
| | | 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. | Solicitud a Gestión del Talento Humano, para la inclusión de obligaciones y responsabilidades específicas frente a la seguridad de la información, tanto para servidores de planta como para contratistas de apoyo. (En trámite). |
| | A.7.2. DURANTE LA EJECUCION DEL EMPLEO | 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. | Resolución 34217 de 2015.<br>Documento Responsabilidades ante el SGSI (en construcción). Este documento pretende explicar las exigencias desde y hacia los colaboradores del Instituto, frente a la seguridad de la Información, haciendo un recorrido, punto a punto de la norma de referencia NTC-ISO 27001 |
| | | 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. | Bienvenidas, Inducciones, reinducciones, Campañas con OAC, Tertulias. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 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. | Procedimiento de control disciplinario ordinario (PR-007)<br><br>Procedimiento de control disciplinario verbal (PR-008)<br><br>Procedimiento de Gestión de Incidentes de Seguridad de la Información |
| | A.7.3. TERMINACION Y CAMBIO DE EMPLEO | 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. | Suscripción de cláusulas de confidencialidad y no divulgación de la información del Instituto, por un periodo de hasta seis (6) meses de la desvinculación o terminación del contrato. (Solicitud enviada a Gestión del Talento Humano). |
| A.8. GESTION DE ACTIVOS | A.8.1. RESPONSABILIDAD POR LOS ACTIVOS | 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. | Procedimiento Gestión de activos de información (PR-TI-13)<br><br>Formato Matriz de activos de información (FO-TI-03)<br><br>Inventario publicado en la Intranet |
| | | 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. | Procedimiento Gestión de activos de información (PR-TI-13)<br><br>Formato Matriz de activos de información (FO-TI-03)<br><br>Inventario publicado en la Intranet |
| | | 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. | Instructivo de Uso adecuado de los recursos de TI (IN-TI- 06). |
| | | 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. | Instructivo de Uso adecuado de los recursos de TI (IN-TI- 06). |
| | A.8.2. CLASIFICACION DE LA INFORMACION | 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. | Acta del comité de archivo para la presentación y aprobación de instrumentos archivísticos del IDU del 05/Nov/2015 |
| | | 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. | Acta del comité de archivo para la presentación y aprobación de instrumentos archivísticos del IDU del 05/Nov/2015.<br><br>Instrumentos de etiquetado en construcción. Estos controles deben permitir a los colaboradores marcar e identificar los activos de información respecto a su accesibilidad, teniendo en cuenta los acuerdos aprobados en comité de archivo. |

| FORMATO<br>DECLARACIÓN DE APLICABILIDAD (DDA) PARA SEGURIDAD DE LA INFORMACIÓN | | | | | | ALCALDÍA MAYOR DE BOGOTÁ D.C.<br>Desarrollo Urbano |
|---|---|---|---|---|---|---|
| CODIGO<br>FO-TI-27 | PROCESO<br>GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN | | | | VERSIÓN<br>1.0 | |
| | | 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. | Procedimiento Gestión de activos de información (PR-TI-13)<br><br>Formato Matriz de activos de información (FO-TI-03)<br><br>Instructivo de Uso adecuado de los recursos de TI (IN-TI- 06) |
| | A.8.3. MANEJO DE MEDIOS | 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. | Instructivo de uso adecuado de los dispositivos de almacenamiento de información (IN-TI-05) |
| | | 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. | Instructivo borrado seguro de datos y formateo final de equipos (en construcción). Este documento describe las actividades necesarias para eliminar permanentemente información de los medios de almacenamiento. |
| | | 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. | Instructivo de uso adecuado de los dispositivos de almacenamiento de información (IN-TI-05) |
| | A.9.1. REQUISITOS DEL NEGOCIO PARA EL CONTROL DE ACCESO. | 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. | Resolución 34217 de 2015. |
| | | 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. | Procedimiento de Gestión de telecomunicaciones (PR-TI-23)<br><br>Documento de gestión de las telecomunicaciones del Instituto (en construcción). Este documento centraliza las actividades que se realizan para gestionar la conectividad de los usuarios a la red de datos. |
| | A.9.2. GESTIÓN DE ACCESO A USUARIOS. | 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. | Procedimiento Gestionar usuarios tecnológicos (PR-TI-02)<br><br>Formato Solicitud creación usuarios (FO-TI-11)<br><br>Formato Solicitud desactivación servicios tecnología(FO-TI-01) |
| | | 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. | Procedimiento Gestionar usuarios tecnológicos (PR-TI-02) |
| | | 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. | Instructivo Revisión de los Derechos de Acceso de los Usuarios (En construcción). Pretende que los líderes de los procesos institucionales revisen los derechos de acceso a los recursos de TI de personal a su cargo. |

| | | | | | | |
|---|---|---|---|---|---|---|
| A.9. CONTROL DE ACCESO | | 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. | Procedimiento Gestionar usuarios tecnológicos (PR-TI-02) |
| | | 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. | Instructivo Revisión de los Derechos de Acceso de los Usuarios (En construcción). Pretende que los líderes de los procesos institucionales revisen los derechos de acceso a los recursos de TI del personal a su cargo. |
| | | 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. | Procedimiento Gestionar usuarios tecnológicos (PR-TI-02)<br><br>Formato Solicitud desactivación servicios tecnologia(FO-TI-01) |
| | A.9.3. RESPONSABILIDADES DE LOS USUARIOS. | 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. | Procedimiento Gestionar usuarios tecnológicos (PR-TI-02) |
| | A.9.4. CONTROL DE ACCESO A SISTEMAS Y APLICACIONES. | 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. | Instructivo de uso adecuado de las carpetas compartidas (en construcción). Este control pretende establecer normas para la correcta utilización de los recursos compartidos. |
| | | 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. | Procedimiento Gestionar usuarios tecnológicos (PR-TI-02) |
| | | 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 | Procedimiento Gestionar usuarios tecnológicos (PR-TI-02)<br><br>Instructivo de administración del directorio activo (IN-TI-07) |
| | | 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. | Instructivo de uso de herramientas de la mesa de servicios (Control en construcción). Este control pretende identificar y delimitar el uso las herramientas de software especializadas para la prestación de soporte informático. |
| | | 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. | Manual de Gestión de la configuración para proyectos de tecnologías de información (En construcción). Pretende establecer y mantener la integridad sobre los productos que se obtienen a lo largo de la ejecución del ciclo de vida de un proyecto de construcción de software.<br><br>Instructivo de definición y uso de los ambientes de trabajo para desarrollo de software (En construcción). Este documento pretende formalizar las condiciones de trabajo y responsabilidades de uso de los diferentes ambientes de trabajo para la construcción de software. |

| FORMATO<br>DECLARACIÓN DE APLICABILIDAD (DDA) PARA SEGURIDAD DE LA INFORMACIÓN | | | | | | ALCALDÍA MAYOR DE BOGOTÁ D.C.<br>Instituto<br>Desarrollo Urbano |
|---|---|---|---|---|---|---|
| CODIGO<br>FO-TI-27 | PROCESO<br>GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN | | | | VERSIÓN<br>1.0 | |
| A.10. CRIPTOGRAFIA | A.10.1. CONTROLES CRIPTOGRAFICOS | 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. | Resolución 34217 de 2015.<br><br>Instructivo protección de la información digital (en revisión) |
| | | 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. | Resolución 34217 de 2015.<br><br>Instructivo protección de la información digital (en revisión) |
| A.11. SEGURIDAD FÍSICA Y DEL ENTORNO | A.11.1. AREAS SEGURAS. | 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. | Memorando 20155260339143 de Gestión de Recursos Físicos respecto al SGSI |
| | | 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. | Memorando 20155260339143 de Gestión de Recursos Físicos respecto al SGSI<br><br>Manual seguridad y vigilancia (MG-RF-03), numeral 6.5 Procedimientos de Ingreso. |
| | | 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. | Memorando 20155260339143 de Gestión de Recursos Físicos respecto al SGSI |
| | | 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. | Memorando 20155260339143 de Gestión de Recursos Físicos respecto al SGSI |
| | | 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. | Memorando 20155260339143 de Gestión de Recursos Físicos respecto al SGSI |
| | | 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. | Memorando 20155260339143 de Gestión de Recursos Físicos respecto al SGSI |
| | | 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. | Instructivo de Uso adecuado de los recursos de TI (IN-TI-06). |
| | | 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. | Memorando 20155260339143 de Gestión de Recursos Físicos respecto al SGSI |
| | | 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. | Procedimiento de Gestión de telecomunicaciones (PR-TI-23)<br><br>Documento de gestión de las telecomunicaciones del instituto (en construcción). Este documento centraliza las actividades que se realizan para gestionar la conectividad de los usuarios a la red de datos. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | A.11.2. EQUIPOS. | 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. | Mantenimiento preventivo y correctivo (PR-RF-01)<br><br>Contrato de mantenimiento preventivo y bolsa de repuestos para equipos de cómputo. |
| | | 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. | Memorando 20155260339143 de Gestión de Recursos Físicos respecto al SGSI<br><br>Manual seguridad y vigilancia (MG-RF-03) |
| | | 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. | Manual administración del programa de seguros para los bienes del IDU (MG-RF-002)<br><br>Instructivo de Uso adecuado de los dispositivos de almacenamiento de información (IN-TI-05) |
| | | 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. | Instructivo borrado seguro de datos y formateo final de equipos (en construcción). Este documento describe las actividades necesarias para eliminar permanentemente información de los medios de almacenamiento. |
| | | A.11.2.8 | Equipos de Usuario Desatendido | SI | Se adopta este control, puesto que los usuarios deben asegurarse de que a los equipos desatendidos se les da protección adecuada. | Instructivo de administración del directorio activo (IN-TI-07) |
| | | 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. | Resolución 34217 de 2015. |
| | A.12.1. PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES | 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. | Intranet IDU - Documentación SIG |
| | | 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. | Procedimiento Gestión de cambios (PR-TI-08) |
| | | 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. | Procedimiento Gestión de capacidad y disponibilidad (PR-TI-16) |
| | | A.12.1.4 | Separación de las instalaciones 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. | Instructivo de definición y uso de los ambientes de trabajo para desarrollo de software (En construcción). Este documento pretende formalizar las condiciones de trabajo y responsabilidades de uso de los diferentes ambientes de trabajo para la construcción de software. |

| | | | | | | |
|---|---|---|---|---|---|---|
| A.12. SEGURIDAD DE LAS OPERACIONES | A.12.2. PROTECCION CONTRA CODIGO MALICIOSO | 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. | Software de Antivirus Corporativo.<br><br>Instructivo de uso del antivirus (En construcción). Con este control se debe enseñar a los usuarios a usar la aplicación del antivirus. |
| | A.12.3. COPIAS DE RESPALDO | 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. | Procedimiento Generación de copias de seguridad (PR-TI-11)<br><br>Procedimiento Restauración de copias de seguridad (PR-TI-12)<br><br>Formato Solicitud de restauración de backup (FO-TI-185)<br><br>Formato Solicitud realización de backup (FO-TI-218)<br><br>Formato Bitácora de control de restauraciones de copias de seguridad (FO-TI-24) |
| | A.12.4. REGISTRO Y SEGUIMIENTO | 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. | Instructivo Revisión de registros automáticos de la plataforma de TI (en construcción). Este documento permite que se definan aspectos básicos para tener en cuenta en la tarea de revisar los archivos de registro de eventos, de los elementos de tecnología. |
| | | 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. | Instructivo Revisión de registros automáticos de la plataforma de TI (en construcción). Este documento permite que se definan aspectos básicos para tener en cuenta en la tarea de revisar los archivos de registro de eventos, de los elementos de tecnología. |
| | | 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. | Instructivo Revisión de registros automáticos de la plataforma de TI (en construcción). Este documento permite que se definan aspectos básicos para tener en cuenta en la tarea de revisar los archivos de registro de eventos, de los elementos de tecnología. |
| | | 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. | Instructivo de Sincronización de Relojes para la plataforma de TI (en construcción). Mediante este documento se describen las actividades de configuración y seguimiento a la distribución del servicio de fecha y hora (sincronización con la hora legal colombiana) para los elementos de TI administrables.<br><br>Instructivo Revisión de registros automáticos de la plataforma de TI (en construcción). Este documento permite que se definan aspectos básicos para tener en cuenta en la tarea de revisar los archivos de registro de eventos, de los elementos de tecnología. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | A.12.5. CONTROL DE SOFTWARE OPERACIONAL | 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. | Instructivo de Administración del directorio activo. (IN-TI-07)<br><br>Instructivo preparación de un equipo de cómputo para usuario final (En construcción). Describe los pasos para configurar un equipo para un usuario final y las restricciones que se aplican. |
| | A.12.6. GESTION DE LA VULNERABILIDAD TECNICA | 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. | Procedimiento Revisión a la plataforma de tecnología de información (PR-TI-18)<br><br>Implementación de consola centralizada de monitoreo de la plataforma. (Proyecto)<br><br>Revisión externa de las condiciones de la plataforma (Contrato de Ethical Hacking) - Proyecto |
| | | 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. | Instructivo de Administración del Directorio Activo. (IN-TI-07) |
| | A.12.7. CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS DE INFORMACION | 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. | Procedimiento Revisión a la plataforma de tecnología de información (PR-TI-18)<br><br>Auditorías regulares de OCI<br><br>Instructivo Revisión de registros automáticos de la plataforma de TI (en construcción). Este documento permite que se definan aspectos básicos para tener en cuenta en la tarea de revisar los archivos de registro de eventos, de los elementos de tecnología. |
| | A.13.1 GESTION DE LA SEGURIDAD DE LAS REDES | 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. | Procedimiento de Gestión de telecomunicaciones (PR-TI-23)<br><br>Documento de gestión de las telecomunicaciones del Instituto (en construcción). Este documento centraliza las actividades que se realizan para gestionar la conectividad de los usuarios a la red de datos. |
| | | 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. | Procedimiento de Gestión de telecomunicaciones (PR-TI-23)<br><br>Documento de gestión de las telecomunicaciones del instituto (en construcción). Este documento centraliza las actividades que se realizan para gestionar la conectividad de los usuarios a la red de datos. |

| | | | | | | |
|---|---|---|---|---|---|---|
| A.13. SEGURIDAD DE LAS COMUNICACIONES | | 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. | Procedimiento de Gestión de telecomunicaciones (PR-TI-23)<br><br>Documento de gestión de las telecomunicaciones del instituto (en construcción). Este documento centraliza las actividades que se realizan para gestionar la conectividad de los usuarios a la red de datos. |
| | A.13.2 TRANSFERENCIA DE INFORMACION | 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. | Procedimiento de Gestión de telecomunicaciones (PR-TI-23)<br><br>Instructivo de Uso adecuado de los dispositivos de almacenamiento de información (IN-TI-05)<br><br>Documento de gestión de las telecomunicaciones del instituto (en construcción). Este documento centraliza las actividades que se realizan para gestionar la conectividad de los usuarios a la red de datos. |
| | | 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. | Procedimiento de Gestión de telecomunicaciones (PR-TI-23)<br><br>Documento de gestión de las telecomunicaciones del instituto (en construcción). Este documento centraliza las actividades que se realizan para gestionar la conectividad de los usuarios a la red de datos. |
| | | A.13.2.3 | Mensajería Electrónica | SI | Se adopta este control, puesto que se debe proteger adecuadamente la información incluida en la mensajería electrónica. | Instructivo uso del servicio de correo electrónico institucional (En construcción). Regular el uso adecuado del servicio del correo electrónico institucional por parte de los usuarios finales.<br><br>Instructivo de uso de servicios de mensajería instantánea. (En construcción). Definir la reglas de uso del servicio de mensajería instantánea. |
| | | 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. | Formato Acuerdo de confidencialidad con terceros (FO-TI-04)<br><br>Revisión de obligaciones contractuales para que se incluya de oficio una clausula de confidencialidad.<br><br>Revisión de las funciones de los servidores en donde se incluya una clausula de confidencialidad. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | A.14.1. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN. | 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. | Procedimiento Gestión de desarrollo de tecnologías de información (PR-TI-04)<br><br>Procedimiento Gestión de sistemas de información (PR-TI-15)<br><br>Formato Solicitud requerimientos aplicaciones (FO-TI-06) |
| | | 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. | Procedimiento Gestión de desarrollo de tecnologías de información (PR-TI-04)<br><br>Procedimiento de Gestión de telecomunicaciones (PR-TI-23)<br><br>Documento de gestión de las telecomunicaciones del instituto (en construcción). Este documento centraliza las actividades que se realizan para gestionar la conectividad de los usuarios a la red de datos. |
| | | 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. | Procedimiento Gestión de desarrollo de tecnologías de información (PR-TI-04)<br><br>Instructivo de definición y uso de los ambientes de trabajo para desarrollo de software (En construcción). Este documento pretende formalizar las condiciones de trabajo y responsabilidades de uso de los diferentes ambientes de trabajo para la construcción de software.<br><br>Procedimiento de Gestión de telecomunicaciones (PR-TI-23)<br><br>Documento de gestión de las telecomunicaciones del instituto (en construcción). Este documento centraliza las actividades que se realizan para gestionar la conectividad de los usuarios a la red de datos.<br><br>Formato Acuerdo de confidencialidad con terceros (FO-TI-04) y cláusulas en los contratos. Resolución 3421 de 2013. |
| | | 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 | Procedimiento Gestión de desarrollo de tecnologías de información (PR-TI-04)<br><br>Instructivo de definición y uso de los ambientes de trabajo para desarrollo de software (En construcción). Este documento pretende formalizar las condiciones de trabajo y responsabilidades de uso de los diferentes ambientes de trabajo para la construcción de |

| | | | | | | |
|---|---|---|---|---|---|---|
| A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS. | A.14.2. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE. | 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. | Procedimiento Gestión de desarrollo de tecnologías de información (PR-TI-04)<br><br>Procedimiento Gestión de sistemas de información (PR-TI-15)<br><br>Procedimiento Gestión de cambios (PR-TI-08) |
| | | A.14.2.3 | Revisión Técnicas 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. | Procedimiento Gestión de desarrollo de tecnologías de información (PR-TI-04)<br><br>Procedimiento Gestión de sistemas de información (PR-TI-15) |
| | | 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. | Procedimiento Gestión de desarrollo de tecnologías de información (PR-TI-04)<br><br>Procedimiento Gestión de cambios (PR-TI-08)<br><br>Instructivo de definición y uso de los ambientes de trabajo para desarrollo de software (En construcción). Este documento pretende formalizar las condiciones de trabajo y responsabilidades de uso de los diferentes ambientes de trabajo para la construcción de software. |
| | | 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. | Procedimiento Gestión de desarrollo de tecnologías de información (PR-TI-04)<br><br>Procedimiento Gestión de sistemas de información (PR-TI-15) |
| | | 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. | Procedimiento Gestión de desarrollo de tecnologías de información (PR-TI-04)<br><br>Instructivo de definición y uso de los ambientes de trabajo para desarrollo de software (En construcción). Este documento pretende formalizar las condiciones de trabajo y responsabilidades de uso de los diferentes ambientes de trabajo para la construcción de software. |
| | | 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. | Procedimiento Gestión de desarrollo de tecnologías de información (PR-TI-04)<br><br>Procedimiento Gestión de sistemas de información (PR-TI-15)<br><br>Procedimiento Gestión de compras de productos y o servicios de tecnología de información (PR-TI-21) |
| | | 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 | Instructivo para la realización de pruebas a los desarrollos (en construcción). Pretende establecer el diseño para la ejecución de pruebas en los aplicativos de software de misión crítica del Instituto. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 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 | Instructivo para la realización de pruebas a los desarrollos (en construcción). Pretende establecer el diseño para la ejecución de pruebas en los aplicativos de software de misión crítica del Instituto.<br><br>Formato Aceptación de aplicaciones desarrolladas (FO-TI-15)<br><br>Formato Aceptación de pruebas realizadas a las aplicaciones desarrolladas (FO-TI-16)<br><br>Formato Aceptación de manuales para aplicaciones desarrolladas (FO-TI-17)<br><br>Formato Aceptación de código fuente de |
| | A.14.3. DATOS DE PRUEBA. | 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. | Formato Aceptación de pruebas realizadas a las aplicaciones desarrolladas (FO-TI-16)<br><br>Instructivo para la realización de pruebas a los desarrollos (en construcción). Pretende establecer el diseño para la ejecución de pruebas en los aplicativos de software de misión crítica del Instituto |
| A.15. RELACIONES CON LOS PROVEEDORES | A.15.1. SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES. | 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. | Resolución 34217 de 2015.<br><br>Procedimiento Gestión de compras de productos y o servicios de tecnología de información (PR-TI-21) |
| | | 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. | Procedimiento Gestión de compras de productos y o servicios de tecnología de información (PR-TI-21) |
| | | 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 | Procedimiento Gestión de compras de productos y o servicios de tecnología de información (PR-TI-21) |
| | A.15.2. GESTIÓN DE LA PRESTACIÓN DE LOS SERVICIOS DE PROVEEDORES. | 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. | Procedimiento Gestión de compras de productos y o servicios de tecnología de información (PR-TI-21) |
| | | 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. | Procedimiento Gestión de compras de productos y o servicios de tecnología de información (PR-TI-21)<br><br>Procedimiento Gestión de cambios (PR-TI-08) |

| | | | | | | |
|---|---|---|---|---|---|---|
| A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | A.16.1. GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN. | 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. | Procedimiento de Gestión de Incidentes de Seguridad de la Información (En publicación) |
| | | 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. | Procedimiento de Gestión de Incidentes de Seguridad de la Información (En publicación) |
| | | 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. | Procedimiento de Gestión de Incidentes de Seguridad de la Información (En publicación) |
| | | 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. | Procedimiento de Gestión de Incidentes de Seguridad de la Información (En publicación) |
| | | 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. | Procedimiento de Gestión de Incidentes de Seguridad de la Información (En publicación) |
| | | 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. | Procedimiento de Gestión de Incidentes de Seguridad de la Información (En publicación) |
| | | 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. | Procedimiento de Gestión de Incidentes de Seguridad de la Información (En publicación) |
| A.17.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACION | A.17.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN | 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. | Documento Plan de continuidad de negocios para los servicios de TI (En construcción) |
| | | 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. | Documento Plan de continuidad de negocios para los servicios de TI (En construcción) |
| | | 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. | Documento Plan de continuidad de negocios para los servicios de TI (En construcción) |
| | A.17.2. REDUNDANCIAS | 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. | Documento Plan de continuidad de negocios para los servicios de TI (En construcción) |

| FORMATO<br>DECLARACIÓN DE APLICABILIDAD (DDA) PARA SEGURIDAD DE LA INFORMACIÓN | | | | | | ALCALDÍA MAYOR DE BOGOTÁ D.C.<br>Desarrollo Urbano |
|---|---|---|---|---|---|---|
| CODIGO<br>FO-TI-27 | PROCESO<br>GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN | | | | VERSIÓN<br>1.0 | |
| A.18. CUMPLIMIENTO | A.18.1. CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES | 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. | Formato Actualización y evaluación del normograma institucional (FO-GL-02), diligenciado |
| | | 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. | Procedimiento Gestión de licenciamiento de SW (PR-TI-14)<br><br>Formato Cesión derechos patrimoniales (FO-TI-02)<br><br>Formato Inventario aplicaciones (FO-TI-25) |
| | | 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. | Instructivo de revisión de registros automáticos de la plataforma de TI (En construcción). Este documento permite que se definan aspectos básicos para tener en cuenta en la tarea de revisar los archivos de registro de eventos, de los elementos de tecnología. |
| | | 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. | Política de tratamiento de protección de datos personales de los titulares IDU - Circular 19 del 26-12-2013<br><br>Documento Condiciones de uso y políticas de privacidad de la pagina web del IDU (DU-TI-03) |
| | | 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. | Instructivo protección de la información digital (en revisión) |
| | A.18.2. REVISIONES DE SEGURIDAD DE LA INFORMACION | 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. | Procedimiento Revisión a la plataforma de tecnología de Información (PR-TI-18)<br><br>Procedimiento Evaluación independiente y auditorías internas (PR-EC-01) |
| | | 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. | Procedimiento de Seguimiento a la Gestión de TI (en publicación) |
| | | 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. | Procedimiento de Seguimiento a la Gestión de TI (en publicación) |

| | |
|---|---|
| Total controles implementados | 114 |
| Total controles SIN implementar | 0 |

Revisado por: _____ Fecha de Revisión: _____

Profesional Delegado de la SGGC.