No del Control	Objetivo de control	Control	SI/NO	Declaración de Aplicabilidad	Aplicación		
					Nacional	Regional	Zonal
A.5	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**						
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**						
A.5.1.1	Políticas para la seguridad de la información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y las partes externas pertinentes.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información . - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información.	X	X	X
A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	SI	- PL10.GTI. Plan de Seguridad y Privacidad de la Información - Revisión por la Dirección - Resolución 11980 del 30/12/2019 "Por la cual se adopta el Modelo de Planeación y Sistema Integrado de Gestión del ICBF." - Resolución 6659 de 15/12/2020 "Por el cual se modifica el Modelo de Planeacióny el Sistema Integrado de Gestión" La Política de Seguridad de la Información del ICBF es revisada en intervalos planificados por la Dirección de Información y Tecnológia.	X		
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**						
A.6.1	**Organización interna**						
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Se debe definir y asignar todas las responsabilidades de la seguridad de la información.	SI	- Resolución 11980 del 30/12/2019 "Por la cual se adopta el Modelo de Planeación y Sistema Integrado de Gestión del ICBF." - Resolución 6659 de 15/12/2020 "Por el cual se modifica el Modelo de Planeacióny el Sistema Integrado de Gestión" - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información.	X	X	X
A.6.1.2	Separación de deberes	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.	SI	- Resolución 11980 del 30/12/2019 "Por la cual se adopta el Modelo de Planeación y Sistema Integrado de Gestión del ICBF." - Resolución 6659 de 15/12/2020 "Por el cual se modifica el Modelo de Planeacióny el Sistema Integrado de Gestión" - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - G9.GTI Guía para Control de Accesos a Centros de Cableado y Data Center - F2.G10.GTI Formato de Identificación de Áreas Seguras a Nivel Nacional - P6.GTI Procedimiento para el desarrollo y mantenimiento de los sistemas de información (solo aplica para la Sede de la Dirección General).	X	X	X
A.6.1.3	Contacto con las autoridades	Se deben tener contactos apropiados con las autoridades pertinentes	SI	Se realiza contacto CSIRT Gobierno, Policía Nacional y la Fiscalía dependiendo del incidente presentado. Contacto con el grupo de respuestas a emergencias cibernéticas de colombia COLCERT y con el Comando Conjunto Cibernético, el cual se desempeña como unidad élite en aspectos relacionados con la Ciberseguridad y Ciberdefensa. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - A1.P21.DE Anexo Identificación y Actualización de Necesidades y Expectativas de las Partes Interesadas. - PL6.GTI. Plan de cambio y cultura de seguridad y privacidad de la información	X	X	X
A.6.1.4	Contacto con grupos de interés especial	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	SI	Se tiene contacto con grupos de interés especial: - Se participa en la Reunión de Infraestructura Critica, Riesgo operacional y Ciberdefensa. Participación en talleres organizados por MINTIC en los diferentes temas enmarcados frente a temas de seguridad de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información.	X		
A.6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información . - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - G7.ABS. Guía para la Adquisición de Bienes y Servicios de Calidad.	X	X	X
A.6.2	**Dispositivos Móviles y teletrabajo**						
A.6.2.1	Política para dispositivos móviles	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - F1.P2.GTI Formato de solicitud de servicios de tecnología. - F9.P2.GTI Formato verificación de equipos Personales. - G22.GTI Guía para Uso de Dispositivos Personales BYOD.	X	X	X
A.6.2.2	Teletrabajo	Se deben 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 teletrabajo.	SI	- Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones - Resolucion 7600 de 2016 "Por la cual se adopta la modalidad de Teletrabajo Suplementario a nivel nacional en el Instituto Colombiano de Bienestar Familiar Cecilia de la Fuente de Lleras y se hace una delegación". - Resolución 4594 del 15 de junio de 2017 "Por la cual se modifica la Resolución 7600 de 2016" . - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - G22.GTI Guía para Uso de Dispositivos Personales BYOD. - F1.P2.GTI. Formato de solicitud de servicios de tecnología. - IT1.P2.GTI . Instructivo para gestión de solicitudes de VPN. - F9.P2.GTI Formato Verificación de Equipos Personales. - Circular Externa 0027 del 12 de abril 2019	X		
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**						
A.7.1	**Antes de asumir el empleo**						
A.7.1.1	Selección	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 de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información . - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. Numeral 6 Seguridad del Recurso Humano. Para los servidores públicos: - P21.GTH Procedimiento Provision de Empleos - F3.P21.GTH. Formato Relación de Documentos para Nombramiento y Posesión Para los contratistas: - P5.ABS Procedimiento para la Solicitud e Inicio del Proceso de Selección y Contratación - F1.P5.ABS. Formato Lista de Chequeo Contratación Directa.	X	X	X
A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	SI	- Resolución 2677 de 02 de mayo de 2022, Por la cual se modifica el Manual Específico y Competencias Laborales del Instituto Colombiano de Bienestar Familiar, adoptado mediante Resolución 1818 de 2019 y modificado por las resoluciones 7444 de 2019, 4122 de 2020 y 4451 de 2020 -Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. Numeral 6 Seguridad del Recurso Humano. **Para los funcionarios públicos:** - Ley 734 de 2002 Código Disciplinario Único, artículo 34 Deberes. Numeral 4 " Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos" y Numeral 5 " Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos". - P21.GTH Procedimiento Provisión de Empleos - F5.P21.GTH Formato Autorización de Tratamiento de Datos Personales. - F12.P21.GTH Formato Compromiso de Confidencialidad de Información. **Para los contratista:** - P2.ABS Procedimiento Contrato para la Prestación de Servicios y de Apoyo a la Gestión - F7.P2.ABS Formato Compromiso de Confidencialidad de Información - F6.P2.ABS Formato Autorización de Tratamiento de Datos Personales Contratistas - F1.P4.RC Formato Compromiso de Confidencialidad y No Divulgación de la Información.	X	X	X
A.7.2	**Durante la ejecución del empleo**						
A.7.2.1	Responsabilidades de la dirección	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.	SI	- Resolución 11980 de 2019, Por la cual se adopta el Modelo de Planeación y Sistema Integrado de Gestión del ICBF - Resolución 6659 del 15/12/2020 Por la cual se modifica el modelo de Planeación y Sistema Integrado de Gestión. '- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información . - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. Numeral 6 Seguridad del Recurso Humano.	X	X	X

No del Control	Objetivo de control	Control	SI/NO	Declaración de Aplicabilidad	Aplicación		
					Nacional	Regional	Zonal
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	SI	- El ICBF cuenta con un módulo SGSI inmerso en el curso virtual SIGE. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - PL6.GTI Plan de Cambio y Cultura de Seguridad y Privacidad de la Información. - P10.GTH Procedimiento Inducción y Reinducción. - PIC P7.GTH Procedimiento para la Formulación y Ejecución del Plan Institucional de Capacitación. '- A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. Numeral 6 Seguridad del Recurso Humano. -PL5.GTI Plan de Uso y Apropiación de TI.	X	X	X
A.7.2.3	Proceso disciplinario	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.	SI	Control Interno Disciplinario investiga acciones de los empleados que hayan cometido violación a la seguridad de la información. '- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P3.GTH Procedimiento Proceso Disciplinario Verbal. - P2.GTH. Procedimiento Proceso Disciplinario Ordinario.	X	X	X
A.7.3	**Terminación y cambio de empleo**						
A.7.3.1	Terminación o cambio de responsabilidades de empleo	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.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información . - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. **Para funcionarios Públicos:** - P30.GTH Procedimiento para Entrega de Cargo por Parte de Servidores Públicos - F1.P30.GTH Formato Lista de Chequeo Entrega del Cargo - F2.P30.GTH Formato Informe Final de Entrega de Cargo - F3.P30.GTH Formato Entrevista de Retiro **Para Contratistas:** - P25.ABS Procedimiento Finalización de contrato de prestación de servicios profesionales y de apoyo a la gestión. - F1.P25.ABS Formato lista de chequeo finalización de contrato de prestación de servicios profesionales y de apoyo a la gestión.	X	X	X
A.8	**GESTIÓN DE ACTIVOS**						
A.8.1	**Responsabilidad por los activos**						
A.8.1.1	Inventario de activos	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.	SI	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - G10.GTI Guía para el Desarrollo de Inventario y Clasificación de Activos. - F1.G10.GTI Formato para levantamiento de activos de información. - F2.G10.GTI Formato de Identificación de Áreas Seguras a Nivel Nacional. - G11.GTI Guía para la Clasificación y Etiquetado de la Información. - Herramienta automatizada para el levantamiento de activos de información.	X	X	X
A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario y custodio.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - G10.GTI. Guía para el Desarrollo de Inventario y Clasificación de Activos. - F1.G10.GTI Formato para levantamiento de activos de información. - Herramienta para el levantamiento de activos de información,	X	X	X
A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - G10.GTI Guía para el Desarrollo de Inventario y Clasificación de Activos. - PL6.GTI. Plan de cambio y cultura de seguridad y privacidad de la información -PL5.GTI Plan de Uso y Apropiación de TI - F1.P2.GTI Formato solicitud de servicios de tecnología. - P2.GTI Procedimiento de gestión de solicitudes de tecnología. - F2.G10.GTI Formato de Identificación de Áreas Seguras a Nivel Nacional V2 - Herramienta automatizada para el levantamiento de activos de información - G22.GTI Guía para Uso de Dispositivos Personales BYOD - F9.P2.GTI Formato Verificación de Equipos Personales -G11.GTI Guía para la Clasificación y Etiquetado de la Información -G23.GTI Guía Metodológica para la Anonimización de Registros -IT1.G12.GTI Instructivo Nomenclatura de Equipos -PL11.GTI Plan de Transformación Digital Visión Digital y Hoja de Ruta 2020 - 2022 - Procuedimiento Control Préstamo y Devolución de Expedientes -F1. P21.SA Formato Control Préstamo y Devolución de Expedientes	X	X	X
A.8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se entregan a su cargo, al terminar su empleo, contrato o acuerdo.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - G2.SA Guia Gestion de Bienes - F2.G2.SA Formato Devolución de Bienes al Almacén - IT3.P2.GTI Instructivo para gestionar solicitudes de borrado de información de los dispositivos de cómputo. - IT8.P2.GTI Instructivo Borrado y Destrucción de Soportes de Almacenamiento. **Para servidores públicos:** - P30.GTH Procedimiento para Entrega de Cargo por Parte de Servidores Públicos y Contratistas. - F1.P30.GTH Formato Lista de Chequeo Entrega del Cargo. **Para usuarios de partes externas y/o contratistas:** - G7.ABS Guía para la Adquisicion de Bienes y Servicios de Calidad desde el proceso de Adquisición de Bienes y Servicios. - P21.ABS Procedimiento para Terminación y Liquidación Anticipada de Contrato de Prestación de Servicios y Apoyo a la Gestión. - F1.P25.ABS Formato lista de chequeo finalización de contrato de prestación de servicios profesionales y de apoyo a la gestión.	X	X	X
A.8.2	**Clasificación de la información**						
A.8.2.1	Clasificación de la información	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o modificación no autorizada.	SI	La Dirección de Servicio y Atención, y la Oficina de Asesoría Jurídica, revisan el levantamiento de activos para dar cumplimiento a la ley de transparencia 1712 de 2014. - El ICBF debe conocer y clasificar los activos de información. -Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - Indice de Información Clasificada y Reservada. - G10.GTI Guía para el Desarrollo de Inventario y Clasificación de Activos. - G11.GTI Guía para la Clasificación y Etiquetado de la Información.	X	X	X
A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de la información adoptado por la organización.	SI	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - G11.GTI Guía para la Clasificación y Etiquetado de la Información.	X	X	X
A.8.2.3	Manejo de activos	Se deben desarrollar e implementar procedimientos para el manejo de activos de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI	Se tiene en cuenta en el levantamiento de activos; su clasificación está basada en la afectación a la triada de la información y al criterio de privacidad de los datos personales. El ICBF cuenta con la documentación que especifica los esquemas para el manejo de permisos en los repositorios, los cuales se encuentran definidos en la documentación del Servicio de Almacenamiento. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - G10.GTI Guía para el Desarrollo de Inventario y Clasificación de Activos. - G11.GTI Guía para la Clasificación y Etiquetado de la Información - IT3.P2.GTI Instructivo para gestionar solicitudes de borrado de información de los dispositivos de cómputo. -IT8.P2.GTI Instructivo Borrado y Destrucción de Soportes de Almacenamiento.	X	X	X

No del Control	Objetivo de control	Control	SI/NO	Declaración de Aplicabilidad	Aplicación		
					Nacional	Regional	Zonal
A.8.3	**Manejo de medios**						
A.8.3.1	Gestión de medios removibles	Se deben implementar procedimientos para la gestión de medios removibles de acuerdo con el esquema de clasificación adoptado por la organización.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - P9.GTI Procedimiento para el manejo de medios removibles. - IT1.P9.GTI Instructivo para cifrado de información.	X	X	X
A.8.3.2	Disposición de los medios	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - G2.SA Guía gestión de bienes. - F2.G2.SA Devolución de Bienes al Almacén. - P9.GTI Procedimiento para el manejo de medios removibles. - IT3.P2.GTI Instructivo para gestionar solicitudes de borrado de información de los dispositivos de cómputo. - IT8.P2.GTI Instructivo Borrado y Destrucción de Soportes de Almacenamiento. - P57.SA Procedimiento manejo residuos especiales.	X	X	X
A.8.3.3	Transferencia de medios físicos	Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - G3.SA Guía para la Gestión Documental del ICBF - P32.SA ProcedimientoTransferencias Documentales Primarias. - P31.SA Procedimiento Transferencias Documentales Secundarias a cargo del proceso de Servicios Administrativos. - PL37.SA Plan de Transferencias Documentales Secundarias. - PT4.SA Protocolo de Transporte para Transferencias Primarias y Secundarias. Con el proveedor encargado del transporte, almacenamiento y custodia de los activos de información se fijan las condiciones de seguridad que permiten la debida protección de dichos elementos.	X	X	X
A.9	**CONTROL DE ACCESOS**						
A.9.1	**Requisitos del negocio para control de accesos**						
A.9.1.1	Política de control de acceso	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.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P2.GTI Procedimiento de gestión de solicitudes de tecnología. - F1.P2.GTI Formato solicitud de servicios de tecnología. - G9.GTI Guía para el Control de Accesos a Centros de Cableado y Data Center.	X	X	X
A.9.1.2	Acceso a redes y a servicios en red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	SI	'- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P2.GTI Procedimiento de gestión de solicitudes de tecnología. - F1.P2.GTI Formato solicitud de servicios de tecnología. - F9.P2.GTI Formato Verificación de Equipos Personales. - G22.GTI Guía para Uso de Dispositivos Personales BYOD. - G27.GTI Guía Politicas Navegación.	X	X	X
A.9.2	**Gestión de acceso de usuarios**						
A.9.2.1	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P2. GTI Procedimiento Gestión de Solicitudes de Tecnología. - F1.P2.GTI Formato solicitud de servicios de tecnología. - P4.GTH Procedimiento para la Activación, Actualización y Desactivación de las Cuentas de Usuario Institucionales. - F1.P4.GTH Formato Informe Bimestral Directorio Activo.	X	X	X
A.9.2.2	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P2.GTI Procedimiento de gestión de solicitudes de tecnología. - F1.P2.GTI Formato solicitud de servicios de tecnología. - F8.P2.GTI Formato de Gestión de Usuarios Sistemas de Información. - P4.GTH Procedimiento para la Activación, Actualización y Desactivación de las Cuentas de Usuario Institucionales. - F1.P4.GTH Formato Informe Bimestral Directorio Activo. - G27.GTI Guía Politicas Navegación.	X	X	X
A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P2. GTI Procedimiento Gestión de Solicitudes de Tecnología. - F1.P2.GTI Formato de Solicitud Servicios de Tecnología. - P4.GTH Procedimiento para la Activación, Actualización y Desactivación de las Cuentas de Usuario Institucionales. - F1.P4.GTH Formato Informe Bimestral Directorio Activo. -G27.GTI Guía Politicas Navegación.	X	X	X
A.9.2.4	Gestión de información de autenticación secreta de usuarios	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. Desde el Directorio Activo se establece que se debe cambiar la contraseña en el primer inicio de sesión y cada **30** días o cuando lo establezca la Dirección de Información y Tecnología. - La política se aplica desde la Dirección de Información y Tecnología, y se despliega de forma automática a todos los usuarios a nivel país. Estos últimos, son quienes tienen la responsabilidad de asignar su contraseña segura en la periodicidad establecida mediante el Directorio Activo.	X	X	X
A.9.2.5	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	SI	Desde el Directorio Activo se revisan los derechos de acceso en caso de que haya finalización de contrato o empleo; o cambios de rol dentro del ICBF. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P2.GTI Procedimiento de gestión de solicitudes de tecnología. - F1.P2.GTI Formato solicitud de servicios de tecnología. - F8.P2.GTI Formato de Gestión de Usuarios Sistemas de Información.	X	X	X
A.9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de 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.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P2.GTI Procedimiento de Gestión de Solicitudes de Tecnología. - F1.P2.GTI Formato de Solicitud Servicios de Tecnología - P4.GTH Procedimiento para la Activación, Actualización y Desactivación de las Cuentas de Usuario Institucionales. - F1.P2.GTI Formato solicitud de servicios de tecnología - F8.P2.GTI Formato de Gestión de Usuarios Sistemas de Información	X	X	X
A.9.3	**Responsabilidades de los usuarios**						
A.9.3.1	Uso de información de autenticación secreta	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	SI	La Dirección de Información y Tecnológia a través del Eje de Seguridad de la información sensibiliza y apropia a los funcionarios y colaboradores regularmente en temas de seguridad de la información y buenas prácticas. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - PL6.GTI Plan de Cambio y Cultura de Seguridad y Privacidad de la Información - P2.GTI Procedimiento de gestión de solicitudes de tecnología	X	X	X

No del Control	Objetivo de control	Control	SI/NO	Declaración de Aplicabilidad	Aplicación		
					Nacional	Regional	Zonal
A.9.4				**Control de acceso a sistemas y aplicaciones**			
A.9.4.1	Restricción de acceso a la información	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.	SI	A una cuenta de usuario se le asigna permisos o privilegios para acceder a los sistemas de información y desarrollar actividades dentro de los mismos. Los privilegios delimitan las actividades que el usuario puede desarrollar sobre los sistemas de información. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P2.GTI Procedimiento de gestión de solicitudes de tecnología - F1.P2.GTI Formato solicitud de servicios de tecnología - F8.P2.GTI Formato de Gestión de Usuarios Sistemas de Información.	X	X	X
A.9.4.2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	SI	Se hace a través del Directorio Activo, y la política de control de acceso se maneja desde cada aplicativo. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P2.GTI Procedimiento de Gestión de Solicitudes de Tecnología. - F1.P2.GTI Formato de Solicitud Servicios de Tecnología - F8.P2.GTI Formato de Gestión de Usuarios Sistemas de Información. - Las buenas prácticas de control de acceso deben aplicarlas a nivel regional.	X	X	X
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	SI	Desde el Directorio Activo se establecen acciones para asegurar la complejidad de las contraseñas y se establece un tiempo de **XX** días o el tiempo que establezca la Dirección de Información y Tecnología para su cambio. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información.. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - La política se aplica desde la Dirección de Información y Tecnología, y se despliega de forma automática a todos los usuarios a nivel país. Estos últimos, son quienes tienen la responsabilidad de asignar su contraseña segura en la periodicidad establecida mediante el Directorio Activo	X	X	X
A.9.4.4	Uso de programas utilitarios privilegiados	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.	SI	Desde el Directorio activo se asignan privilegios de administrador a las personas que pueden instalar y hacer uso de programas utilitarios. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información.	X	X	X
A.9.4.5	Control de acceso a códigos fuente de programas	Se debe registrar el acceso a los códigos fuente de los programas.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P6.GTI Procedimiento para desarrollo y mantenimiento de sistemas de información. - G1.GTI Guía de Estándares de Desarrollo y Arquitectura de Sistemas de Información -G21.GTI Guía de Arquitectura de Referencia de Interoperabilidad -F13.P6.GTI Formato Lista de Chequeo Codigo Fuente	X		
A.10				**CRIPTOGRAFIA**			
A.10.1				**Controles criptográficos**			
A.10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - G1.GTI Guía de Estándares de Desarrollo y Arquitectura de Sistemas de Información - G1.P17.GF Guía de políticas y seguridad para el manejo y control de recursos financieros administrados ICBF. - F1.P2.GTI Formato solicitud de servicios de tecnología. - B69IT1.P9.GTI Instructivo para cifrado de información.	X	X	X
A.10.1.2	Gestión de llaves	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante su ciclo de vida.	SI	Para la transferencia electrónica se tienen en cuenta aspectos de seguridad sobre la información y realización de pagos del ICBF. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - G1.GTI Guía de Estándares de Desarrollo y Arquitectura de Sistemas de Información. - IT1.P9.GTI Instructivo para cifrado de información. - G1.P17.GF Guía de Politicas y Seguridad para el Manejo y Control de Recursos Financieros Administrados ICBF.	X		
A.11				**SEGURIDAD FÍSICA Y DEL ENTORNO**			
A.11.1				**Áreas seguras**			
A.11.1.1	Perímetro de seguridad física	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.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - F2.G10.GTI Formato de Identificación de Áreas Seguras a Nivel Nacional - G9.GTI Guía para Control de Accesos a Centros de Cableado y Data Center - F1.G9.GTI Formato bitácora de ingreso	X	X	X
A.11.1.2	Control de accesos físicos	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite acceso a personal autorizado.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - G9.GTI Guía para Control de Accesos a Centros de Cableado y Data Center. - F1.G9.GTI Formato bitácora de ingreso. - Contrato de Servicio de Vigilancia Vigente.	X	X	X
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P50.SA Procedimiento Seguridad y Vigilancia Privada - F1.G9.GTI Formato bitácora de ingreso. - G9.GTI Guía para Control de Accesos a Centros de Cableado y Data Center	X	X	X
A.11.1.4	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P29.SA Procedimiento para la Gestión Ambiental. - P22.SA Procedimiento Aspectos e Impactos Ambientales y Otros Requisitos. - PT3.SA Protocolo Manejo y Atención de Emergencias Ambientales Relacionadas con Derrames. - F4.PL36.SA Formato Monitoreo y Control de Condiciones Ambientales. - P9.GTH Procedimiento para la elaboración de planes de emergencias y contingencias.	X	X	X
A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P50.SA Procedimiento Seguridad y Vigilancia Privada. - F2.G10.GTI Áreas Seguras a Nivel Nacional	X	X	X
A.11.1.6	Áreas de despacho y carga	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información.	X	X	
A.11.2				**Equipos**			
A.11.2.1	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	SI	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - IT1.P9.GTI Instructivo para cifrado de información -F3.G9.GTI Formato Monitoreo de Temperatura	X	X	X
A.11.2.2	Servicios de suministro	Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	SI	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - PT1.SA Protocolo Cargue Combustible Plantas Eléctricas	X	X	X

No del Control	Objetivo de control	Control	SI/NO	Declaración de Aplicabilidad	Aplicación		
					Nacional	Regional	Zonal
A.11.2.3	Seguridad del cableado	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.	SI	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. -F3.G9.GTI Formato Monitoreo de Temperatura	X	X	X
A.11.2.4	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	SI	Existen actas de mantenimiento de equipos realizados por los ingenieros regionales y la UT. -Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - G12.GTI Guía para el Mantenimiento Preventivo de Equipos - F1.G12.GTI Formato Acta Mantenimiento Preventivo Equipos Portatiles y de Escritorio. - Anexo Estándar de Nombramiento de Estaciones - F2.G12.GTI Formato relación mantenimientos preventivos impresoras y scanner - F3.G12.GTI Formato acta mantenimientos preventivos de switches - F4.G12.GTI Formato lista de chequeo mantenimiento de Red LAN - F5.G12.GTI Formato Acta Mantenimientos Preventivos de Telefonia IP	X	X	X
A.11.2.5	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	SI	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - G2.SA Guia gestión de bienes. - F3.G2.SA Formato traslado elementos devolutivos. - Minuta de vigilancia para la salida de los equipos.	X	X	X
A.11.2.6	Seguridad de activos y equipos fuera de la oficina	Se deben aplicar medidas de seguridad a los activos que se encuentran instalaciones fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - Resolución 4594 del 15 de junio de 2017 "Por la cual se modifica la Resolución 7600 de 2016" - Resolución 7600 de 2016 "Por la cual se adopta la modalidad de Teletrabajo Suplementario a nivel nacional en el Instituto Colombiano de Bienestar Familiar Cecilia de la Fuente de Lleras y se hace una delegación" - Memorando 9/12/2021 Medidas Salida de Bienes Muebles devolutivos instalaciones ICBF. - Memorando 9/12/2021 Responsabilidad del manejo, cuidado y custodia de los bienes muebles propiedad del ICBF, a cargo de los colaboradores del ICBF. - IT1.P2.GTI Instructivo para Gestión de Solicitudes de VPN.	X	X	X
A.11.2.7	Disposición segura o reutilización de equipos	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.	SI	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - Anexo 4 Manual de Políticas de Seguridad de la Información A4.MS.DE. - G2.SA Guia Gestion de Bienes - F2.G2.SA Formato Devolución de Bienes al Almacén. - F3.G2.SA FormatoTraslado Elementos Devolutivos - IT3.P2.GTI Instructivo para Gestionar Solicitudes de Borrado de Información de los Dispositivos de Cómputo -IT8.P2.GTI Instructivo Borrado y Destrucción de Soportes de Almacenamiento - G12.GTI Guía para el Mantenimiento Preventivo de Equipos - F1.G12.GTI Formato acta mantenimiento preventivo equipos portátiles y de escritorio - F2.G12.GTI Formato relación mantenimientos preventivos impresoras y scanner - F3.G12.GTI Formato acta mantenimientos preventivos de switches - P2.GTI Procedimiento de Gestión de Solicitudes de Tecnología - F3.P2.GTI Formato diagnóstico de hardware.	X	X	X
A.11.2.8	Equipos de usuario desatendido	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	SI	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información.	X	X	X
A.11.2.9	Políticas de escritorio limpio y pantalla limpia	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.	SI	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información.	X	X	X
A.12	**SEGURIDAD DE LAS OPERACIONES**						
A.12.1	**Procedimientos operacionales y responsabilidades**						
A.12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	SI	Se encuentra publicado en la página Web e Intranet todos los procedimientos operativos de cada proceso del ICBF, para la Seguridad de la Información, los procedimientos correspondientes al Proceso de Gestión de la Tecnología e Información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P1.GTI Procedimiento seguimiento, control y atención de vulnerabilidades técnicas. - P2.GTI. Procedimiento de gestión de solicitudes de tecnología. - P3.GTI Procedimiento gestión de cambios de emergencia de tecnologías de la información. (Solo a la DIT) - P4.GTI Procedimiento gestión de cambios de tecnologías de la información. (Solo a la DIT) - P5.GTI Procedimiento Gestión De Incidentes de Seguridad Digital. - P6.GTI Procedimiento para desarrollo y mantenimiento de sistema de información. (Solo a la DIT) - P7.GTI Procedimiento de gestión de problemas de tecnología (Solo a la DIT) - P8.GTI Procedimiento Gestión de Incidentes de Tecnologías de la Información v8 - P9.GTI Procedimiento para el manejo de medios removibles - P11.GTI Procedimiento de Gestión de Eventos y Alertas (Solo a la DIT) - P12.GTI Procedimiento Interno_Registro Bases Datos Datos Personales (Solo a la Sede de la Dirección General) - P20.GTI Procedimiento Gestión de Usuarios SIIF Nación II v4	X	X	X
A.12.1.2	Gestión de cambios	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	SI	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - P3.GTI Procedimiento gestión de cambios de emergencia de tecnologías de la información. - P4.GTI Procedimiento gestión de cambios de tecnologías de la información.	X		
A.12.1.3	Gestión de capacidad	Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	SI	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - PL1.GTI Plan de Gestión de Capacidad.	X		
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operación	Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	SI	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información - G3.GTI Guía de Estándares de Especificación de Requerimientos	X		
A.12.2	**Protección contra códigos maliciosos**						
A.12.2.1	Controles contra códigos maliciosos	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.	SI	Se cuenta con el Servicio de SOC tercerizado con un proveedor y se tienen herramientas de seguridad perimetral como antivirus, firewall, filtros de contenido, filtro de correos, endpoint, WAF, SIEM. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - PL6.GTI Plan de Cambio y Cultura de Seguridad y Privacidad de la Información - Informe del agente y versión de la firma de virus -IT2.P2.GTI Instructivo para Gestión de Solicitudes de Permiso de Firewall	X	X	X
A.12.3	**Proteger contra la pérdida de datos**						
A.12.3.1	Respaldo de la información	Se deben hacer copias de respaldo de información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	SI	Se cuenta con procedimientos, guías e instructivos referentes al respaldo y restauración de información. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - P2.GTI Procedimiento de gestión de solicitudes de tecnología - F4.P2.GTI Formato solicitud de respaldo para equipos de centros de cómputo - F5.P2.GTI Formato solicitud restauración de copias de seguridad - G8.GTI Guía respaldo y restauración de copias de seguridad - IT4.P2.GTI Instructivo para gestionar solicitudes de restauración de copias - IT5.P2.GTI Instructivo para gestión de solicitudes de copias de seguridad. - G15.GTI Guía Integral para el Servicio de Almacenamiento. - F2.P2.GTI Formato Acta de Entrega de Copia de Información.	X	X	X

No del Control	Objetivo de control	Control	SI/NO	Declaración de Aplicabilidad	Aplicación		
					Nacional	Regional	Zonal
A.12.4	**Registro y seguimiento**						
A.12.4.1	Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros a cerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información	SI	Se tiene Servicio de SOC contratado con el proveedor de servicios. -Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - P11.GTI Procedimiento de Gestión de Eventos y Alertas. - P5.GTI Procedimiento Gestión de Incidentes de Seguridad Digital - F1.P11.GTI Formato Bitacora Eventos SOC	X		
A.12.4.2	Protección de la información de registro	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado	SI	Se cuenta con el Servicio de SOC tercerizado con un proveedor y se tienen herramientas de seguridad que con base en el análisis apoyan la detección de afectación a la seguridad de la información. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - P11.GTI Procedimiento De Gestion De Eventos y Alertas.	X		
A.12.4.3	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	SI	Se cuenta con el Servicio de SOC tercerizado con un proveedor y se tienen herramientas de seguridad, como el correlacionador de eventos que con base en el análisis apoyan la detección de afectación a la seguridad de la información. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - P11.GTI Procedimiento de Gestion de Eventos y Alertas	X		
A.12.4.4	Sincronización de reloj	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	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información.	X	X	X
A.12.5	**Control de software operacional**						
A.12.5.1	Instalación de software en sistemas operativos.	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P2.GTI Procedimiento de Gestión de Solicitudes de Tecnología. - F1.P2.GT Formato de Solicitud de Servicios de Tecnología.	X	X	X
A.12.6	**Gestión de la vulnerabilidad técnica**						
A.12.6.1	Gestión de las vulnerabilidades técnicas	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 estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	SI	Se elabora y ejecuta Test de Penetración, y se elabora Informe de resultados. -Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - P1.GTI Procedimiento seguimiento, control y atención de vulnerabilidades técnicas. - F1.P1.GTI Formato registro de pruebas y remediación de vulnerabilidades -G14.GTI Guía para el Desarrollo de Pruebas de Penetración	X		
A.12.6.2	Restricciones sobre la instalación de software	Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información	X	X	X
A.12.7	**Consideraciones sobre auditorías de sistemas de información**						
A.12.7.1	Controles de auditorías de sistemas de información	Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información	X		
A.13	**SEGURIDAD DE LAS COMUNICACIONES**						
A.13.1	**Gestión de la seguridad de las redes**						
A.13.1.1	Controles de redes	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	SI	Se cuenta con una plataforma tecnológica capaz de proteger y soportar los sistemas y aplicaciones. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información -IT1.P2.GTI Instructivo para Gestión de Solicitudes de VPN	X	X	
A.13.1.2	Seguridad de los servicios de red	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	SI	Se cuenta con informes mensuales de los servicios firewall, WAN y LAN realizados por los proveedores. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información	X		
A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	SI	Se cuenta con segmentación de redes en el ICBF. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información	X	X	X
A.13.2	**Transferencia de información**						
A.13.2.1	Políticas y procedimientos de transferencia de información	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.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - IT1.P9.GTI Instructivo para cifrado de información - G11.GTI Guía para el Etiquetado y Clasificación de la Información - G5. GTI Guía de recolección de evidencias de elementos informáticos - Política de tratamiento de datos personales - P14.GTI Procedimiento intercambio o suministro de información - Tablas de retención documental	X	X	X
A.13.2.2	Acuerdos sobre transferencia de información	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	SI	Se cuenta con acuerdos de confidencialidad para la transferencia de información entre el ICBF y las partes externas (Información recopilada de los repositorios del ICBF, los cuales requieren permisos de acceso). - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - P14.GTI Procedimiento Intercambio o Suministro de Informacion - F1.P14.GTI Formato Carta Compromiso de Confidencialidad y No Divulgación - F2.P14.GTI Formato Acuerdo de Intercambio de Información - F3.P14.GTI Formato Documento Tecnico Acuerdo de Intercambio de Información.	X	X	X
A.13.2.3	Mensajería electrónica	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	SI	Se realiza monitoreo al correo electrónico institucional Exchange y 365 a través del proveedor de servicos. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información.	X		
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Se deben identificar, revisar regularmente 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.	SI	Desde la Dirección de Contratación se incluye en las fichas de condiciones técnicas y estudios previos las obligaciones correspondientes al Eje de Segruidad. -Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - G7.ABS Guía para la Adquisicion de Bienes y Servicios. - F7.P2.ABS Formato Compromiso de Confidencialidad Información Contratistas. - F5.G7.ABS Compromiso de Confidencialidad - F6.P2.ABS Formato Autorización de Tratamiento de Datos Personales Contratistas. - F5.G7.ABS Formato Compromiso de Confidencialidad - Operadores - F12.P21.GTH, Formato Compromiso de Confidencialidad de Información - F5.P21.GTH Formato Autorización de Tratamiento de Datos Personales -G23.GTI Guía Metodológica para la Anonimización de Registros	X	X	X
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**						
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	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. https://www.icbf.gov.co/sites/default/files/procesos/a4.ms_.de_manual_de_politicas_de_seguridad_de_la_informacion_v8.pdf - P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información https://www.icbf.gov.co/system/files/procesos/p6.gti_procedimiento_para_desarrollo_y_mantenimiento_sistemas_de_informacion_v11.pdf - G1.GTI Guía de estándares de desarrollo y arquitectura de sistemas de información. https://intranet.icbf.gov.co/sites/default/files/procesos/g1.gti_guia_de_estandares_de_desarrollo_y_arquitectura_de_sistemas_de_informacion_v11.pdf - G3.GTI Guía de estándares de especificación de requerimientos. https://www.icbf.gov.co/system/files/procesos/g3.gti_guia_de_estandares_de_especificacion_de_requerimientos_v4.pdf	X		

No del Control	Objetivo de control	Control	SI/NO	Declaración de Aplicabilidad	Aplicación		
					Nacional	Regional	Zonal
A.14.1.2	Seguridad de servicio de las aplicaciones en redes publicas	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	SI	Se evidencia que mediante lo siguiente se apican y definen las directrices de seguridad para los servicios accedidos mediante redes públicas: - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. https://www.icbf.gov.co/sites/default/files/procesos/a4.ms_.de_manual_de_politicas_de_seguridad_de_la_informacion_v8.pdf - G1.GTI Guía de estándares de desarrollo y arquitectura de sistemas de información. https://intranet.icbf.gov.co/sites/default/files/procesos/g1.gti_guia_de_estandares_de_desarrollo_y_arquitectura_de_sistemas_de_informacion_v11.pdf - Uso de certificados digitales	X		
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado la alteración no autorizada de mensajes, la divulgación no autorizada y la divulgación o reproducción de mensajes no autorizados.	SI	La protección de transacciones de servicios de aplicaciones se encuentran definidas y aplicadas de la siguiente manera: - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. https://www.icbf.gov.co/sites/default/files/procesos/a4.ms_.de_manual_de_politicas_de_seguridad_de_la_informacion_v8.pdf - G1.GTI Guía de estándares de desarrollo y arquitectura de sistemas de información. https://intranet.icbf.gov.co/sites/default/files/procesos/g1.gti_guia_de_estandares_de_desarrollo_y_arquitectura_de_sistemas_de_informacion_v11.pdf - Utilización de certificados digitales (SSL) para las aplicaciones. - Todas las aplicaciones web son compatibles con https.	X		
A.14.2	**Seguridad en los procesos de desarrollo y soporte**						
A.14.2.1	Políticas de desarrollo seguro	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	SI	Las directrices de acuerdo a la política de desarrollo se definen mediante la siguiente documentación: - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. https://www.icbf.gov.co/sites/default/files/procesos/a4.ms_.de_manual_de_politicas_de_seguridad_de_la_informacion_v8.pdf - P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información https://www.icbf.gov.co/system/files/procesos/p6.gti_procedimiento_para_desarrollo_y_mantenimiento_sistemas_de_informacion_v11.pdf - G1.GTI Guía de estándares de desarrollo y arquitectura de sistemas de información. https://intranet.icbf.gov.co/sites/default/files/procesos/g1.gti_guia_de_estandares_de_desarrollo_y_arquitectura_de_sistemas_de_informacion_v11.pdf	X		
A.14.2.2	Procedimiento de control de cambios en sistemas	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.	SI	ICBF establece los procedimientos formales para controlar los cambios en los ambientes productivos de las aplicaciones, lo cual es liderado por la SRT. En lo relacionado con los cambios en el ciclo de desarrollo, lo lidera la SSII: '- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. https://www.icbf.gov.co/sites/default/files/procesos/a4.ms_.de_manual_de_politicas_de_seguridad_de_la_informacion_v8.pdf - P4.GTI Gestión de Cambios de Tecnologías de la Información https://www.icbf.gov.co/system/files/procesos/p4.gti_procedimiento_gestion_de_cambios_de_tecnologias_de_la_informacion_v6.pdf - P3.GTI Procedimiento Gestión Cambios Emergencia Tecnologías de Información https://www.icbf.gov.co/sites/default/files/procesos/p3.gti_procedimiento_gestion_cambios_emergencia_tecnologias_de_informacion_v3.pdf - P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información https://www.icbf.gov.co/system/files/procesos/p6.gti_procedimiento_para_desarrollo_y_mantenimiento_sistemas_de_informacion_v11.pdf - F1.P4.GTI Formato Requerimiento de Cambios Informático (RFC) de Infraestructura Tecnológica y Sistemas de Información https://www.icbf.gov.co/system/files/procesos/f1.p4.gti_formato_requerimiento_de_cambios_informaticos_rfc_v6.docx	X		
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	SI	- A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. https://www.icbf.gov.co/sites/default/files/procesos/a4.ms_.de_manual_de_politicas_de_seguridad_de_la_informacion_v8.pdf. - P4.GTI Gestión de Cambios de Tecnologías de la Información https://www.icbf.gov.co/system/files/procesos/p4.gti_procedimiento_gestion_de_cambios_de_tecnologias_de_la_informacion_v6.pdf - P3.GTI Procedimiento Gestión Cambios Emergencia Tecnologías de Información https://www.icbf.gov.co/sites/default/files/procesos/p3.gti_procedimiento_gestion_cambios_emergencia_tecnologias_de_informacion_v3.pdf - F1.P4.GTI Formato Requerimiento de Cambios Informático (RFC) de Infraestructura Tecnológica y Sistemas de Información https://www.icbf.gov.co/system/files/procesos/f1.p4.gti_formato_requerimiento_de_cambios_informaticos_rfc_v6.docx	X		
A.14.2.4	Restricción en los cambios a los paquetes de software	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.	SI	Los cambios en el software de terceros, se rigen bajo los procedimientos de control de cambios definidos por la Entidad: '- A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. https://www.icbf.gov.co/sites/default/files/procesos/a4.ms_.de_manual_de_politicas_de_seguridad_de_la_informacion_v8.pdf. - P4.GTI Gestión de Cambios de Tecnologías de la Información https://www.icbf.gov.co/system/files/procesos/p4.gti_procedimiento_gestion_de_cambios_de_tecnologias_de_la_informacion_v6.pdf - P3.GTI Procedimiento Gestión Cambios Emergencia Tecnologías de Información https://www.icbf.gov.co/sites/default/files/procesos/p3.gti_procedimiento_gestion_cambios_emergencia_tecnologias_de_informacion_v3.pdf - P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información https://www.icbf.gov.co/system/files/procesos/p6.gti_procedimiento_para_desarrollo_y_mantenimiento_sistemas_de_informacion_v11.pdf - F1.P4.GTI Formato Requerimiento de Cambios Informático (RFC) de Infraestructura Tecnológica y Sistemas de Información https://www.icbf.gov.co/system/files/procesos/f1.p4.gti_formato_requerimiento_de_cambios_informaticos_rfc_v6.docx	X		
A.14.2.5	Principios de construcción de los sistemas seguros	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros , y aplicarlos a cualquier actividad de implementación de sistemas de información.	SI	Mediante los siguientes documentos se definen los principios para la construcción de sistemas seguros que son aplicados para el ciclo de desarrollo: '- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. https://www.icbf.gov.co/sites/default/files/procesos/a4.ms_.de_manual_de_politicas_de_seguridad_de_la_informacion_v8.pdf - P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información https://www.icbf.gov.co/system/files/procesos/p6.gti_procedimiento_para_desarrollo_y_mantenimiento_sistemas_de_informacion_v11.pdf - G1.GTI Guía de estándares de desarrollo y arquitectura de sistemas de información. https://intranet.icbf.gov.co/sites/default/files/procesos/g1.gti_guia_de_estandares_de_desarrollo_y_arquitectura_de_sistemas_de_informacion_v11.pdf	X		

No del Control	Objetivo de control	Control	SI/NO	Declaración de Aplicabilidad	Aplicación		
					Nacional	Regional	Zonal
A.14.2.6	Ambiente seguro de desarrollo	Las organizaciones 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 sistemas .	SI	La SSII define los ambientes de desarrollo, pruebas, aceptación, incidentes, preproducción y capacitación seguro. El ambiente productivo es liderado por la SRT. Lo anterior, está consignado en los siguientes documentos: - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. https://www.icbf.gov.co/sites/default/files/procesos/a4.ms_.de_manual_de_politicas_de_seguridad_de_la_informacion_v8.pdf. - P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información https://www.icbf.gov.co/system/files/procesos/p6.gti_procedimiento_para_desarrollo_y_mantenimiento_sistemas_de_informacion_v11.pdf - G1.GTI Guía de estándares de desarrollo y arquitectura de sistemas de información. https://intranet.icbf.gov.co/sites/default/files/procesos/g1.gti_guia_de_estandares_de_desarrollo_y_arquitectura_de_sistemas_de_informacion_v11.pdf - Guía de Integración, Entrega y Despliegue Conitnuo (CI/CD) en Azure Devops https://intranet.icbf.gov.co/sites/default/files/procesos/g26.gti_guia_de_integracion_entrega_y_despliegue_continuo_cicd_en_azure_devops_v1.pdf	X		
A.14.2.7	Desarrollo externamente contratado	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	SI	Se obliga al cumplimiento a través de las cláusulas de los contratos asociados al desarrollo de software - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. https://www.icbf.gov.co/sites/default/files/procesos/a4.ms_.de_manual_de_politicas_de_seguridad_de_la_informacion_v8.pdf. - P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información https://www.icbf.gov.co/system/files/procesos/p6.gti_procedimiento_para_desarrollo_y_mantenimiento_sistemas_de_informacion_v11.pdf -Obligaciones contractuales sobre cumplimiento de lineamientos de desarrollo establecidos por el ICBF en contratos asociados al desarrollo de sistemas contratados externamente	X		
A.14.2.8	Pruebas de seguridad de sistemas	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	SI	- A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. https://www.icbf.gov.co/sites/default/files/procesos/a4.ms_.de_manual_de_politicas_de_seguridad_de_la_informacion_v8.pdf. - P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información https://www.icbf.gov.co/system/files/procesos/p6.gti_procedimiento_para_desarrollo_y_mantenimiento_sistemas_de_informacion_v11.pdf	X		
A.14.2.9	Prueba de aceptación de sistemas	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados .	SI	- A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. https://www.icbf.gov.co/sites/default/files/procesos/a4.ms_.de_manual_de_politicas_de_seguridad_de_la_informacion_v8.pdf.' - P6.GTI Procedimiento para Desarrollo y Mantenimiento Sistemas de Información https://www.icbf.gov.co/system/files/procesos/p6.gti_procedimiento_para_desarrollo_y_mantenimiento_sistemas_de_informacion_v11.pdf	X		
A.14.3	**Datos de pruebas**						
A.14.3.1	Protección de datos de pruebas	Los datos de prueba se deben seleccionar, proteger y	SI	- A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información.	X		
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	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 con éstos y se deben documentar.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - G7.ABS Guía para la Adquisición de Bienes y Servicios de Calidad. - Contratos suscritos	X	X	X
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - G7.ABS Guía para la Adquisición de Bienes y Servicios de Calidad. - Contratos suscritos - P22.GTI Procedimiento de Transición de Entrada y Salida Proveedores (Solo para la DIT)	X	X	X
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - G7.ABS Guía para la adquisición de bienes y servicios de calidad - Contratos suscritos - Estudios previos	X		
A.15.2	**Gestión de la prestación de servicios de proveedores**						
A.15.2.1	Seguimiento y revisión a los servicios proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - G7.ABS Guía para la adquisición de bienes y servicios de calidad - Contratos suscritos - F43.G7.ABS Formato Seguimiento Cumplimiento Controles Seguridad Información Proveedores Servicios Tecnologicos.	X	X	X
A.15.2.2	Gestión de cambios en los servicios de los proveedores	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 seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE Manual de Políticas de Seguridad de la información. - P4.GTI Procedimiento Gestión de Cambios de Tecnologías de la Información - F1.P4.GTI Formato Requerimiento de Cambios Informático (RFC) de Infraestructura Tecnológica y Sistemas de Información - F3.P4.GTI Formato Bitácora de Controles de Cambios (RFC)	X		
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	Responsabilidades y procedimientos	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.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - F1.P5.GTI Formato Informe Incidente de Seguridad Digital.	X		
A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P5.GTI Procedimiento Gestión de Incidentes de Seguridad Digital. - F1.P5.GTI Formato informe Incidente de Seguridad de Digital. - G5.GTI Guía de recolección de evidencias de elementos informáticos.	X	X	X
A.16.1.3	Reporte de debilidades de seguridad de la información	Se debe exigir a todos los empleados y contratistas que usan los 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.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P5.GTI Procedimiento Gestión de Incidentes de Seguridad Digital.	X	X	X
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se deben evaluar y se debe decir si se van a clasificar como incidentes de seguridad de la información.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - P5.GTI Procedimiento Gestión de Incidentes de Seguridad Digital.	X		
A.16.1.5	Respuesta a incidentes de seguridad de la información	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - P5.GTI Procedimiento Gestión de Incidentes de Seguridad Digital. - F1.P5.GTI Formato Informe Incidente de Seguridad Digital. - F2.P5.GTI Fomato reporte incidentes bases de datos personales Superintendencia de Industria y Comercio.	X		

No del Control	Objetivo de control	Control	SI/NO	Declaración de Aplicabilidad	Aplicación		
					Nacional	Regional	Zonal
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	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.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - F1.P10.GTI Formato Postulación Conocimiento Tecnológico. -P10.GTI Procedimiento Gestión del Conocimiento Tecnológico - P5.GTI Procedimiento Gestión de Incidentes de Seguridad Digital. - F1.P5.GTI Formato Informe Incidente de Seguridad Digital.	X		
A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de la información que puede servir como evidencia.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - G5.GTI Guía de Recolección de Evidencias de Elementos Informáticos	X		
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO**						
A.17.1	**Continuidad de seguridad de la información**						
A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debe determinar sus requisitos para la seguridad de la y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - P18.DE Procedimiento Plan de Continuidad de la Operación - PL9.GTI Plan de Recuperacion de Desastres Tecnologicos - F1.PL9.GTI Formato Plan de Pruebas del Plan de Recuperación de Desastres Tecnológicos - F2.PL9.GTI Formato Resultado Ejecución del Plan de Recuperación de Desastres Tecnológicos - F3.PL9.GTI Formato Cronograma de Pruebas Plan de Recuperación de Desastres Tecnológicos - F4.PL9.GTI Formato Bitácora de Actividades del Plan de Recuperación de Desastres Tecnológicos - F5.PL9.GTI Formato Árbol de Comunicaciones Plan de Recuperación de Desastres Tecnológicos - F6.PL9.GTI Formato Requisitos de Seguridad de la Información	X	X	
A.17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P18.DE Procedimiento Plan de Continuidad de la Operación (Solo aplica para la Sede de la Dirección General) - P4.GTI Procedimiento gestión de cambios de tecnologías de la información (Solo aplica para la Sede de la Dirección General) - P3.GTI Procedimiento Gestión de Cambios de Emergencia de Tecnologías de la Información y los planes de contingencia en el formato. (Solo aplica para la Sede de la Dirección General) - F1.P4.GTI Formato requerimiento de cambios informáticos-RFC. (Solo aplica para la Sede de la Dirección General) - G8.GTI Guía Respaldo y restauración de copias de seguridad. (Solo aplica para la Sede de la Dirección General) - PL9.GTI Plan de recuperación de desastres tecnológicos. (Solo aplica para la Sede de la Dirección General) - F1.PL9.GTI Formato plan de pruebas del plan de recuperación de desastres tecnológicos. (Aplica para la Regional y Sede de la Dirección General) - F2.PL9.GTI Formato Resultado ejecución del plan de recuperación de desastres tecnológicos. (Aplica para la Regional y Sede de la Dirección General) - F3.PL9.GTI Formato cronograma de pruebas plan de recuperación de desastres tecnológicos (Aplica para la Regional y Sede de la Dirección General) - F4.PL9.GTI Formato bitácora de actividades del plan de recuperación de desastres tecnológicos (Aplica para la Regional y Sede de la Dirección General) -F5.PL9.GTI Formato árbol de comunicaciones plan de recuperación de desastres tecnológicos (Solo aplica para la Sede de la Dirección General) - F6.PL9.GTI Formato requisitos de seguridad de la información (Aplica para la Regional y Sede de la Dirección General) - F2.P18.DE Estratégico escenarios y estrategias plan de continuidad de la operación. - F1.P18.DE Plan de Sucesión - F3.P18.DE Formato informe final plan de continuidad.	X		
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	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.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P18.DE Procedimiento Plan de Continuidad de la Operación. - PL9.GTI Plan de Recuperacion de Desastres Tecnologicos. - F1.PL9.GTI Formato Plan de Pruebas del Plan de Recuperación de Desastres Tecnológicos. - F2.PL9.GTI Formato Resultado Ejecución del Plan de Recuperación de Desastres Tecnológicos. - F3.PL9.GTI Formato Cronograma de Pruebas Plan de Recuperación de Desastres Tecnológicos. - F4.PL9.GTI Formato Bitácora de Actividades del Plan de Recuperación de Desastres Tecnológicos. - F6.PL9.GTI Formato requisitos de seguridad de la información. En las Regionales se realizan ejercicios de continuidad conforme a un escenario propuesto el cual se evalúa en el Plan Operativo del SGSI.	X	X	
A.17.2	**Redundancia**						
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P18.DE Procedimiento Plan de Continuidad de la Operación. - PL9.GTI Plan de recuperación de desastres tecnológicos.	X		
A.18	**CUMPLIMIENTO**						
A.18.1	**Cumplimiento de requisitos legales y contractuales**						
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	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 y para la organización.	SI	Se cuenta con la Matriz de verificación de Requisitos Legales. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - P4.MI Procedimiento Identificación y Evaluación de Requisitos Legales. - IT1.P4.MI Instructivo matriz de verificación de requisitos legales.	X	X	X
A.18.1.2	Derechos de propiedad intelectual	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.	SI	El análisis de propiedad intelectual se encuentra desarrollado normativamente en la legislación interna mediante la Ley 23 de 1982 y en la legislación de la Comunidad Andina de Naciones (CAN) mediante la Decisión 351 de 1993. Se cuenta con el servicio de licenciamiento de software; se cuenta con un compromiso de Antipiratería ACUERDO No. 3 de 2017 del Instituto Colombiano de Bienestar Familiar; Se cuenta con una serie de obras y software registrado ante el MINISTERIO DEL INTERIOR DIRECCIÓN NACIONAL DE DERECHO DE AUTOR, de igual manera se encuentran registradas algunas marcas ante la SuperIntendencia de Industria y Comercio - SIC. -Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información.	X	X	X
A.18.1.3	Protección de registros	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.	SI	La Dirección Administrativa a través del grupo de Gestión Documental establece directrices de retención de registros e información contenidas en las Tablas de Retención Documental de la Entidad. -Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - PL35.SA Plan Institucional de Archivos - PINAR. - P1.SA Procedimiento Organización de Archivos. - Tablas de Retención Documental - TRD.	X	X	X
A.18.1.4	Privacidad y protección de información de datos personales	Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	SI	-Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - Política de Protección de datos personales - P12.GTI Procedimiento Interno de Registro de Bases Datos Personales. - P15.GTI Procedimiento para la consulta, actualización, revocación y supresión de datos personales. - P14.GTI Procedimiento para el intercambio o suministro de información - Política de tratamiento de Datos Personales - F5.P21.GTH Formato Autorización de Tratamiento de Datos Personales - F6.P2.ABS Formato Autorización de Tratamiento de Datos Personales Contratistas -G23.GTI Guía Metodológica para la Anonimización de Registros -A2.P12.GTI Anexo 2 Paso a Paso Registro Bases de Datos Personales - RNBD -F1.P12.GTI Formato Consolidado Bases de Datos Personales	X	X	X

No del Control	Objetivo de control	Control	SI/NO	Declaración de Aplicabilidad	Aplicación		
					Nacional	Regional	Zonal
A.18.1.5	Reglamentación de controles criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	SI	Se cuenta con Controles Criptográficos identificados, los cuales se encuentran definidos en la documentación del Servicio de Seguridad Perimetral. -Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información	X		
A.18.2				**Revisiones de seguridad de la información**			
A.18.2.1	Revisión independiente de la seguridad de la información	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 seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información - P2.El Procedimiento Auditorias Internas SIGE y la formulación del plan de auditorias. - Revisión por la Dirección.	X	X	X
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	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.	SI	Se han identificado oportunidades de mejora y acciones correctivas para el incumplimiento de las políticas de seguridad de la información. - Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información.	X	X	X
A.18.2.3	Revisión del cumplimiento técnico	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	SI	- Resolución por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información. - A4.MS.DE. Anexo 4 Manual de Políticas de Seguridad de la Información. - P1.GTI Procedimiento Seguimiento, Control y Atención de Vulnerabilidades Técnicas - F1.P1.GTI Formato de Registro de Pruebas y Remediacion de Vulnerabilidades - G14.GTI Guía Desarrollo Pruebas Penetración. - G3.GTI. Guía de Estándares de Desarrollo y Arquitectura de Sistemas de Información	X		

CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
28/06/2022	A3.MS.DE V11	Se realiza actualización conforme a las modificaciones de los diferentes documentos asociados a la implementación al Sistema de Gestión de Seguridad de la Información, por lo cual se realizaron ajustes sobre los siguientes dominios y controles del Anexo A: A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN A.7. SEGURIDAD DE LOS RECURSOS HUMANOS A.8. GESTIÓN DE ACTIVOS A.9. CONTROL DE ACCESOS A.10. CRIPTOGRAFIA A.11. SEGURIDAD FÍSICA Y DEL ENTORNO A.12. SEGURIDAD DE LAS OPERACIONES A.13. SEGURIDAD DE LAS COMUNICACIONES A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS A.15. RELACIONES CON LOS PROVEEDORES A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO A.18. CUMPLIMIENTO
3/05/2022	A3.MS.DE V10	Se realiza actualización conforme a la nueva normatividad, documentación asociada a la mejora del Sistema de Gestión de Seguridad de la Información, por lo cual se realizaron modificaciones sobre los siguientes dominios y controles del Anexo A: A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN A.7. SEGURIDAD DE LOS RECURSOS HUMANOS A.8. GESTIÓN DE ACTIVOS A.9. CONTROL DE ACCESOS A.10. CRIPTOGRAFIA A.11. SEGURIDAD FÍSICA Y DEL ENTORNO A.12. SEGURIDAD DE LAS OPERACIONES A.13. SEGURIDAD DE LAS COMUNICACIONES A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS A.15. RELACIONES CON LOS PROVEEDORES A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO A.18. CUMPLIMIENTO
30/06/2020	A3.MS.DE V9	Se realiza actualización conforme a la documentación que se tiene formalizada en el SIGE, los ajustes se realizaron en los siguientes dominios y controles del Anexo A: A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN A.7. SEGURIDAD DE LOS RECURSOS HUMANOS A.8. GESTIÓN DE ACTIVOS A.9. CONTROL DE ACCESOS A.10. CRIPTOGRAFIA A.11. SEGURIDAD FÍSICA Y DEL ENTORNO A.12. SEGURIDAD DE LAS OPERACIONES A.13. SEGURIDAD DE LAS COMUNICACIONES A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS A.15. RELACIONES CON LOS PROVEEDORES A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO A.18. CUMPLIMIENTO
8/03/2019	A3.MS.DE V8	Se realiza actualización conforme a la documentación que se tiene formalizada en el SIGE, los ajustes se realizaron en los siguientes dominios: A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN A.7. SEGURIDAD DE LOS RECURSOS HUMANOS A.8. GESTIÓN DE ACTIVOS A.9. CONTROL DE ACCESOS A.10. CRIPTOGRAFIA A.11. SEGURIDAD FÍSICA Y DEL ENTORNO A.12. SEGURIDAD DE LAS OPERACIONES A.13. SEGURIDAD DE LAS COMUNICACIONES A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS A.15. RELACIONES CON LOS PROVEEDORES A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO A.18. CUMPLIMIENTO
16/08/2018	A3.MS.DE V7	Se elimina la columna Observaciones Se incluye en el documento la tabla de cambios realizados al anexo. Se realiza actualización en los nombres de la documentación relacionada en las descripciones A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN A.7 SEGURIDAD DE LOS RECURSOS HUMANOS A.8 GESTIÓN DE ACTIVOS A.9 CONTROL DE ACCESOS A.11 SEGURIDAD FÍSICA Y DEL ENTORNO A.12 SEGURIDAD DE LAS OPERACIONES A.13 SEGURIDAD DE LAS COMUNICACIONES A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS A.15 RELACIONES CON LOS PROVEEDORES A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO A.18 CUMPLIMIENTO
8/06/2018	A3.MS.DE V6	La Declaración de Aplicabilidad se modifica, ya que se derogan las Resoluciones 9364 y 3600 y se crea la Resolución No. 9674 del 27 de julio de 2018 "Por la cual se adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación, las Políticas Generales de Manejo y se definen lineamientos frente al uso y manejo de la información".
26/10/2017	A3.MS.DE V5	Se eliminan de la declaración los link asociados con cada uno de los objetivos de control. Se actualiza el rotulado del documento de acuerdo con lo definido en la G11.GTI Guía para la Rotulación de la Información.

17/05/2017	A3.MS.DE V4	Producto de la auditoría interna efectuada al SGSI en el año 2017, se generó el hallazgo "AI.SGSI.DG.03 Una vez verificada la acción correctiva No.6727 relacionada con el requisito 7.5.3. Control de la información documentada literal c), se encontró que la Declaración de aplicabilidad V4, no cuenta con control de cambios y sus hipervínculos relacionados con el Manual de Seguridad V4 se encuentran rotos, situaciones que evidencian falta de eficacia, incumpliendo lo establecido en la NTC-ISO-IEC 27001:2013 requisito 10.1 No conformidades y Acciones correctiva literal d)". en el marco del cual, de acuerdo con el análisis de causas elaborado conjuntamente con el proceso de Mejora e Innovación, se identificó la necesidad de realizar corrección enfocada a efectuar revisión y ajustes en el Anexo 3 Declaración de aplicabilidad. Los cambios realizados en la declaración de aplicabilidad fueron los siguientes: A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN: Se realiza actualización en los enlaces de los documentos. A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN: Se realiza actualizaciones de descripciones y enlaces. A.7 SEGURIDAD DE LOS RECURSOS HUMANOS: Se realiza actualizaciones de descripciones y enlaces. A.8 GESTIÓN DE ACTIVOS: Se realiza actualización en los enlaces de los documentos. A.9 CONTROL DE ACCESOS: Se realiza actualizaciones de descripciones y enlaces. A.11 SEGURIDAD FÍSICA Y DEL ENTORNO: Se realiza actualizaciones de descripciones y enlaces. A.12 SEGURIDAD DE LAS OPERACIONES: Se realiza actualizaciones de descripciones y enlaces. A.13 SEGURIDAD DE LAS COMUNICACIONES: Se realiza actualizaciones de descripciones y enlaces. A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS: Se realiza actualizaciones de descripciones y enlaces. A.15 RELACIONES CON LOS PROVEEDORES: Se realiza actualizaciones de descripciones y enlaces. A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: Se realiza actualizaciones de descripciones y enlaces. A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO: se realiza actualización en los enlaces de los documentos. A.18 CUMPLIMIENTO: Se realiza actualización de descripciones y enlaces.
5/05/2017	A3.MS.DE V3	Se surten ajustes y actualización en las rutas relacionadas dentro de la declaración, como evidencia del cumplimiento de los controles que aplican al ICBF.
7/10/2016	A3.MS.DE V2	Teniendo en cuenta que la Entidad adoptó un nuevo modelo de operación por procesos e implementó Teletrabajo, se actualiza la exclusión que existía en la Declaración de Aplicabilidad publicada actualmente, además siguiendo las acciones correctivas de la Auditoria Interna 2016 Regional Caldas.
24/08/2016	A3.MS.DE V1	Actualización de Anexos con respecto a la codificación según el nuevo modelo de procesos.