DECLARACIÓN DE APLICABILIDAD (SOA) ISO 27001:2013 Anexo A

Fecha de actualización: enero 2019

Sección	Control	Descripción del Control	Aplica	Justificación Desde el Negocio	Justificación de la Inclusión
A5	Políticas de la Seguridad de la información				
A.5.1	Orientación de la dirección para la gestión de la seguridad de la información.		Aplica	Razón para la selección / Justificación	Documentos
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	En el FNG los Sistemas de Gestión cuenta con directrices establecidas por la alta dirección que funcionen como base para la implementación del dichos sistemas	PD-GTE-CIN-019 Cifrado de Información, MA-GTE-010 Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.2 Del uso de los controles criptográficos MA-GTE-010 Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.6.4 Dispositivos móviles PD-GTE-IHS-007 Instalación de Hardware y Software MA-GTE-010 Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.12.2. De la instalación de software . MA-GTE-003 Metodología Ciclo de Vida de Desarrollo de Software - Cap. 8 Seguridad de la Información MA-GTE-010 Manual de Gestión tecnológica y seguridad informática -Cap. 3.3 Gestión de Proveedores Contratos con proveedores MA-GQU-001 - Manual del Sistema de Gestión Integrado - Cap. 27.1 Desarrollo Seguro MA-GTE-003 Metodología Ciclo de Vida de Desarrollo de Software - Cap. 3.2.4 Desarrollo MA-GQU-001 - Manual del Sistema de Gestión Integrado - Cap. 27.1 Desarrollo Seguro MA-GTE-003 Metodología Ciclo de Vida de Desarrollo de Software - Cap. 5 Esquema de Desarrollo del Software - Cap. 3.2.4 Desarrollo PD-GTE-014 Administración de Cambios MA-GTE-010 Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.12.5 Gestión de Cambios MA-GDO-003 Programa de Gestión Documental -Cap. 1.2.1.1 Políticas relacionadas con seguridad de la información MA-GQU-001 - Manual del Sistema de Gestión Integrado - Cap. 27.1 Desarrollo Seguro MA-GTE-010 Manual de Gestión tecnológica y seguridad informática - Cap. 4.3.1.1. Políticas de hardware IN-GTE-014 Borrado de Información Equipo de Escritorio PD-GTE-RIR-010 Respaldo y Recuperación de la información MA-GQU-001 - Manual del Sistema de Gestión Integrado - Cap. 19.2. Contacto con la Autoridades y Grupos de interés. MA-GTE-010 Manual de Gestión tecnológica y seguridad informática - Cap. 3.2.1. Gestión de Relaciones internas y Externas MA-GQU-001 - Manual del Sistema de Gestión Integrado - Cap. 24.1 Política Puesto de trabajo limpio y pantalla segura MA-GTE-010 Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.5.3. Del retiro de equipos de las instalaciones del FNG. - Cap. 4.6.8.1 De la seguridad y el uso adecuado de los equipos propiedad del FNG. - Cap. 4.6.4.4. De los equipos móviles. - Cap. 4.6.6.4. Dispositivos Móviles. PD-GTE-CIN-019 Cifrado de la información Actos Administrativos de Comités de Alta Dirección (CCSCI, Operaciones del SGI, Proyectos, Presidencia, etc.) MA-GQU-001 - Manual del Sistema de Gestión Integrado - Cap. 19.1 Roles, responsabilidades y separación de deberes MA-GHU-007 Manual Específico de Funciones y Competencias Laborales Reglamento de Garantías V 3.1 MA-GQU-001 - Manual del Sistema de Gestión Integrado - Cap. 21.1 Inventario de Activos MA-GDO-003 Programa de Gestión Documental - Cap. 1.2.1.1.1 Clasificación de los activos de información PD-SAD-002 Administración de activos fijos MA-SAD-002 Manual para el control de acceso y permanencia en las instalaciones del FNG - Cap. 4.4 Sobre la salida o ingreso de los activos fijos tecnológicos y demás equipos de computo del FNG MA-GQU-001 - Manual del Sistema de Gestión Integrado - Cap. 24.1 Puesto de trabajo limpio y pantalla seguro MA-GTE-010 Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.1.1 Del acceso a la información PD-GTE-006 Administración de usuarios - Cap. 1 Lineamientos Generales de Seguridad PD-GTE-018 Gestión de logs PD-GTE-018 Gestión de logs MA-SAD-002 Manual para el Control de Acceso y Permanecia en las Instalaciones del FNG - Cap. 4.7.3 Departamento de Tecnología PD-GTE-008 Procedimiento de Administración de la Infraestructura de redes y comunicaciones MA-GDO-003 Programa de Gestión Documental - Cap. 1.2.1.1.2 Etiquetado de la Información MA-GQU-004 - Manual de Gestión de Incidentes de Seguridad de la Información PD-GTE-016 Gestión de Incidentes Cambios y mejoras PD-GQU-003 - Atención a incidentes de Seguridad de la Información IN-GTE-002 Sincronización Horario de los Sistemas MA-GTE-003 Metodología Ciclo de Vida de Desarrollo de Software - Cap. 3.2.5. Pruebas PD-GTE-007 Instalación de Hardware o Software
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	Existe un procedimiento de Revisión por la Dirección que incluye la responsabilidad de validar periódicamente el estado de los sistemas de gestión	Actos Administrativos de conformación del CCSCI, Comité de Operaciones de SGSI, Comité de datos personales Actas del CCCI, Comité de Operaciones de SGSI, Comité de datos personales PD-GQU-ACP Acciones Correctivas y Preventivas
A6	Organización de la seguridad de la información				
A.6.1	Organización interna		Cumplimiento		Documentos
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	SI	En el FNG se encuentran conformados diferentes comités de alta dirección y de operación a los cuales se les deben atribuir funciones relacionadas con el SGSI	Actos Administrativos de Comités de Alta Dirección (CCSCI, Operaciones del SGI, Proyectos, Presidencia, etc.) MA-GHU-007 Manual Específico de Funciones y Competencias Laborales. MA-GQU-001 - Manual del Sistema de Gestión Integrado - Cap. 19.1 Roles, responsabilidades y separación de deberes
A.6.1.2	Separación de deberes	Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de la organización.	SI	Por la estructura establecida en la entidad y considerando que hay actividades críticas que deben ser manejadas por diferentes niveles jerárquicos la separación de deberes se hace fundamental como control para mitigar los riesgos	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.1.1 Del acceso a la información, - Cap. 4.6.10 De la utilización de los recursos de red MA-GTE-006 Manual para la Administración de usuarios. - Cap2 Roles y Responsabilidades MA-GQU-001 - Manual del sistema de Gestión Integrado. - Cap. 25.4 Segregación de Funciones PD-GTE-AUS-006 Administración de Usuarios Matrices de Roles y Perfiles MA-GTC-001 Manual de Contratación-Cap. 3.6 Etapas de la Contratación PD-GHU-PHU-021 Pagos de Gestión Humana MA-GTC-001 Manual de Contratación Matriz de Roles y Perfiles SAP y CUD MA-GHU-007 Manual Específico de Funciones y Competencias Laborales PD-GCA-007 Identificación y aplicación de Ingresos MA-GCA Políticas internas subdirección de Cartera. PD-GCA-009 Otorgación de Paz y salvos
A.6.1.3	Contacto con las autoridades	Se deben mantener contactos apropiados con las autoridades pertinentes	SI	El FNG es una entidad del estado y por su naturaleza se hace fundamental mantener contactos con las autoridades	MA-GQU-001 Manual del Sistema de Gestión Integrado - Anexo 5 Contacto con Autoridades y grupos de interés
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	Con el fin de adquirir conocimiento en buenas prácticas o experiencias que sean de utilidad para minimizar los riesgos de seguridad de la información.	
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	El plan de acción del FNG funciona mediante proyectos, muchos de los cuales manejan activos de información críticos	MA-GTC-001 Manual de Contratación MA-GES-002 - Manual de Proyectos -Cap. 2.1.1.5. Seguridad de la información en los proyectos MA-GES-002 - Manual de Proyectos-Cap. 2.4 Etapa de Control y Seguimiento MA-GES-002 - Manual de Proyectos-Cap. 2.4 Etapa de Control y Seguimiento
A.6.2	Dispositivos Móviles y teletrabajo		Cumplimiento		Documentos
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 los dispositivos móviles.	SI	Algunos funcionarios de la entidad usan dispositivos móviles para la ejecución de sus labores	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.6.4 Dispositivos Móviles
A.6.2.2	Teletrabajo	Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza el teletrabajo.	No	No aplica para el FNG por directriz de la Alta Dirección ya que no incorpora el Teletrabajo en su operación.	N/A

Sección	Control	Descripción del Control	Aplica	Justificación Desde el Negocio	Justificación de la Inclusión
A.7	Seguridad de los Recursos Humanos				
A.7.1	Antes de asumir empleo		Cumplimiento		Documentos
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	En el FNG existen procedimientos formales de selección de personal	PD-GHU-SVI-024 Selección, Vinculación e Inducción del Personal
					FD-GHU-VTO-022 Vinculación de personal por la Temporal y/o Outsourcing.
					MA-GHU-007 Manual Específico de Funciones y Competencias Laborales
					Reglamento Interno de Trabajo FNG - Cap. 2 Condiciones de Admisión y Vinculación.
					PD-GHU-SVI-024 Selección, Vinculación e Inducción del Personal
					PD-GHU-VT-026 Vinculación de personal por la Temporal y/o Outsourcing.
					PD-GHU-SVI-024 Selección, Vinculación e Inducción del Personal
					PD-GHU-VT-026 Vinculación de personal por la Temporal y/o Outsourcing.
					PD-GHU-VIR-025 Selección, Vinculación e Inducción del Personal
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	Por las características del negocio y considerando que la información es vital para todos los cargos se han definido condiciones contractuales con las responsabilidades sobre el uso de la información. Esto aunado a las exigencias y responsabilidades que establece el AGN	FR-GHU-019 Contrato de Trabajo- CLÁUSULA NOVENA.- Autorización para el tratamiento de datos personales: EL TRABAJADOR
A.7.2	Durante la ejecución del empleo		Cumplimiento		Documentos
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	En el FNG se encuentran conformados diferentes comités de alta dirección y de operación a los cuales se les deben atribuir funciones relacionadas con el SGSI	MA-GQU-001 - Manual del sistema de Gestión Integrado. - Cap. 10 Compromisos de la Dirección del SGI.
					MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.1.2. Contratos, alianzas y convenios con terceros
					MA-GDO-003 Programa de Gestión Documental- Cap. 1.1.2.1. Responsables de la Gestión documental.
					MA-GHU-007 Manual Específico de Funciones y Competencias Laborales.
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	Es necesario para el FNG realizar sensibilizaciones y divulgaciones que permitan la implementación del SGSI	MA-GQU-001 - Manual del sistema de Gestión Integrado. - Cap. 10 Compromisos de la Dirección del SGI.
					MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.1. Políticas generales
					MA-GDO-003 Programa de Gestión Documental - Cap. 1.1.5. Capacitación y Sensibilización.
					MA-GHU-007 Manual Específico de Funciones y Competencias Laborales.
					PD-GHU-DEP-023 Evaluación de Desempeño y Desarrollo de Personal
					PD-GHU-VIR-025 Selección, Vinculación, Inducción y Reinducción del Personal
					Plan de Capacitación Anual.
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	Requisitos legales del FNG	PD-ESP-CDO-006 Control Interno Disciplinario.
					PD-GHU-DEP-023 Evaluación de Desempeño y Desarrollo de Personal
					PD-GHU-VIR-025 Selección, Vinculación, Inducción y Reinducción del Personal
					FR-GHU-050 Evaluación de la capacitación interna, externa e inducción
					Plan de Capacitación Anual
A.7.3	Terminación y cambio de empleo		Cumplimiento		Documentos
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen validos despues de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir	SI	Por las características del negocio y considerando que la información es vital para todos los cargos se han definido condiciones contractuales con las responsabilidades sobre el uso de la información. Esto aunado a las exigencias y responsabilidades que establece el AGN	FR-GHU-019 Contrato de Trabajo- CLÁUSULA DECIMA PRIMERA- deber de confidencialidad
A.8	Gestión Activos				
A.8.1	Responsabilidad por los activos		Cumplimiento		Documentos
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	Por cumplimiento de requisitos legales el FNG debe identificar la información crítica.	PD-SAD-002 Administración de Activos Fijos
					PD-SAD-002 Administración de Activos Fijos
					Informe detallado de los activos fijos en el que se relacionan faltantes y sobrantes
					MA-GQU-001 - Manual del sistema de Gestión Integrado- Cap 21. Gestión de Activos
					MA-GDO-003 Programa de Gestión Documental- Cap 1.2.1.1.1 Clasificación de los activos de información
					PD-SAD-002 Administración de Activos Fijos
					Listado Activos de Información del SGSI
A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deben tener un propietario	SI	Se manejan diferentes tipos de activos los cuales son responsabilidad de diferentes áreas lo que implica que cada activo este asignado a un propietario	PD-SAD-002 Administración de Activos Fijos
					PD-SAD-002 Administración de Activos Fijos
					PD-SAD-002 Administración de Activos Fijos
					Informe detallado de los activos fijos en el que se relacionan faltantes y sobrantes
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	El FNG ha definido directrices para el manejo de los activos de información con el fin de garantizar su uso adecuado	PD-SAD-002 Administración de Activos Fijos
					PD-SAD-002 Administración de Activos Fijos
					MA-SAD-002 - Manual para el Control de Acceso y Permanencia en las Instalaciones del FNG-Cap. 4 Contenido del Manual para el Control de Acceso y permanencia en las Instalaciones del FNG.
					MA-SAD-002 - Manual para el Control de Acceso y Permanencia en las Instalaciones del FNG-Cap. 4 Contenido del Manual para el Control de Acceso y permanencia en las Instalaciones del FNG.
					PD-SAD-002 Administración de Activos Fijos
					Informe detallado de los activos fijos en el que se relacionan faltantes y sobrantes
					MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 21.5 Manejo de Activos
					MA-GDO-003 Programa de Gestión Documental- Cap. 1.2.1.1.1 Clasificación de los activos de información
					PD-GDO-CEI-001 Correspondencia Externa e Interna
					PD-GDO-CPA-012 Consulta y préstamo de archivos
					PD-SAD-002 Administración de Activos Fijos
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 encuentren a su cargo, al terminar su empleo, contrato o acuerdo	SI	El FNG ha definido directrices para el manejo de los activos de información con el fin de garantizar su uso adecuado	PD-SAD-002 Administración de Activos Fijos
					MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 21.5 Manejo de Activos
					MA-GDO-003 Programa de Gestión Documental- Cap. 1.2.1.1.1 Clasificación de los activos de información
					PD-SAD-002 Administración de Activos Fijos
A.8.2	Clasificación de la información		Cumplimiento		Documentos
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 a modificación no autorizado	SI	Por requisitos legales	MA-GDO-003 Programa de Gestión Documental- Cap. 1.2.1.1.1 Clasificación de los activos de información
					MA-GDO-003 Programa de Gestión Documental- Cap. 1.2.1.1.1 Clasificación de los activos de información
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 información adoptado por la organización.	SI	Por requisitos legales	MA-GDO-003 Programa de gestión documental - Cap. 1.2.1.1.2 Etiquetado de la información
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	El FNG ha definido directrices para el manejo de los activos de información con el fin de garantizar su uso adecuado	MA-GDO-003 Programa de Gestión Documental- Cap. 1.2.1.1.1 Clasificación de los activos de información
					MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 21 Gestión de Activos
					MA-GDO-003 Programa de Gestión Documental- Cap. 1.2.1.1.1 Clasificación de los activos de información
					PD-SAD-002 Administración de Activos Fijos
A.8.3	Manejo de medios		Cumplimiento		Documentos
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	Algunas Áreas,funcionarios de la entidad usan dispositivos móviles para la ejecución de sus labores.	MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 24.1 Política puesto de trabajo limpio y pantalla segura
					MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.8.2 De los medios removibles
					MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 24.1 Política puesto de trabajo limpio y pantalla segura
A.8.3.2	Disposición de los medios	Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales.	SI	Existen procedimientos para disponer de los medios cuando ya no se requieran	Contrato de Custodia de Medios Magnéticos
					MA-GDO-003 Programa de Gestión Documental - Cap. 1.2.2.8. Disposición de Documentos
					IN-GTE-014 Borrado Seguro de Información
					Contrato de Custodia de Medios Magnéticos
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	Por requisitos legales, cumplimiento de la ley de archivo	Contrato de Custodia de Medios Magnéticos
					MA-GDO-003 Programa de Gestión Documental - Cap. 1.2.2.6 Transferencias

Sección	Control	Descripción del Control	Aplica	Justificación Desde el Negocio	Justificación de la Inclusión
A.9	Control de Acceso				
A.9.1	Requisitos del negocio para control de acceso		Cumplimiento		Documentos
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	El FNG maneja políticas de control de acceso de acuerdo a las labores de cada una de las dependencias.	MA-SAD-002 - Manual para el Control de Acceso y Permanencia en las Instalaciones del FNG MA-GDO-003 Programa de Gestión Documental- Cap. 1.2.3 Acceso y Seguridad PD-GDO-CPA-012 Consulta y préstamo de archivos MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.1.1. Del acceso a la información, - Cap. 4.6.10. De la utilización de los recursos de red PD-GTE-AUS-006 Administración de usuarios
A.9.1.2	Acceso a redes y a servicios de red	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados especificamente.	SI	Por Requisitos del Negocio Por operaciones críticas del Negocio Por Actividades de operación tecnológica que hacen parte del core del negocio.	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.10. Utilización de recursos de red MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.11. De la Segregación de la Red MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.3.Del acceso a la red
A.9.2	Gestión de Acceso de usuarios		Cumplimiento		Documentos
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	El FNG tiene definidas directrices para registrar y cancelar usuarios cuando corresponda.	PD-GTE-AUS-006 Administración de usuarios MA-GTE-006 Manual para la administración de usuarios - Cap2 Roles y Responsabilidades MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.6.1. Control de acceso a Equipos MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 22.2 Control de acceso lógico MA-GTE-006 Manual para la administración de usuarios Matrices de Roles y Perfiles MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática- Cap. 4.6.6.2. Usuario y clave de red MA-GTE-006 Manual para la administración de usuarios - Cap. 2 Roles y Responsabilidades
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	El FNG tiene definidas directrices para registrar y cancelar usuarios cuando corresponda.	PD-GTE-AUS-006 Administración de usuarios MA-GTE-006 Manual para la administración de usuarios - Cap. 2 Roles y Responsabilidades MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.6.1. Control de acceso a Equipos MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 22.2 Control de acceso lógico MA-GTE-006 Manual para la administración de usuarios Matrices de Roles y Perfiles
A.9.2.3	Gestión de derechos de acceso privilegiado	Se debe restringir y controlar la asignación y uso. Gestión de los derechos de acceso con privilegios especiales: La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado.	SI	El FNG tiene definidas directrices para registrar y cancelar usuarios cuando corresponda.	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática- Cap. 4.6.6.2. Usuario y clave de red PD-GTE-GDL-018 Gestión de logs IN-GTE-030 Instructivo Generación de reportes de registros de Eventos (Logs) MA-GTE-006 Manual para la administración de usuarios. Cap. 4 Administración de Roles Instructivo SGD
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. Gestión de información confidencial de autenticación de usuarios: La asignación de información confidencial para la autenticación debería ser	SI	El FNG maneja autenticación secreta en varias de sus aplicaciones por lo que ha generado directrices para su gestión	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática- Cap. 4.6.6.2. Usuario y clave de red MA-GTE-006 Manual para la administración de usuarios
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	El FNG tiene definidas directrices para registrar y cancelar usuarios cuando corresponda.	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática- Cap. 4.6.6.2. Usuario y clave de red MA-GTE-006 Manual para la administración de usuarios
A.9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de los usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	SI	El FNG tiene definidas directrices para registrar y cancelar usuarios cuando corresponda.	PD-GTE-AUS-006 Administración de usuarios MA-GTE-006 Manual para la administración de usuarios - Cap. 1. Lineamientos Generales de Seguridad
A.9.3	Responsabilidad de los usuarios		Cumplimiento		Documentos
A.9.3.1	Uso de la información de autenticación secreta	Se debe exigir a los usuarios que cumplan las practicas de la organización para el uso de información de autenticación secreta	SI	El FNG maneja autenticación secreta en varias de sus aplicaciones por lo que ha generado directrices para su gestión.	MA-GTE-006 Manual para la administración de usuarios MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.6.2. Usuario y Clave de red
A.9.4	Control de acceso a sistemas y aplicaciones		Cumplimiento		Documentos
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	Por Requisitos del Negocio	MA-GTE-006 Manual para la administración de usuarios MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática. - Cap. 4.6.8.1. De la seguridad y uso adecuado de los equipos propiedad del FNG. MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.6.2. Usuario y Clave de red
A.9.4.2	Procedimiento de Ingreso Seguro	Cuando lo requiera la política de control de acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	SI	Por Requisitos del Negocio	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.6.2. Usuario y Clave de red
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	El FNG maneja autenticación secreta en varias de sus aplicaciones por lo que ha generado directrices para su gestión.	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.6.2. Usuario y Clave de red MA-GTE-006 Manual para la administración de usuarios
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. Uso de herramientas de administración de sistemas: El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas deberían estar restringidos y estrechamente controlados.	SI	El FNG ha cen tralizado la autorización de hacer uso de programas utilitarios y de instalación de software con el fin de garantizar la seguridad de la información	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática. - Cap. 4.6.12.1. De la instalación de software.
A.9.4.5	Control de acceso a códigos fuente de programas	Se debe restringir el acceso a los códigos fuente de los programas.	SI	El FNG ha definido políticas de restricción de acceso a los códigos fuente de los programas	MA-GTE-003 - Metodología Ciclo de Vida del Desarrollo de Software
A.10	Criptografía				
A.10.1	Controles criptográficos		Cumplimiento		Documentos
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	El FNG recibe y envía información a través de diferentes mecanismos es necesario definir directrices para realizar dichas operaciones	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática. - Cap. 4.6.2. Del uso de los controles criptográficos PD-GTE-CIN-019 Cifrado de información IN-GTE-025 Envío y visualización de correos encriptados
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 todo su ciclo de vida.	SI	El FNG recibe y envía información a través de diferentes mecanismos es necesario definir directrices para realizar dichas operaciones	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática. - Cap. 4.6.2. Del uso de los Controles Criptográficos
A.11	Seguridad Física y del Entorno				
A.11.1	Áreas Seguras		Cumplimiento		Documentos
A.11.1.1	Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad y usuarios para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	SI	El FNG ha delimitado sus perímetros de seguridad	MA-SAD-002 Manual para el control de acceso y permanencia en las instalaciones del FNG - Cap. 4.9.2 Personal autorizado para el accesso a la Bóveda de Seguridad MA-SAD-002 Manual para el control de acceso y permanencia en las instalaciones del FNG - Cap. 3, Políticas Generales MA-GPO-001 Manual de Operaciones de Tesorería - Cap. 2.2.1 Medios de comunicación y equipos de cómputo
A.11.1.2	Controles de acceso físicos	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permita el acceso a personal autorizado.	SI	El FNG cuenta con diferentes controles de acceso físicos y los ha establecido de manea formal.	MA-GDO-003 Programa de gestión documental - Cap. 1.1.2.1 Responsabilidades personal de archivo MA-SAD-002 Manual para el control de acceso y permanencia en las instalaciones del FNG - Cap. 4.9.2 Personal autorizado para el accesso a la Bóveda de Seguridad MA-SAD-002 Manual para el control de acceso y permanencia en las instalaciones del FNG - Cap. 4.7. Sobre el ingreso a áreas restringidas MA-SAD-002 Manual para el control de acceso y permanencia en las instalaciones del FNG - Cap. 3, Políticas Generales MA-SAD-002 Manual para el control de acceso y permanencia en las instalaciones del FNG - Cap. 3, Políticas Generales
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	SI	El FNG cuenta con diferentes controles de acceso físicos y los ha establecido de manea formal.	MA-SAD-002 Manual para el control de acceso y permanencia en las instalaciones del FNG - Cap. 4.9.2 Personal autorizado para el accesso a la Bóveda de Seguridad MA-SAD-002 Manual para el control de acceso y permanencia en las instalaciones del FNG - Cap. 4.7. Sobre el ingreso a áreas restringidas MA-SAD-002 Manual para el control de acceso y permanencia en las instalaciones del FNG - Cap. 3, Políticas Generales MA-SAD-002 Manual para el control de acceso y permanencia en las instalaciones del FNG - Cap. 3, Políticas Generales
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	El FNG cuenta con planes de emergencia, pólicas de seguro y otros controles para garantizar su protección contra amenazas externas, algunas derivadas de la ubicación física de la entidad.	PD-GTE-009 - Mantenimiento de Equipos PD-GTE-009 - Mantenimiento de Equipos PD-GTE-009 - Mantenimiento de Equipos PD-GTE-009 - Mantenimiento de Equipos Pólizas MA-GDO-003 Programa de Gestión Documental - Cap. - 2.6.3. Lineamientos c) Condiciones Ambientales. Manual del Plan de continuidad de Negocio
A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras	SI	El FNG cuenta con áreas seguras	MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 22.1 Seguridad Física MA-SAD-002 Manual para el control de acceso y permanencia en las instalaciones del FNG. - Cap. 4.7. Sobre el ingreso a áreas restringidas MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática
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 para evitar acceso no autorizado.	SI	El FNG cuenta con áreas de despacho de correspondencia donde pueden entrar personas ajenas al negocio	MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 22.1 Control de acceso, Seguridad Física y del entorno MA-SAD-002 Manual para el control de acceso y permanencia en las instalaciones del FNG.- Cap. 4.9.3. Deberes del personal autorizado para el ingreso al Archivo Central y a la bóveda de seguridad. MA-GTE-010- Manual de Gestión tecnológica y seguridad informática.- Cap. 4.6.4.2. De los equipos de misión crítica:

Sección	Control	Descripción del Control	Aplica	Justificación Desde el Negocio	Justificación de la Inclusión
A.11.2	Equipos		Cumplimiento		Documentos
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	El FNG define de manera cuidadosa donde se ubicaran los equipos que se requieren para la operación	MA-GTE-010- Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.4.1. De los aspectos generales de instalación y ubicación de equipos de cómputo PO-GTE-009 - Mantenimiento de Equipos PO-GTE-009 - Mantenimiento de Equipos PO-GTE-009 - Mantenimiento de Equipos PO-GTE-009 - Mantenimiento de Equipos
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	Por Requisitos del Negocio Por operaciones criticas del Negocio	MA-GRI-003 Manual del plan de continuidad del negocio. PL-GHU-001 Plan de emergencias PO-GTE-009 - Mantenimiento de Equipos
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	Por Requisitos del Negocio Por operaciones criticas del Negocio	PO-GTE-009 - Mantenimiento de Equipos
A.11.2.4	Mantenimiento de equipos	Lo equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	SI	El FNG requiere que los equipos estén siempre en condiciones óptimas para poder cumplir con las actividades del negocio	PO-GTE-009 - Mantenimiento de Equipos MA-GRI-003 Manual del plan de continuidad del negocio. PL-GHU-001 Plan de emergencias PO-GTE-009 - Mantenimiento de Equipos PO-GTE-009 - Mantenimiento de Equipos PO-GTE-009 - Mantenimiento de Equipos PO-GTE-009 - Mantenimiento de Equipos PO-SAD-002 - Administración de Activos Fijos Contrato de Garantía de infraestructura
A.11.2.5	Retiro de activos	Los equipos información o software no se deben retirar de su sitio sin autorización previa	SI	El FNG ha centralizado la autorización de retirar activos físicos o tecnológicos de su sitio	MA-GTE-010 Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.5.3. Del retiro de equipos de las instalaciones del FNG.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	SI	En el FNG hay actividades que requieren que los funcionarios saquen los equipos y activos de las instalaciones	MA-GTE-010 Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.8.1. De la seguridad y uso adecuado de los equipos propiedad del FNG
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 reuso.	SI	Existen procedimientos para disponer de los medios cuando se reúsen o ya no se requieran	IN-GTE-014 Borrado de información Equipo de Escritorio Contrato de Custodia de Medios Magnéticos
A.11.2.8	Equipos de usuario desatendido	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	SI	Por las condiciones de trabajo se pueden presentar momentos en que los equipos estén desatendidos.	MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 24.1 Política Puesto de Trabajo Limpio y Pantalla Segura.
A.11.2.9	Política 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	Por Requisitos del Negocio Por operaciones criticas del Negocio	MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 24.1 Política Puesto de Trabajo Limpio y Pantalla Segura.
A.12	SEGURIDAD DE LAS OPERACIONES				
A.12.1	Procedimientos operaciones y responsabilidades		Cumplimiento		Documentos
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	El FNG ha documentado todos los procedimientos de operación para la seguridad de la información y los ha dispuesto para su consulta en la intra e internet de la entidad	PO-GDO-ECD-005 Elaboración y control de documentos Registros y documentación del SGI en ISOLUCION.
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	Por Requisitos del Negocio Por operaciones criticas del Negocio	PO-GTE-014 Administración de Cambio MA-GQU-001 Manual del sistema de Gestión Integrado - Cap. 12 Gestión de Cambios MA-GTE-003 Metodología Ciclo de Vida del Desarrollo de Software -Cap. 8 Seguridad de la Información
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	Debido a que el core del negocio depende de la capacidad que asegure el desempeño de los sistemas	MA-GQU-001 Manual del sistema de Gestión Integrado - Cap. 25.3 Gestión de la capacidad / Stretch Factor MA-GTE-010 Manual de Gestión tecnológica y seguridad informática - Cap. 4.5 Adquisición de Hardware y Software PETI Contrato de Garantía de infraestructura
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	En el FNG se gestionan actividades asociadas a desarrollo.	PO-GTE-014 Administración de Cambio MA-GQU-001 Manual del sistema de Gestión Integrado - Cap. 27.1 Desarrollo seguro MA-GTE-003 Ciclo de Vida del Desarrollo de Software -Cap. 5 Esquema de Desarrollo del Software
A.12.2	Protección contra códigos maliciosos		Cumplimiento		Documentos
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	Por Requisitos del Negocio Por operaciones criticas del Negocio Por Actividades de operación tecnológica que hacen parte del core del negocio.	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.13. De la Administración de la Seguridad PO-GTE-ASE-005 Administración de seguridad MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. - 4.6.13.1 De los Servicios Tecnológicos..
A.12.3	Copias de Respaldo		Cumplimiento		Documentos
A.12.3.1	Respaldo de la información	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	SI	Por Requisitos del Negocio Por operaciones criticas del Negocio Por Actividades de operación tecnológica que hacen parte del core del negocio.	PO-GTE-RRI -010 Respaldo y Recuperación de la información PO-GTE-RRI -010 Respaldo y Recuperación de la información PO-GTE-RRI -010 Respaldo y Recuperación de la información MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 25.5 Copias de Respaldo PO-GTE-RRI -010 Respaldo y Recuperación de la información IN-GTE-011 Validar copias de respaldo MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.7 Del almacenamiento y respaldo de la información
A.12.4	Registro y seguimiento		Cumplimiento		Documentos
A.12.4.1	Registro de eventos	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	SI	El FNG garantiza la trazabilidad de las operaciones realizadas en las aplicaciones físicas	PO-GTE-GDL-018 Gestión de Logs IN-GTE-030 Instructivo Generación de reportes de registro de eventos (Logs)
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	El FNG garantiza la trazabilidad de las operaciones realizadas en las aplicaciones físicas	MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 25.6 Registro y Seguimiento. IN-GTE-030 Instructivo Generación de reportes de registro de eventos (Logs) MA-SAD-002 Manual para el control de acceso y permanencia en las instalaciones del FNG. MA-GRI -004 Manual de la bases de datos del SARG
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	El FNG garantiza la trazabilidad de las operaciones realizadas en las aplicaciones físicas	PO-GTE-GDL-018 Gestión de Logs Módulo FI Contabilidad y TR de Tesorería MA-GTE-010 Manual de Gestión Tecnológica y seguridad informática - Cap. 4.6.7.3 Registros (log) del administrador y del Operador
A.12.4.4	Sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	SI	El FNG garantiza la trazabilidad de las operaciones realizadas en las aplicaciones físicas	MA-GQU-001 - Manual del sistema de Gestión Integrado Cap. 16.7.7- Registro de Eventos y Seguimiento. IN-GTE-002 Sincronización Horario de los Sistemas
A.12.5	Control de software operacional		Cumplimiento		Documentos
A.12.5.1	Instalación de software en sistemas operativos	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	SI	El FNG ha centralizado la autorización de hacer uso de programas utilitarios y de instalación de software con el fin de garantizar la seguridad de la información	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.3.1.2 Políticas de software MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.3.1.2 Políticas de software
A.12.6	Gestión de la vulnerabilidad técnica		Cumplimiento		Documentos
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debe 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	Debido a que el core del negocio depende de la capacidad que asegure el desempeño de los sistemas	PO-GTE-ASE-005 Administración de seguridad PO-GTE-ASE-005 Administración de seguridad PO-GTE-ASE-005 Administración de seguridad
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	El FNG ha centralizado la autorización de hacer uso de programas utilitarios y de instalación de software con el fin de garantizar la seguridad de la información	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.3.1.2 Políticas de software PO-GTE-ISP-013 Instalación de Service Pack
A.12.7	Consideraciones sobre autoridades de sistemas de información		Cumplimiento		Documentos
A.12.7	Controles de auditorías de sistemas de información	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	SI	El FNG debe cumplir los requisitos de auditoría exigidos para las auditorías de gestión y las auditorías internas a sistemas de gestión	PO-DSP-002 - Auditorías de Gestión al Sistema de Control Interno. Informe de auditoría de certificación

Sección	Control	Descripción del Control	Aplica	Justificación Desde el Negocio	Justificación de la Inclusión
A.13	**Seguridad de las Comunicaciones**				
A.13.1	**Gestión de la seguridad de las redes**		**Cumplimiento**		**Documentos**
A.13.1.1	**Controles de redes**	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones	SI	Por Requisitos del Negocio Por operaciones criticas del Negocio	PD-GTE-008 Procedimiento de Administración de la Infraestructura de redes y comunicaciones
					MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática, - Cap. 4.6.3 Del acceso a la Red, - Cap. 4.6.11 De la segregación de la red, - Cap. 4.6.10 De la utilización de los recursos de Red
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 de red, ya sea que los servicios se presenten internamente o se contraten externamente.	SI	Por Requisitos del Negocio Por operaciones criticas del Negocio	PD-GTE-008 Procedimiento de Administración de la Infraestructura de redes y comunicaciones
					Contrato de Garantía de infraestructura
					MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Registro de eventos
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	Por Requisitos del Negocio Por operaciones criticas del Negocio	PD-GTE-008 Procedimiento de Administración de la Infraestructura de redes y comunicaciones
					MA-GTE-010 - Manual de Gestión Tecnológica y seguridad informática - Cap. 4.6.11 De la segregación de la red
A.13.2	**Transferencia de información**		**Cumplimiento**		**Documentos**
A13.2.1	**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	El FNG realiza operaciones de transferencia de información con sus usuarios	Reglamento de Garantías - Protocolo de comunicaciones
A13.2.2	**Acuerdos sobre transferencia de información.**	Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	SI	El FNG realiza operaciones de transferencia de información con sus usuarios	Reglamento de Garantías
A13.2.3	**Mensajería electrónica**	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	SI	El FNG utiliza mensajería electrónica	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática- Cap. 4.6.2. Del uso de los controles criptográficos, - Cap. 4.6.6.3 Cuenta de Correo
					IN-GTE-025 Envío y visualización de correos encriptados
A13.2.4	**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	Por las características del negocio y considerando que la información es vital para todos los cargos se han definido condiciones contractuales con las responsabilidades sobre el uso de la información. Esto aunado a las exigencias y responsabilidades que establece el AGN	MA-GCT -01 - Manual de Contratación - Cap. 3.9.1 Clausulas Generales de los contratos
					FR-GHU-019 Contrato de Trabajo
					Reglamento interno de trabajo
A.14	**Adquisición, desarrollo y mantenimiento de sistemas**				
A.14.1	**Requisitos de seguridad de los sistemas de información**		**Cumplimiento**		**Documentos**
A.14.1.1	**Análisis 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	Por Requisitos del Negocio Por operaciones criticas del Negocio	MA-GTE-003 - Metodología Ciclo de Vida del Desarrollo de Software - Cap. 8 Seguridad de la Información
					PD-GTE-AOC-014 Administración de cambios
					MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 27.1 Desarrollo Seguro
A.14.1.2	**Seguridad de servicios de las aplicaciones en redes publicas.**	La información involucrada en los servicios de las aplicaciones que pasan sobre redes publicas se deba proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	SI	Por Requisitos del Negocio Por operaciones criticas del Negocio	MA-GTE-010 Manual de Gestión tecnológica y seguridad Informática. - Cap. 4.6.2. Del uso de los controles criptográficos
					PD-GTE- 005 Procedimiento Administración de seguridad
					PD-GTE- 005 Procedimiento Administración de seguridad
					MA-GTE-010 Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.13.2 De la seguridad de los servicios tecnológicos
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 debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizada.	SI	Por Requisitos del Negocio Por operaciones criticas del Negocio	Reglamento de Garantías - Protocolo de comunicaciones
A.14.2	**Seguridad en los procesos de desarrollo y de soporte**		**Cumplimiento**		**Documentos**
A.14.2.1	**Política 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	En el FNG se gestionan actividades asociadas a desarrollo.	MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 27.1 Desarrollo Seguro
					MA-GTE-003 - Metodología Ciclo de Vida del Desarrollo de Software.
					PD-GTE-016 Gestión de incidentes, cambios y mejoras
A.14.2.2	**Procedimientos 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	En el FNG se gestionan actividades asociadas a desarrollo.	PD-GTE-016 Gestión de incidentes, cambios y mejoras
					MA-GTE-003 Metodología Ciclo de Vida del Desarrollo de Software - Cap. 3.2.2 Elaboración de la historia de usuario o especificación funcional
A.14.2.3	**Revisión técnica de las aplicaciones despues de cambios en la plataforma de operación.**	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones criticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	SI	En el FNG se gestionan actividades asociadas a desarrollo.	MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 27.1 Desarrollo Seguro
					PD-GTE-016 Gestión de incidentes, cambios y mejoras
					MA-GTE-003 - Metodología Ciclo de Vida del Desarrollo de Software - Cap. 3.2.5 Pruebas
A.14.2.4	**Restricciones 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	En el FNG se gestionan actividades asociadas a desarrollo.	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.12.5 Gestión de Cambios
					MA-GTE-003 - Metodología Ciclo de Vida del Desarrollo de Software
					PD-GTE-AOC-014 Administración de Cambios
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	En el FNG se gestionan actividades asociadas a desarrollo.	MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 27.1 Desarrollo Seguro
A.14.2.6	**Ambiente de desarrollo seguro**	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	En el FNG se gestionan actividades asociadas a desarrollo.	MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 27.1 Desarrollo Seguro
					MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 27.1 Desarrollo Seguro
					MA-GTE-003 - Metodología Ciclo de Vida del Desarrollo de Software - Cap. 3.2.5 Pruebas
					MA-GTE-003 - Metodología Ciclo de Vida del Desarrollo de Software
					MA-GTE-003 - Metodología Ciclo de Vida del Desarrollo de Software - Cap. 3.2.5 Pruebas
					PD-GTE-014 Administración de Cambios
A.14.2.7	**Desarrollo contratado externamente**	La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	SI	En el FNG se gestionan actividades asociadas a desarrollo.	PD-GCT-ECT-018 Ejecución de Contratos
					MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 3.3 Gestión de Proveedores
					MA-GTE-003 - Metodología Ciclo de Vida del Desarrollo de Software - Cap. 3.2.4.1 Desarrollo externo de software
A.14.2.8	**Pruebas de seguridad de sistemas**	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de seguridad.	SI	En el FNG se gestionan actividades asociadas a desarrollo.	MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 27.1 Desarrollo Seguro
					MA-GTE-003 - Metodología Ciclo de Vida del Desarrollo de Software - Cap. 3.2.5 Pruebas
					PD-GTE-ICM-016 Gestión de incidentes cambios y mejoras.
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	En el FNG se gestionan actividades asociadas a desarrollo.	PD-GTE-ICM-016 Gestión de incidentes cambios y mejoras.
					Reglamento de Garantías
A.14.3	**Datos de prueba**		**Cumplimiento**		**Documentos**
A.14.3.1	**Protección de datos de prueba**	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	SI	En el FNG se gestionan actividades asociadas a desarrollo.	MA-GTE-003 Metodología Ciclo de Vida del Desarrollo de Software
A.15	**Relaciones con los proveedores**				
A.15.1	**Seguridad de la información en las relaciones con los proveedores**		**Cumplimiento**		**Documentos**
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 estos y se deben documentar.	SI	El FNG mantiene relaciones contractuales con proveedores que tienen acceso a los activos de la organización	MA-GTC-001 - Manual de Contratación
					MA-GTC-001 - Manual de Contratación
					MA-GTC-001 - Manual de Contratación
					Pólizas
					PD-GCT-ECT-018 Ejecución de Contratos
					PD-GCT-ECT-018 Ejecución de Contratos
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	El FNG mantiene relaciones contractuales con proveedores que tienen acceso a los activos de la organización	MA-GTC-001 - Manual de Contratación
					MA-GTC-001 - Manual de Contratación
					Pólizas
					PD-GCT-ECT-018 Ejecución de Contratos
					PD-GCT-ECT-018 Ejecución de Contratos
					Contrato con proveedores
					Contrato - Matriz de riesgos de contratación
A.15.1.3	**Cadena de suministro de tecnología de información y comunicación**	Los acuerdos con los 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	El FNG mantiene relaciones contractuales con proveedores que tienen acceso a los activos de la organización	MA-GTC-001 - Manual de Contratación
					MA-GTE-003 Metodología Ciclo de Vida del desarrollo de software - Seguridad de la información
					MA-SJU-001 Manual de políticas para el tratamiento de datos personales del FNG
					Contrato - Matriz de riesgos de contratación

Sección	Control	Descripción del Control	Aplica	Justificación Desde el Negocio	Justificación de la Inclusión
A.15.2	Gestión de la prestación de servicios de proveedores		Cumplimiento		Documentos
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	SI	proveedores que tienen acceso a los activos de la organización	PO-GCT-ECT-018 Ejecución de Contratos
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	El FNG mantiene relaciones contractuales con proveedores que tienen acceso a los activos de la organización	MA-GTC-001 - Manual de Contratación PO-GCT-ECT-018 Ejecución de Contratos MA-GTC-001 - Manual de Contratación
A.16	Gestión de incidentes de seguridad de la información.				
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información.		Cumplimiento		Documentos
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	El FNG cumple con directrices de las autoridades relacionadas con el reporte de eventos de riesgo operativo	MA-GQU-004 - Manual de Gestión de Incidentes de Seguridad de la Información PO-GTE-ICM-016 Gestión de Incidentes, Cambios y Mejoras PO-GQU-003 - Atención a incidentes de Seguridad de la Información
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	El FNG cumple con directrices de las autoridades relacionadas con el reporte de eventos de riesgo operativo	
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	El FNG cumple con directrices de las autoridades relacionadas con el reporte de eventos de riesgo operativo	
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 decidir si se van a clasificar como incidentes de seguridad de la información.	SI	El FNG cumple con directrices de las autoridades relacionadas con el reporte de eventos de riesgo operativo	
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 los procedimientos documentados.	SI	El FNG cumple con directrices de las autoridades relacionadas con el reporte de eventos de riesgo operativo	
A.16.1.6	Aprendizaje obteniendo 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	El FNG cumple con directrices de las autoridades relacionadas con el reporte de eventos de riesgo operativo	
A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	SI	El FNG cumple con directrices de las autoridades relacionadas con el reporte de eventos de riesgo operativo	
A.17	Aspectos de Seguridad de la información de la Gestión de Continuidad de Negocio				
A.17.1	Continuidad de seguridad de la información		Cumplimiento		Documentos
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 información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.	SI	El FNG ha definido un plan de continuidad del negocio para restablecer la operación crítica en situación de crisis	PO-GTE-RRI-010 Respaldo y Recuperación de la información Estrategias de contingencias tecnológicas. MA-GRI-003 - Manual del Plan de Continuidad del Negocio Contrato con Datacenter PL-GHU-001 - Plan de Emergencias del FN
A.17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	SI	El FNG ha definido un plan de continuidad del negocio para restablecer la operación crítica en situación de crisis	MA-GRI-003 - Manual del Plan de Continuidad del Negocio PL-GRI-002 Plan de recuperación de TI PL-GHU-001 - Plan de Emergencias del FN
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 validos y eficaces durante situaciones adversas.	SI	El FNG ha definido un plan de continuidad del negocio para restablecer la operación crítica en situación de crisis	MA-GRI-003 - Manual del Plan de Continuidad del Negocio Contrato con Datacenter MA-GRI -003 - Manual del Plan de Continuidad del Negocio
A.17.2	Redundancias		Cumplimiento		Documentos
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	Por Requisitos del Negocio Por operaciones criticas del Negocio	MA-GRI -003 - Manual del Plan de Continuidad del Negocio Estrategias de contingencias tecnológicas. BIA
A.18	Cumplimiento				
A.18.1	Cumplimiento de requisitos legales y contractuales		Cumplimiento		Documentos
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	Por Requisitos Legales y Contractuales	PO-SJU-RAN-005 Revisión y Actualización de Normas Relacionadas con el Objeto Social del FNG Normograma FNG Circulares normativas y Resoluciones FNG. PO-SJU-RAN-005 Revisión y Actualización de Normas Relacionadas con el Objeto Social del FNG . MA-GFI-001 Manual de Políticas contables PO-SJU-ECJ-003 Emisión de conceptos Jurídicos PO-SJU-RAN-005 Revisión y Actualización de Normas Relacionadas con el Objeto Social del FNG .
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	Por Requisitos Legales y Contractuales	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.4 Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática Cap. 4.6.12.4 Del uso del Software Propiedad de la entidad. MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.13.2. De la seguridad de los servicios tecnológicos.
A.18.1.3	Protección de registros	Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos de reglamentación contractuales y de negocio.	SI	Por Requisitos Legales y Contractuales	PO-AGA-FAC-004 Facturación IN-AGA-040 Validaciones proceso de facturación PO-AGA-FAC-004 Facturación IN-AGA-040 Validaciones proceso de facturación MA-SCL-003 Manual de Políticas Casos Excepcionales PO-AGA-RLA-020 Reclamación, liquidación y aprobación para pago de garantías IN-AGA-014 Validaciones calidad de datos PO-GCO-VCC-006 Vinculación y conocimiento de clientes MA-SAD-002 Manual para el control de acceso y permanencia en las instalaciones del FNG MA-GHU-007 Manual Específico de Funciones y Competencias Laborales PO-GFI-ACH-019 Administración de cheques MA-GFI-003 Manual de Caja y Bancos PO-GFI-ACH-019 Administración de cheques MA-GFI-003 Manual de Caja y Bancos TR-GDO-010 Diligencias Subdirección Operaciones de tesorería MA-GFI-003 Manual de Caja y Bancos MA-GDO-003 Programa Gestión Documental PO-GDO-CPA-012 Consulta y préstamo de archivos PO-GDO-CPA-012 Consulta y préstamo de archivos PO-GDO-CPA-012 Consulta y préstamo de archivos PO-GDO-CPA-012 Consulta y préstamo de archivos MA-GFI-003 Manual de Caja y Bancos PO-GME-CPE-028 Creación de programas especiales MA-GFI-003 Manual de Caja y Bancos Carta de Instrucciones de los bancos MA-GPO-001 Manual de Operaciones de Tesorería - Cap 2.2.3 Grabación de Llamadas PO-GTE-GVL-012 Grabación y verificación de llamadas MA-GPO-001 Manual de Operaciones de Tesorería TR-GPO-009 Acta de arqueo diario Portafolio de Inversiones TR-GPO-010 Acta de arqueo mensual Portafolio de Inversiones PO-GRI-SRM-034 Seguimiento y control de riesgo de mercado PO-SCL-LMD-007 Liquidación de mandatos

Sección	Control	Descripción del Control	Aplica	Justificación Desde el Negocio	Justificación de la Inclusión
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	Por Requisitos Legales y Contractuales	MA-SJU-001 Manual de políticas para el tratamiento de datos personales del FNG
					PD-GDO-CPA-012 Consulta y préstamo de archivos
					PD-GDO-CPA-012 Consulta y préstamo de archivos
					Procedimientos de Bienes y servicios
					MA-SAD-002 Manual para el control e acceso y permanencia en las instalaciones del FNG
					FR-GHU-071 Documentos de ingreso y autorización Tratamiento de datos personales
					FR-GHU-019 Contrato de trabajo
					MA-SJU-001 Manual de políticas para el tratamiento de datos personales del FNG
A.18.1.5	Reglamentación de controles criptográficos	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	SI	Por Requisitos del Negocio Por operaciones criticas del Negocio Por Actividades de operación tecnológica que hacen parte del core del negocio. Por Requisitos del Negocio y Alineación con los procesos del negocio.	MA-GTE-010 - Manual de Gestión tecnológica y seguridad informática - Cap. 4.6.2 Del uso de los controles criptográfico
A.18.2	**Revisiones de seguridad de la información**		**Cumplimiento**		**Documentos**
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 significativos.	SI	El FNG cuenta con procesos formales de auditoria a la gestión de la entidad	MA-GQU-001 - Manual del sistema de Gestión Integrado - Cap. 17 Medición Análisis y Mejora.
					PD-ESP-AIS-001 Auditorias Internas al Sistema de Gestión Integrado
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	Por direccionamiento estratégico del FNG, Alineación con los Procesos corporativos , lineamientos del gobierno, GEL, Conpes 3854- Política Nacional de Seguridad Digital.	MA-GQU-001 - Manual del sistema de Gestión Integrado- Cap 18 Seguridad de la información
					MA-ESP-004 Manual de Auditoria
					MA-ESP-002 Código de Ética de la Oficina de Control Interno
					MA-ESP-003 Estatuto de Auditoria Interna de la Oficina de Control Interno
					PD-ESP-AIS-001 Auditorias Internas al Sistema de Gestión Integrado
A.18.2.3	Revisión del cumplimiento técnico	Los sistema de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	SI	Por direccionamiento estratégico del FNG, Alineación con los Procesos corporativos , lineamientos del gobierno, GEL, Conpes 3854- Política Nacional de Seguridad Digital.	PD-GTE-ASE-005 Administración de Seguridad
					PD-ESP-AIS-001 Auditorias Internas al Sistema de Gestión Integrado
					Informe de auditoria de certificación
					PD-ESP-AIN-002 Auditorias de Gestión al Sistema de Control Interno
					MA-GHU-007 Manual de Funciones