MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	DECLARACIÓN DE APLICABILIDAD	SOMOSIG Sistema Integrado de Gestión
	Gestión Estratégica de Tecnologías de la información	
Versión: 1	**Vigencia:** 18/07/2024	**Código:** DS-E-GET-36

NOTA: RL: Requerimientos Legal, **OC**: Obligaciones Contractuales, **RN/MP**: Requerimientos del negocio/Mejores Practicas, **RER**: Resultados Evaluación de Riesgos

CONTROLES ISO 27001			CONTROLES ACTUALES	CUMPLE	EXCLUSION	Justificación de inclusión	Selección Controles y Razón de la selección				Comentario / Descripción General del Control	EVIDENCIAS
				SI/NO	SI/NO		RL	OC	RN/MP	RER		
CLAUSULA	Sec	Objetivo de Control										
	A.5	POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN										
5. Políticas de Seguridad de la Información	A.5.1	DIRECTRICES ESTABLECIDAS POR LA DIRECCIÓN PARA LA SEGURIDAD DE LA INFORMACION	**Objetivo: : Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.**									
	A.5.1.1	Políticas de Seguridad de la Información.	**Control** **Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.**	SI	NO	Se adopta este control, puesto que es necesario la definición de políticas de Seguridad de la Información, las cuales deben ser aprobadas, publicadas y comunicadas a los funcionarios, contratistas y terceras partes interesadas.	X		X		**Solicite la política de seguridad de la información de la entidad y evalúe:** **a) Si se definen los objetivos, alcance de la política** **b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad** **c) Si fue debidamente aprobada y socializada al interior de la entidad por la alta dirección** **Revise si la política:** **a)Define que es seguridad de la información** **b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos;** **c) Los procesos para manejar las desviaciones y las excepciones.** **Indague sobre los responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas.** **Verifique cada cuanto o bajo que circunstancias se revisan y actualizan, verifique la ultima fecha de emisión de la política frente a la fecha actual y que cambios a sufrido, por lo menos debe haber una revisión anual.**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información DS-E-GET-01 Política de Tratamiento y Protección de Datos personales
	A.5.1.2	Revisión de las Política de Seguridad de la Información.	**Control** **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 continúas.**	SI	NO	Se adopta este control, puesto que las políticas se deben revisar a intervalos planificados, o si ocurren cambios significativos asegurando su conveniencia, adecuación y mejora continua.	X		X			M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información DS-E-GET-01 Política de Tratamiento y Protección de Datos personales
	A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN										
6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	A.6.1	ORGANIZACIÓN INTERNA	**Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.**									
	A.6.1.1	Roles y responsabilidades para la seguridad de la información.	**Control** **Se deben definir y asignar todas las responsabilidades de la seguridad de la información.**	SI	NO	Se adopta este control, puesto que la asignación de responsabilidades de seguridad de la información se deben asignar de acuerdo con las políticas.	X	X	X		**verifique si 1) los roles y responsabilidades frente a la ciberseguridad han sido establecidos 2) los roles y responsabilidades de seguridad de la información han sido coordinados y alineados con los roles internos y las terceras partes externas 3) Los a) proveedores, b) clientes, c) socios, d) funcionarios, e) usuarios privilegiados, f) directores y gerentes (mandos senior), g) personal de seguridad física, h) personal de seguridad de la información entienden sus roles y responsabilidades, i) Están claros los roles y responsabilidades para la detección de incidentes.** **Solicite el acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o e que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección.** **Revise la estructura del SGSI:** **1) Tiene el SGSI suficiente apoyo de la alta dirección?, esto se ve reflejado en comités donde se discutan temas como la política de SI, los riesgos o incidentes.** **2) Están claramente definidos los roles y responsabilidades y asignados a personal con las competencias requeridas?,** **3) Están identificadas los responsables y responsabilidades para la protección de los activos? (Una práctica común es nombrar un propietario para cada activo, quien entonces se convierte en el responsable de su protección)** **4) Están definidas las responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales?** **5) Están definidos y documentados los niveles de autorización?** **6) Se cuenta con un presupuesto formalmente asignado a las actividades del SGSI (por ejemplo campañas de sensibilización en seguridad de la información)**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información F-A-ATH-30 Ajustes al Manual de Funciones F-E-GET-18 Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE G-E-SIG-05 Guía de administración del riesgo
	A.6.1.2	Separación de deberes.	**Control** **Las funciones 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	NO	Se adopta este control, puesto que ningún funcionario, contratista, tercero o persona pueda acceder, modificar o usar activos de información sin autorización del propietario.	X	X	X		**Indague como evitan que una persona pueda acceder, modificar o usar activos sin autorización ni detección. La mejor práctica dicta que el inicio de un evento deber estar separado de su autorización. Al diseñar los controles se debería considerar la posibilidad de confabulación. Tenga en cuenta que para las organizaciones pequeñas la separación de deberes puede ser difícil de lograr, en estos casos se deben considerar controles compensatorios como revisión periódica de los rastros de auditoría y la supervisión de cargos superiores.**	M-E-GET-04 Manual de políticas específicas de Seguridad de la Información. I-E-GET-02 Metodología para la identificación gestión y clasificación de activos de información F-E-GET-18 Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE * Directorio Activo, Usuarios categorizados en aplicaciones mediante perfiles (administrador de sistema, administrador funcional, usuario final).
	A.6.1.3	Contacto con las Autoridades.	**Control** **Se deben mantener contactos apropiados con las autoridades pertinentes.**	SI	NO	Se adopta este control, puesto que es necesario especificar cuando contactar a las autoridades y la manera de reportar de forma oportuna los incidentes de seguridad de la información.	X		X		**Solicite los procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debería contactar a las autoridades, verifique si de acuerdo a estos procedimientos se han reportado eventos o incidentes de SI de forma consistente.**	DS-E-GET-03 Contacto con Autoridades y Grupos de Interés M-E-GET-04 Manual de políticas específicas de Seguridad de la Información. P-A-GTI-09 Gestión de incidentes de seguridad y privacidad de la información G-A-ATH-03 Plan de emergencias y contingencias.
	A.6.1.4	Contacto con Grupos de Interés Especiales.	**Control** **Se debería mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.**	SI	NO	Se adopta este control, puesto que es necesario el contacto con grupos de interés para mejorar el conocimiento y mejores prácticas en seguridad, recibir advertencias tempranas de alertas y parches de seguridad, intercambiar información y gestionar incidentes de seguridad.	X		X		**Pregunte sobre las membrecías en grupos o foros de interés especial en seguridad de la información en los que se encuentran inscritos las personas responsables de la SI.**	DS-E-GET-03 Contacto con Autoridades y Grupos de Interés M-E-GET-04 Manual de políticas específicas de Seguridad de la Información. El Ministerio cuenta con información actualizada de temas de Seguridad de la Información mediante la suscripción a páginas especializadas en seguridad, adicionalmente cuenta con el apoyo del Ministerio de Tecnologías de la Información y Comunicaciones, el Comando Conjunto Cibernético adscrito al Comando General de las Fuerzas Militares, ISC2 Capítulo Colombia. Con el fin de mantener una actualización constante se ha dispuesto de un correo electrónico institucional para la recepción constante de información, buenas prácticas y posibles nuevas amenazas.
	A.6.1.5	Seguridad de la Información en la gestión de proyectos.	**Control** **La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.**	SI	NO	Se adopta este control, puesto que la seguridad de la información se debe integrar en la gestión de proyectos de la Entidad, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto.			X		**Pregunte como la Entidad integra la seguridad de la información en el ciclo de vida de los proyectos para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto. Tenga en cuenta que esto no solamente aplica para proyectos de TI, por ejemplo puede aplicar en proyectos de traslado de activos de información, gestión de instalaciones, personal en outsourcing que soporta procesos de la organización.** **Las mejores prácticas sugieren:** **a) Que los objetivos de la seguridad de la información se incluyan en los objetivos del proyecto;** **b) Que la valoración de los riesgos de seguridad de la información se lleve a cabo en una etapa temprana del proyecto, para identificar los controles necesarios;** **c) Que la seguridad de la información sea parte de todas las fases de la metodología del proyecto aplicada.**	P-E-GET-12 Gestionar Proyectos de TI P-A-GTI-03 Desarrollar y Mantener Sistemas de Información y Componentes de Software I-A-GTI-03 Instructivo Para la Elaboración de Arquitecturas de Software
	A.6.2	DISPOSITIVOS MÓVILES Y TELETRABAJO	**Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.**									
	A.6.2.1	Política para dispositivos móviles.	**Control** **Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.**	SI	NO	Se adopta este control, puesto que es necesario asegurar la información de la Entidad cuando se usan dispositivos móviles y se tiene en cuenta los posibles riesgos en entornos no protegidos o controlados.			X	X	**a) El registro de los dispositivos móviles; Se realiza el registro de los dispositivos móviles mediante la validación y control de inventarios de TI de la entidad.** **b) La protección física se encuentra a cargo del grupo de servicios administrativos, mediante la aplicación de controles físicos tales como: sistema de videovigilancia, controles de ingresos y salidas físicas, contratos de vigilancia, entre otros.** **c) Se generan restricciones para la instalación de software por medio de la aplicación de las políticas en el directorio activo en los equipos de la entidad.** **d) Requisitos para las versiones de software de dispositivos móviles y para aplicar parches de conformidad con lo sugerido por el fabricante de las soluciones tecnológicas.** **e) Restricción de la conexión a servicios de información por medio de las restricciones de seguridad aplicadas para los diferentes perfiles de usuarios.** **f) Controles de acceso por medio de la aplicación de las políticas en el directorio activo.** **g) Se deben fortalecer las técnicas criptográficas mediante las herramientas existentes.** **h) protección contra software malicioso con la gestión del antivirus y el sistema de seguridad perimetral.** **i) des habilitación remota, borrado o cierre por medio de la aplicación de las políticas en el directorio activo.** **j) Las copias de respaldo se generan de acuerdo con el plan establecido y adoptado por la entidad.** **k) uso de servicios y aplicaciones web con sus respectivas políticas de seguridad.** **Uso de dispositivos móviles de propiedad personal:** **a) La separación entre el uso privado y de la Entidad de los dispositivos, incluido el uso del software para apoyar esta separación y proteger los datos del negocio en un dispositivo privado con la aplicación de las políticas específicas de seguridad de la información.** **b) Brindar acceso a la información de la Entidad solo cuando los usuarios hayan firmado un acuerdo de usuario final, en el que se reconocen sus deberes (protección física, actualización del software, etc.), desistir de la propiedad de los datos de la Entidad, permitir el borrado remoto de datos por parte de la organización en caso de robo o pérdida del dispositivo, o cuando ya no se posee autorización para usar el servicio. Se tienen acuerdos de confidencialidad; no obstante, es importante tener en cuenta que se presenta debilidad en la aplicación de los controles para realizar el borrado remoto de datos.**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información M-A-GAC-01 Protocolo de seguridad Minambiente (Seguridad del física y del Entorno) M-A-GTI-02 MANUAL GENERAL DE OPERACIONES DE INFRAESTRUCTURA DE TI (ANEXO 5. Manual de operaciones de solución antivirus)

	A.6.2.2	**Teletrabajo.**	**Control:** **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	NO	Se adopta este control, puesto que se deben definir los lineamientos en seguridad de la información para el uso del teletrabajo.	X		X	**De conformidad con lo establecido en la Resolución 404 de 2016 con el cual la entidad implementa la modalidad suplementaria de Teletrabajo como una forma de organización laboral con el fin de mejorar las condiciones de vida, tanto laborales como personales de los servidores públicos.** **a) la seguridad física existente en el sitio del teletrabajo se valida con las inspecciones realizadas en conjunto con la ARL y la entidad para verificar las condiciones mínimas de seguridad en el lugar de teletrabajo.** **b) los requisitos de seguridad de las comunicaciones, teniendo en cuenta la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se tendrá acceso y que pasará a través del enlace de comunicación y la sensibilidad del sistema interno se controla mediante la asignación y monitoreo de la VPN.** **c) el suministro de acceso al escritorio virtual, que impide el procesamiento y almacenamiento de información en equipo de propiedad privada por medio de la asignación de la VPN.** **d) la amenaza de acceso no autorizado a información o a recursos, por parte de otras personas que usan el mismo equipo, por ejemplo, familia y amigos; es necesario validar la aplicación de este control.** **e) el uso de redes domésticas y requisitos o restricciones sobre la configuración de servicios de red inalámbrica; se valida con el análisis técnico realizado por el equipo de mesa de ayuda de la entidad.** **f) acuerdos de licenciamiento de software de tal forma que las organizaciones puedan llegar a ser responsables por el licenciamiento de software de los clientes en estaciones de trabajo de propiedad de los empleados o de usuarios externos; por medio de funcionalidades de Microsoft 365.** **g) requisitos de firewall y de protección contra software malicioso, se valida con el análisis técnico realizado por el equipo de mesa de ayuda de la entidad.** **Las directrices y acuerdos que se consideren deben incluir:** **h) Se validan y se usan los equipos tecnológicos a cargo del teletrabajador.** **i) una definición del trabajo permitido, las horas de trabajo, la clasificación de la información que se puede mantener, y los sistemas y servicios internos a los que el tele trabajador está autorizado a acceder; se definen en los acuerdos de voluntariedad firmados entre las dos partes.** **j) el suministro de equipos de comunicación adecuados, incluidos los métodos para asegurar el acceso remoto; que se garantizan con la habilitación de la VPN.** **l) la revocación de la autoridad y de los derechos de acceso, y la devolución de los equipos cuando las actividades del teletrabajo finalicen; que se validan por parte del equipo de mesa de ayuda de la entidad donde se revocan los permisos de acceso.**	Resolución 404 de 2016 con el cual la entidad implementa la modalidad suplementaria de Teletrabajo M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información M-A-GTI-02 Manual general de operaciones de infraestructura de TI M-A-GTI-02 MANUAL GENERAL DE OPERACIONES DE INFRAESTRUCTURA DE TI (ANEXO 5. Manual de operaciones de solución antivirus)
	A.7	**SEGURIDAD DEL RECURSO HUMANO**										
7. SEGURIDAD DEL RECURSO HUMANO	**A.7.1**	**ANTES DE ASUMIR EL EMPLEO**	**Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.**									
	A.7.1.1	**Selección.**	**Control** **Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos 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	NO	Se adopta este control, puesto que se debe tener en cuenta todo lo relacionado con la privacidad, seguridad y protección de la información de datos personales conforme la legislación laboral, contractual y demás aplicable.	X		X	**a) Referencias satisfactorias cuya validación se aplica desde el procedimiento P-A-ATH-08 Provisión de empleos (vinculación) y el F-A-ATH-32 formato de análisis cumplimiento de requisitos para nombramiento** **b) Verificación de la de la hoja de vida del solicitante incluyendo certificaciones académicas y laborales; se aplica desde el procedimiento P-A-ATH-08 Provisión de empleos (vinculación) y el F-A-ATH-32 formato de análisis cumplimiento de requisitos para nombramiento** **c) Confirmación de las calificaciones académicas y profesionales declaradas; se aplica desde el procedimiento P-A-ATH-08 Provisión de empleos (vinculación) y el F-A-ATH-32 formato de análisis cumplimiento de requisitos para nombramiento** **d) Una verificación de antecedentes penales. Cuando un individuo es contratado para un rol de seguridad de la información específico, las organizaciones deben asegurar que el candidato tenga la competencia necesaria para desempeñar el rol de seguridad; se aplica desde el procedimiento P-A-ATH-08 Provisión de empleos (vinculación) y el F-A-ATH-32 formato de análisis cumplimiento de requisitos para nombramiento** **e) sea confiable para desempeñar el rol, especialmente si es crítico para la organización, se aplica desde el procedimiento P-A-ATH-08 Provisión de empleos (vinculación) y el F-A-ATH-32 formato de análisis cumplimiento de requisitos para nombramiento** **f) Cuando un trabajo, ya sea una asignación o una promoción, implique que la persona tenga acceso a las instalaciones de procesamiento de información, y en particular, si ahí se maneja información confidencial, por ejemplo, información financiera o información muy confidencial, la organización debería también considerar verificaciones adicionales más detalladas, se asegura con la firma del F-A-CTR-36_Acta de confidencialidad e integridad de la información** **g) También se debería asegurar un proceso de selección para contratistas. En estos casos, el acuerdo entre la organización y el contratista debería especificar las responsabilidades por la realización de la selección, y los procedimientos de notificación que es necesario seguir si la selección no se ha finalizado, o si los resultados son motivo de duda o inquietud., mediante la F-A-CTR-28 Verificación de idoneidad y experiencia** **h) La información sobre todos los candidatos que se consideran para cargos dentro de la organización, se debería recolectar y manejar apropiadamente de acuerdo con la ley de protección de datos personales conforme a la DS-E-GET-01 Política de tratamiento y protección de datos personales.**	Se encuentra en: "C-A-ATH-01 caracterización de proceso de administración de Talento Humano" y " P-A-ATH-08 Procedimiento Vinculación y Desvinculación de Personal ". Procesos definidos en el Manual de Contratación del Ministerio de Ambiente y desarrollo Sostenible F-A-ATH-32 formato de análisis cumplimiento de requisitos para nombramiento F-A-CTR-36 Acta de confidencialidad e integridad de la información F-A-CTR-28 Verificación de idoneidad y experiencia DS-E-GET-01 Política de tratamiento y protección de datos personales.
	A.7.1.2	**Términos y condiciones de empleo.**	**Control** **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	NO	Se adopta este control, puesto que las obligaciones contractuales para funcionarios o contratistas deben reflejar el conocimiento y aplicabilidad de las políticas de seguridad de la información de la Entidad.	X		X	**Verificación de la de la hoja de vida del solicitante incluyendo certificaciones académicas y laborales; se aplica desde el procedimiento P-A-ATH-08 Provisión de empleos (vinculación) y el F-A-ATH-32 formato de análisis cumplimiento de requisitos para nombramiento** **Se genera mediante la firma del F-A-CTR-36_Acta de confidencialidad e integridad de la información.** **M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información** **Proceso de acuerdo a la ley y la normatividad vigente tanto para funcionarios como para contratistas, formatos y procedimientos de talento humano, resoluciones de secretaria general, manual de contratación formatos y procedimientos grupo de contratos.** **Manual de funciones, Minutas contractuales**	Se genera mediante la firma del F-A-CTR-36_Acta de confidencialidad e integridad de la información. P-A-ATH-08 Provisión de empleos (vinculación) y el F-A-ATH-32 formato de análisis cumplimiento de requisitos para nombramiento M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información
	A.7.2	**DURANTE LA EJECUCIÓN DEL EMPLEO**	**Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.**									
	A.7.2.1	**Responsabilidades de la dirección.**	**Control** **La dirección debería 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	NO	Se adopta este control, puesto que desde la dirección de la Entidad se debe exigir el cumplimiento de las políticas de seguridad de la información a funcionarios y contratistas.	X		X	**a) Los funcionarios y contratistas están debidamente informados sobre sus roles y responsabilidades de seguridad de la información, antes de que se les otorgue el acceso a información o sistemas de información confidenciales, cuya información esta consignada en el M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información. De igual forma se encuentra articulado con el proceso de inducción.** **b) Se les suministren las directrices que establecen las expectativas de seguridad de la información de sus roles dentro de la Entidad, con las sensibilizaciones programadas por el equipo de seguridad de la información. G-E-GET-41_Plan de sensibilización y comunicaciones en seguridad de la información** **c) Logren un nivel de toma de conciencia sobre seguridad de la información pertinente a sus roles y responsabilidades dentro de la organización y estén motivados para cumplir con las políticas mediante las sensibilizaciones programadas por el equipo de seguridad de la información. G-E-GET-41_Plan de sensibilización y comunicaciones en seguridad de la información** **d) Tengan continuamente las habilidades y calificaciones apropiadas y reciban capacitación en forma regular, mediante las sensibilizaciones programadas por el equipo de seguridad de la información.** **e) Cuenten con un canal para reporte anónimo de incumplimiento de las políticas o procedimientos de seguridad de la información ("denuncias internas"), cuyo control se consigna en el M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información y se realiza mediante la herramienta de gestión de servicios.**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información. G-E-GET-41_Plan de sensibilización y comunicaciones en seguridad de la información
	A.7.2.2	**Toma de conciencia, educación y formación en la seguridad de la información.**	**Control** **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	NO	Se adopta este control, puesto que los funcionarios, contratistas y partes interesadas deben tomar conciencia de sus responsabilidades en seguridad de la información.	X		X	X	**a) Los funcionarios y contratistas están debidamente informados sobre sus roles y responsabilidades de seguridad de la información, antes de que se les otorgue el acceso a información o sistemas de información confidenciales, cuya información esta consignada en el M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información. De igual forma se encuentra articulado con el proceso de inducción.** **b) Se les suministren las directrices que establecen las expectativas de seguridad de la información de sus roles dentro de la Entidad, con las sensibilizaciones programadas por el equipo de seguridad de la información. G-E-GET-41_Plan de sensibilización y comunicaciones en seguridad de la información** **c) Logren un nivel de toma de conciencia sobre seguridad de la información pertinente a sus roles y responsabilidades dentro de la organización y estén motivados para cumplir con las políticas mediante las sensibilizaciones programadas por el equipo de seguridad de la información. G-E-GET-41_Plan de sensibilización y comunicaciones en seguridad de la información** **d) Tengan continuamente las habilidades y calificaciones apropiadas y reciban capacitación en forma regular, mediante las sensibilizaciones programadas por el equipo de seguridad de la información.** **e) Cuenten con un canal para reporte anónimo de incumplimiento de las políticas o procedimientos de seguridad de la información ("denuncias internas"), cuyo control se consigna en el M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información y se realiza mediante la herramienta de gestión de servicios.**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información. G-E-GET-41_Plan de sensibilización y comunicaciones en seguridad de la información
	A.7.2.3	**Proceso disciplinario.**	**Control** **Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.**	SI	NO	Se adopta este control, puesto que se debe asegurar el debido proceso a los funcionarios de quienes se presuma que han cometido violaciones a la seguridad de la información.			X		**En el M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información se relaciona el control a seguir; no obstante es necesario formalizar el proceso a seguir cuando se verifica que ha ocurrido una violación a la seguridad de la información.** **Ver procedimientos: P-A-DIS-01 Indagación Preliminar, P-A-DIS-02 Investigación Disciplinaria, P-A-GR-DI-03 Juzgamiento (Pliego de Cargos), P-A-GR-DI-04 Segunda Instancia, P-A-DIS-05 Disciplinario Verbal.** **Ley 734 de 2002.**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información Ver procedimientos: P-A-DSI-01 Indagación Preliminar, P-A-DIS-02 Investigación Disciplinaria, P-A-GR-DI-03 Juzgamiento (Pliego de Cargos), P-A-DIS-04 Segunda Instancia, P-A-DIS-05 Disciplinario Verbal. Ley 734 de 2002.
	A.7.3	**TERMINACIÓN Y CAMBIO DE EMPLEO**	**Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.**									
	A.7.3.1	**Terminación o Cambio de responsabilidades de empleo.**	**Control** **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	NO	Se adopta este control, puesto que la comunicación de las responsabilidades en la terminación o cambio de empleo, deben incluir requisitos de seguridad de la información.	X		X		**Los términos y condiciones se acuerdan que después de terminada la relación laboral o contrato seguirán vigentes por un periodo de tiempo dentro** **"F-A-ATH-06 Control de legalización Retiro del Servicio". Procedimientos de Talento Humano y requisitos de diferentes áreas en cuanto a responsabilidades.** **F-A-CTR-36_Acta de confidencialidad e integridad de la información**	*Manual de Funciones (Funcionarios). "F-A-ATH-06 Control de Retiro del Servicio". Procedimientos de Talento Humano y requisitos de diferentes áreas en cuanto a responsabilidades. FF-A-CTR-36_Acta de confidencialidad e integridad de la información.

	A.8	**GESTIÓN DE ACTIVOS**										
8. GESTIÓN DE ACTIVOS	**A.8.1**	**RESPONSABILIDAD POR LOS ACTIVOS**	**Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.**									
	A.8.1.1	**Inventario de activos.**	**Control** **Se deben identificar la información, otros activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.**	SI	NO	Se adopta este control, puesto que se deben identificar los activos de información y documentar su relevancia.	X		X		**1) La actualización del inventario de activos de información se presenta para aprobación en el comité de gestión y desempeño por lo menos una vez al año.** **2) Los criterios respecto a la importancia del activo quedaron definidos dentro la I-E-GET-02 Metodología para la identificación gestión y clasificación de activos de información.** **3) El propietario del activo se encuentra relacionado en la F-E-GET-18 Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE.**	I-E-GET-02 Metodología para la identificación gestión y clasificación de activos de información. F-E-GET-18 Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE. M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información
	A.8.1.2	**Propiedad de los activos.**	**Control** **Los activos mantenidos en el inventario deben tener un propietario**	SI	NO	Se adopta este control, puesto que el propietario del activo de información debe ser responsable de su apropiada gestión durante todo el ciclo de vida.	X		X		**a) Los activos están inventariados dentro de la F-E-GET-18 Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE.** **b) Los activos están clasificados y protegidos apropiadamente dentro de la F-E-GET-18 Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE.** **c) Los activos importantes se definen y revisan periódicamente respecto a las restricciones y clasificaciones teniendo en cuenta las políticas de control de acceso aplicables.** **d) El manejo del activo cuando es eliminado o destruido se gestiona conforme a la I-E-GET-02 Metodología para la identificación gestión y clasificación de activos de información**	I-E-GET-02 Metodología para la identificación gestión y clasificación de activos de información. F-E-GET-18 Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE. M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información
	A.8.1.3	**Uso aceptable de los activos.**	**Control** **Los activos mantenidos en el inventario deben tener un propietario**	SI	NO	Se adopta este control, puesto que los funcionarios, contratistas y terceros que usan activos de información de la Entidad, deben tomar conciencia de los requisitos de seguridad de la información y deben ser responsables del uso que hacen.	X	X	X		**En al documento de M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información se encuentra documentada la política de 8.1.3 Uso aceptable de los activos**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información
	A.8.1.4	**Devolución de Activos.**	**Control** **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	NO	Se adopta este control, puesto que los funcionarios, contratistas o terceros deben hacer la devolución de todos los activos físicos y electrónicos a su cargo.	X	X	X		**En al documento de M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información se encuentra documentada la política de 8.1.4 Devolución de activos.** **La entidad realiza el respectivo seguimiento respecto a la devolución de los activos de información por medio del trámite y firma del paz y salvo. Lo anterior aplica para los activos físicos y accesos a los servicios tecnológicos de la entidad.**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información F-A-CTR-35 Paz y salvo contrato de prestación de servicios
	A.8.2	**CLASIFICACIÓN DE LA INFORMACIÓN**	**Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.**									
	A.8.2.1	**Clasificación de la información.**	**Control** **La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.**	SI	NO	Se adopta este control, puesto que la clasificación y control de la información debe tener en cuenta las necesidades de la Entidad en cuanto a intercambio o restricción de la información así como los requisitos legales.	X		X		**En la I-E-GET-02 Metodología para la identificación gestión y clasificación de activos de información, y en F-E-GET-18 Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE, se definen las convenciones y criterios de clasificación de la información desde la confidencialidad, integridad y disponibilidad así como la periodicidad para la revisión de los mismos.** **1) Que las convenciones y criterios de clasificación sean claros y estén documentados** **2) Que se defina cada cuanto debe revisarse la clasificación de un activo** **3) La clasificación debería valorarse analizando la confidencialidad, integridad y disponibilidad.** **F-E-GET-18 Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE.** **M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información se encuentra documentada la política de 8.2.1 Clasificación de la información.**	I-E-GET-02 Metodología para la identificación gestión y clasificación de activos de información F-E-GET-18 Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE. M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información
	A.8.2.2	**Etiquetado de la información.**	**Control** **Se debería 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	NO	Se adopta este control, puesto que el etiquetado de la información debe abarcar la información en formatos físicos y electrónicos.	X		X		**a) Restricciones de acceso que soportan los requisitos de protección para cada nivel de clasificación, las cuales se garantizan por parte de los líderes de cada proceso.** **b) Registro formal de los receptores autorizados de los activos mediante los canales oficiales de comunicación de la entidad.** **c) Protección de copias de información temporal o permanente a un nivel coherente con la protección de la información original con la aplicación de las políticas de respaldo de la información.** **d) Almacenamiento de los activos de TI de acuerdo con las especificaciones de los fabricantes.** **e) Marcado de las copias de medios mediante la identificación de las mismas de conformidad con el I-A-GTI-02 Instructivo para la generación de copias de respaldo BACK-UP.** **f) La entidad almacena la información en sus servidores de acuerdo con el I-A-GTI-02 Instructivo para la generación de copias de respaldo BACK-UP**	I-E-GET-02 Metodología para la identificación gestión y clasificación de activos de información F-E-GET-18 Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE. M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información I-A-GTI-02 Instructivo para la generación de copias de respaldo BACK-UP
	A.8.2.3	**Manejo de activos.**	**Control** **Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización. "M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información"**	SI	NO	Se adopta este control, puesto que se deben elaborar procedimientos para el manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación.			X		a) Restricciones de acceso que soportan los requisitos de protección para cada nivel de clasificación, las cuales se garantizan por parte de los líderes de cada proceso. b) Registro formal de los receptores autorizados de los activos mediante los canales oficiales de comunicación de la entidad. c) Protección de copias de información temporal o permanente a un nivel coherente con la protección de la información original con la aplicación de las políticas de respaldo de la información. d) Almacenamiento de los activos de TI de acuerdo con las especificaciones de los fabricantes. e) Marcado de las copias de medios mediante la identificación de las mismas de conformidad con el DS-A-GTI-02 Plan de generación de copias de respaldo. f) La entidad almacena la información en sus servidores de acuerdo con el I-A-GTI-02 Instructivo para la generación de copias de respaldo BACK-UP	I-E-GET-02 Metodología para la identificación gestión y clasificación de activos de información F-E-GET-18 Matriz inventario de activos de información Ministerio de Ambiente y Desarrollo Sostenible - AMBIENTE. M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información I-A-GTI-02 Instructivo para la generación de copias de respaldo BACK-UP.
	A.8.3	**MANEJO DE MEDIOS**	**Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.**									
	A.8.3.1	**Gestión de medios removibles.**	**Control** **Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.**	SI	NO	Se adopta este control, puesto que es necesario definir procedimientos para la gestión de medios removibles para evitar la modificación, retiro, o destrucción no autorizada de información.			X		**a) Si ya no se requiere, el contenido de cualquier medio reusable que se vaya a retirar de la organización se debe remover de forma que no sea recuperable; con la aplicación de los lineamientos establecidos en la G-E-GTI-04 Guía de borrado seguro.** **b) cuando resulte necesario y práctico, se debe solicitar autorización para retirar los medios de la organización, y se debe llevar un registro de dichos retiros con el fin de mantener un rastro de auditoría; cuyo registro lo gestiona el grupo de servicios administrativos en el acceso a la entidad en el formato F-A-GAC-02 Autorización salida de elementos.** **f) se deben guardar varias copias de los datos valiosos en medios separados, para reducir aún más el riesgo de daño o pérdida casuales de los datos; de conformidad con la clasificación de los activos de información y el I-A-GTI-02 Instructivo para la generación de copias de respaldo BACK UP**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información G-E-GTI-04 Guía de borrado seguro. F-A-GAC-02 Autorización salida de elementos I-A-GTI-02 Instructivo para la generación de copias de respaldo BACK-UP M-A-GTI-02 MANUAL GENERAL DE OPERACIONES DE INFRAESTRUCTURA DE TI (ANEXO 5. Manual de operaciones de solución antivirus) Se controla a través de la consola de antivirus Kaspersky.
	A.8.3.2	**Disposición de los medios.**	**Control** **Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.**	SI	NO	Se adopta este control, puesto que es necesario definir procedimientos formales para la disposición segura de los medios, para minimizar el riesgo de fuga de información a personas no autorizadas.			X		**Se encuentra documentada la guía de borrado seguro G-E-GTI-04 y en el procedimiento P-A-GAC-12 BAJA Y ENAJENACIÓN DE BIENES DEL INVENTARIO identificados como no útiles o en estado de obsolescencia; con el fin de darle una disposición final.** **El área de Infraestructura TI conceptúa técnicamente mediante memorando sobre la obsolescencia o daño total de equipos y remite los elementos para el trámite de baja con el almacén del Ministerio. Se cuenta con acuerdo para borrado seguro y destrucción a través del Sistema de Gestión Ambiental.**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información G-E-GTI-04 Guía de borrado seguro. P-A-GAC-12 BAJA Y ENAJENACIÓN DE BIENES DEL INVENTARIO
	A.8.3.3	**Transferencia de medios físicos.**	**Control** **Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.**	SI	NO	Se adopta este control, puesto que los medios de almacenamiento que contienen información confidencial de la Entidad se deben proteger mientras se transportan.	X		X		**En el documento de M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información se encuentran definidos los lineamientos que contemplan la protección de medios durante el transporte.**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información Procedimiento P-A-GTI-08 Cifrado de Archivos Confidenciales o de Acceso Restringido
	A.9	**CONTROL DE ACCESO**										
	A.9.1	**REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO**	**Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.**									
	A.9.1.1	**Política de control de acceso.**	**Control** **Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.**	SI	NO	Se adopta este control, puesto que se deben definir lineamientos de control de acceso apropiados a los activos de información.		X	X		**a) los requisitos de seguridad para las aplicaciones del negocio;** **b) las políticas para la divulgación y autorización de la información, y los niveles de seguridad de la información y de clasificación de la información;** **c) la coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes;** **d) la legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios;** **e) la gestión de los derechos de acceso en un entorno distribuido y en red, que reconoce todos los tipos de conexiones disponibles;** **f) la separación de los roles de control de acceso, (solicitud de acceso, autorización de acceso, administración del acceso);** **g) los requisitos para la autorización formal de las solicitudes de acceso;** **h) los requisitos para la revisión periódica de los derechos de acceso;** **i) el retiro de los derechos de acceso;** **j) el ingreso de los registros de todos los eventos significativos concernientes al uso y gestión de identificación de los usuarios, e información de autenticación secreta, en el archivo permanente;** **k) los roles de acceso privilegiado;**	A,B,C,D,E,F,G,H,I,J,K) M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. C) I-E-GET-02 METODOLOGÍA PARA LA IDENTIFICACIÓN, GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN F, K) M-A-GTI-02 Manual general de operaciones de infraestructura de TI
	A.9.1.2	**Acceso a redes y servicios de red.**	**Control** **Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.**	SI	NO	Se adopta este control, puesto que se deben definir lineamientos acerca del uso de redes y de servicios de red.			X		**a) las redes y servicios de red a los que se permite el acceso;** **b) los procedimientos de autorización para determinar a quién se permite el acceso a qué redes y servicios de red;** **c) los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y a los servicios de red;** **d) los medios usados para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas);** **e) los requisitos de autenticación de usuarios para acceder a diversos servicios de red;** **f) el seguimiento del uso de servicios de red.**	A,B,C,D,E,F) M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. G-A-GTI-05 Guía del Uso de la Red e Internet, Directorio Activo, F2A, MFA para algunos sistemas de información. P-A-GTI-01 Atención de solicitudes de soporte. Sistema de solicitudes GEMA (Aranda).
	A.9.2	**GESTIÓN DE ACCESO DE USUARIOS**	**Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.**									
	9.2.1	**Registro y cancelación del registro de usuarios.**	**Control** **Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.**	SI	NO	Se adopta este control, puesto que se debe gestionar y monitorear los derechos de acceso de usuarios por medio de un procedimiento en el cual se contemple el registro y cancelación de usuarios.			X		**a) Identificaciones únicas para los usuarios, que les permita estar vinculados a sus acciones y mantener la responsabilidad por ellas; el uso de identificaciones compartidas solo se debe permitir cuando sea necesario por razones operativas o del negocio, y se aprueban y documentan;** **b) deshabilitar o retirar inmediatamente las identificaciones de los usuarios que han dejado la organización;** **c) identificar y eliminar o deshabilitar periódicamente las identificaciones de usuario redundantes;** **d) asegurar que las identificaciones de usuario redundantes no se asignen a otros usuarios.**	A,B,C,D,E,F) M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. - G-A-GTI-05 Guía del Uso de La Red e Internet, Directorio Activo, F2A, MFA para algunos sistemas de información. P-A-GTI-01 Atención de solicitudes de soporte. Sistema de solicitudes GEMA (Aranda). F-A-ATH-06 Control de Legalización Retiro del Servicio
	9.2.2	**Suministro de acceso de usuarios.**	**Control** **Se debería 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	NO	Se adopta este control, puesto que se debe verificar la asignación o revocación de los derechos de acceso de usuario otorgados a los sistemas y servicios.			X		**a) obtener la autorización del propietario del sistema de información o del servicio para el uso del sistema de información o servicio;** **b) verificar que el nivel de acceso otorgado es apropiado a las políticas de acceso y es coherente con otros requisitos, tales como separación de deberes;** **c) asegurar que los derechos de acceso no estén activados antes de que los procedimientos de autorización estén completos;** **d) mantener un registro central de los derechos de acceso suministrados a una identificación de usuario para acceder a sistemas de información y servicios;** **e) adaptar los derechos de acceso de usuarios que han cambiado de roles o de empleo, y retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han dejado la organización;** **f) revisar periódicamente los derechos de acceso con los propietarios de los sistemas de información o servicios.**	A,B,C,D,E,F) M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GTI-02 Manual General de Operaciones de Infraestructura Tecnológica. Anexo 14. Creación de usuarios. P-A-GTI-01 Atención de solicitudes de soporte. Sistema de solicitudes GEMA (Aranda).

9. CONTROL DE ACCESO	9.2.3	**Gestión de derechos de acceso privilegiado.**	**Control** **Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.**	SI	NO	Se adopta este control, puesto que la asignación de derechos de acceso privilegiado se debe controlar mediante un proceso de autorización formal.			X	X		**a) Identificar los derechos de acceso privilegiado asociados con cada sistema o proceso, (sistema operativo, sistema de gestión de bases de datos, y cada aplicación) y los usuarios a los que es necesario asignar;** **b) definir o establecer los derechos de acceso privilegiado a usuarios con base en la necesidad de uso y caso por caso, alineada con la política de control de acceso;** **c) mantener un proceso de autorización y un registro de todos los privilegios asignados. Sólo se debe suministrar derechos de acceso cuando el proceso de autorización esté completo;** **d) definir los requisitos para la expiración de los derechos de acceso privilegiado;** **e) establecer los derechos de acceso privilegiado a través de una identificación de usuario diferente de la usada para las actividades regulares del negocio. Las actividades regulares del negocio no se ejecutan desde una identificación privilegiada;** **f) tener las competencias de los usuarios con derechos de acceso privilegiado y su revisión periódica para verificar si están en línea con sus deberes;** **g) establecer y mantener procedimientos genéricos para evitar el uso no autorizado de identificaciones de usuario de administración genérica, de acuerdo con las capacidades de configuración del sistema;** **h) establecer la confidencialidad de la información de autenticación secreta, para las identificaciones de usuario de administración genérica, cuando se comparta (cambiar las contraseñas con frecuencia, y cuando un usuario privilegiado ha dejado el trabajo o cambia de trabajo, comunicarlas entre los usuarios privilegiados con los mecanismos apropiados).**	A,B,C,D,E,F) M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GTI-02 Manual General de Operaciones de Infraestructura Tecnológica. Anexo 14. Creación de usuarios. P-A-GTI-01 Atención de solicitudes de soporte. Sistema de solicitudes GEMA (Aranda).
	9.2.4	**Gestión de información de autenticación secreta de usuarios.**	**Control** **La asignación de información de autenticación secreta se debería controlar por medio de un proceso de gestión formal.**	SI	NO	Se adopta este control, puesto que se debe definir un procedimiento para la asignación de información secreta para la autenticación.				X		**a) establecer la firma de una declaración para mantener confidencial la información de autenticación secreta personal, y mantener la información de autenticación secreta del grupo (cuando es compartida) únicamente dentro de los miembros del grupo; esta declaración firmada se puede incluir en los términos y condiciones del empleo para todos los que los usuarios ;** **b) estipular que todos los usuarios deben mantener su propia información de autenticación secreta, y se les suministra una autentificación secreta temporal segura, que se obligue a cambiar al usarla por primera vez;** **c) establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle la nueva información de autenticación secreta de reemplazo o temporal;** **d) definir que la información de autenticación secreta temporal se suministra a los usuarios de una manera segura; y se evitar utilizar partes externas o de mensajes de correo electrónico no protegidos (texto claro);** **e) establecer que la información de autenticación secreta temporal es única para un individuo y no es fácil de adivinar;** **f) definir que los usuarios deben acusar recibo de la información de autenticación secreta;** **g) establecer que la información de autenticación secreta por defecto, del fabricante, se modifica después de la instalación de los sistemas o software.**	(A, B) M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. (B, C, D., E, G) M-A-GTI-02 Manual General de Operaciones de Infraestructura Tecnológica. Anexo 14. Creación de usuarios. (F.) P-A-GTI-01 Atención de solicitudes de soporte. Sistema de solicitudes GEMA (Aranda).
	9.2.5	**Revisión de los derechos de acceso de usuarios.**	**Control** **Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.**	SI	NO	Se adopta este control, puesto que es necesario realizar la revisión de los derechos de acceso de usuario por medio de un procedimiento.				X		**a) examinar los derechos de acceso de los usuarios periódicamente y después de cualquier cambio, promoción, cambio a un cargo a un nivel inferior, o terminación del empleo;** **b) establecer que los derechos de acceso de usuario se revisan y reasignan cuando pasan de un rol a otro dentro de la misma organización;** **c) definir las autorizaciones para los derechos de acceso privilegiado y revisar periódicamente;** **d) verificar las asignaciones de privilegios periódicamente, para asegurar que no se hayan obtenido privilegios no autorizados;** **e) revisar y registrar los cambios a las cuentas privilegiadas periódicamente.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GTI-02 Manual General de Operaciones de Infraestructura Tecnológica. Anexo 14. Creación de usuarios.
	9.2.6	**Retiro o ajuste de los derechos de acceso.**	**Control** **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	NO	Se adopta este control, puesto que al terminar el contrato o empleo, los derechos de acceso a la información o activos de información de un funcionario, colaborador o tercero se deben de retirar o suspender.				X		**a) terminación o cambio lo inicia el empleado, el usuario de la parte externa o la dirección, y la razón de la terminación;** **b) revisar las responsabilidades actuales del empleado, el usuario de la parte externa o cualquier otro usuario;** **c) verificar el valor de los activos accesibles en la actualidad.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-01 Atención de solicitudes de soporte. M-A-GTI-02 Manual General de Operaciones de Infraestructura Tecnológica. Anexo 14. Creación de usuarios.
	A.9.3	**RESPONSABILIDADES DE LOS USUARIOS**	Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.										
	A.9.3.1	**Uso de información de autenticación secreta.**	**Control** **Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información secreta para la autenticación.**	SI	NO	Se adopta este control, puesto que se debe exigir a los usuarios que mantengan la confidencialidad de la información de la autenticación secreta.				X		**a) Mantener la confidencialidad de la información de autenticación secreta, asegurándose de que no sea divulgada a ninguna otra parte, incluidas las personas con autoridad;** **b) evitar llevar un registro (en papel, en un archivo de software o en un dispositivo portátil) de autenticación secreta, a menos que se pueda almacenar en forma segura y que el método de almacenamiento haya sido aprobado (una bóveda para contraseñas);** **c) cambiar la información de autenticación secreta siempre que haya cualquier indicio de que se pueda comprometer la información;** **d) definir que cuando se usa contraseñas como información de autenticación secreta, se debe seleccionar contraseñas seguras con una longitud mínima suficiente que:** **1) sean fáciles de recordar;** **2) no estén basadas en algo que otra persona pueda adivinar fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono y fechas de nacimiento, etc.);** **3) no sean vulnerables a ataques de diccionario (es decir, no contienen palabras incluidas en los diccionarios);** **4) estén libres de caracteres completamente numéricos o alfabéticos idénticos consecutivos;** **5) si son temporales, cambiarlos la primera vez que se ingrese;** **e) no compartir información de autenticación secreta del usuario individual;** **f) establecer una protección apropiada de contraseñas cuando se usan éstas como información de autenticación secreta en procedimientos de ingreso automatizados, y estén almacenadas;** **g) no usar la misma información de autenticación secreta para propósitos de negocio y otros diferentes de estos.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-01 Atención de solicitudes de soporte. M-A-GTI-02 Manual General de Operaciones de Infraestructura Tecnológica. Anexo 14. Creación de usuarios.
	A.9.4	**CONTROL DE ACCESO A SISTEMAS Y APLICACIONES**	**Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.**										
	A.9.4.1	**Restricción de acceso a la información.**	**Control** **El acceso a la información y a la funcionalidad de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.**	SI	NO	Se adopta este control, puesto que las restricciones de acceso se deben basar en los lineamientos de la política de control de acceso.				X		**a) suministrar menús para controlar el acceso a las funciones de sistemas de aplicaciones;** **b) controlar a qué datos puede tener acceso un usuario particular;** **c) controlar los derechos de acceso de los usuarios, (a leer, escribir, borrar y ejecutar);** **d) controlar los derechos de acceso de otras aplicaciones;** **e) limitar la información contenida en los elementos de salida;** **f) proveer controles de acceso físico o lógico para el aislamiento de aplicaciones, datos de aplicaciones o sistemas críticos.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. Se tienen aplicativos con perfilamiento y roles independientes mediante menú, la primera asignación se realiza mediante Directorio Activo con usuario river básico.
	A.9.4.2	**Procedimiento de ingreso seguro.**	**Control** **Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.**	SI	NO	Se adopta este control, puesto que se debe definir una técnica de autenticación adecuada para corroborar la identidad declarada de un usuario.				X		**a) no visualizar los identificadores del sistema o de la aplicación sino hasta que el proceso de ingreso se haya completado exitosamente;** **b) visualizar una advertencia general acerca de que sólo los usuarios autorizados pueden acceder al computador;** **c) evitar los mensajes de ayuda durante el procedimiento de ingreso, que ayudarían a un usuario no autorizado;** **d) validar la información de ingreso solamente al completar todos los datos de entrada. ante una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta;** **e) proteger contra intentos de ingreso mediante fuerza bruta;** **f) llevar un registro con los intentos exitosos y fallidos;** **g) declarar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de ingreso;** **h) visualizar la siguiente información al terminar un ingreso seguro:** **1) registrar la fecha y la hora del ingreso previo exitoso;** **2) registrar los detalles de cualquier intento de ingreso no exitoso desde el último ingreso exitoso;** **i) no visualizar una contraseña que se esté ingresando;** **j) no transmitir contraseñas en un texto claro en una red;** **k) terminar sesiones inactivas después de un período de inactividad definido, especialmente en lugares de alto riesgo tales como áreas públicas o externas por fuera de la gestión de seguridad de la organización o en dispositivos móviles;** **l) restringir los tiempos de conexión para brindar seguridad adicional para aplicaciones de alto riesgo y para reducir la ventana de oportunidad para acceso no autorizado.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-01 Atención de solicitudes de soporte. M-A-GTI-02 Manual General de Operaciones de Infraestructura Tecnológica. Anexo 14. Creación de usuarios.
	A.9.4.3	**Sistemas de gestión de contraseñas.**	**Control** **Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.**	SI	NO	Se adopta este control, puesto que se debe asegurar la gestión y calidad de las contraseñas que se usan en los sistemas de información.				X		**a) cumplir el uso de identificaciones y contraseñas de usuarios individuales para mantener la rendición de cuentas;** **b) permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluyan un procedimiento de confirmación para permitir los errores de entrada;** **c) Exigir por que se escojan contraseñas de calidad;** **d) Forzar a los usuarios cambiar sus contraseñas cuando ingresan por primera vez;** **e) Exigir por que se cambien las contraseñas en forma regular, según sea necesario:** **f) llevar un registro de las contraseñas usadas previamente, e impedir su reusó;** **g) no visualizar contraseñas en la pantalla cuando se está ingresando;** **h) almacenar los archivos de las contraseñas separadamente de los datos del sistema de aplicaciones;** **i) almacenar y transmitir las contraseñas en forma protegida.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-01 Atención de solicitudes de soporte. M-A-GTI-02 Manual General de Operaciones de Infraestructura Tecnológica. Anexo 14. Creación de usuarios.
	A.9.4.4	**Uso de programas utilitarios privilegiados.**	**Control** **Se debería restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.**	NO	NO	Se adopta este control, puesto que se deben tener directrices para evitar que el uso de programas utilitarios puedan anular los sistemas y controles de las aplicaciones.				X		**a) utilizar procedimientos de identificación, autenticación y autorización para los programas utilitarios;** **b) separar los programas utilitarios del software de aplicaciones;** **c) limitar el uso de programas utilitarios al número mínimo práctico de usuarios confiables y autorizados;** **d) autorizar el uso adhoc de programas utilitarios;** **e) limitar la disponibilidad de los programas utilitarios;** **f) registrar el uso de los programas utilitarios;** **g) definir y documentar los niveles de autorización para los programas utilitarios;** **h) retirar o deshabilitar todos los programas utilitarios innecesarios;** **i) No poner a disposición los programas utilitarios a los usuarios que tengan acceso a aplicaciones en sistemas en donde se requiera la separación de deberes.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-01 Atención de solicitudes de soporte. M-A-GTI-02 Manual General de Operaciones de Infraestructura Tecnológica. Anexo 14. Creación de usuarios.
	A.9.4.5	**Control de acceso a códigos fuente de programas.**	**Control** **Se debería restringir el acceso a los códigos fuente de los programas.**	SI	NO	Se adopta este control, puesto que se debe controlar el acceso a los códigos fuente de programas para evitar la introducción de funcionalidades no autorizadas o cambios involuntarios en la aplicación.				X		**a) definir en donde sea posible, las librerías de fuentes de programas no se deben mantener en los sistemas operativos;** **b) gestionar los códigos fuente de los programas y las librerías de las fuentes de los programas se debería hacer de acuerdo con procedimientos establecidos;** **c) establecer que el personal de soporte deben tener acceso restringido a las librerías de las fuentes de los programas;** **d) definir que la actualización de las librerías de fuentes de programas y elementos asociados, y la entrega de fuentes de programas a los programadores sólo se deben hacer una vez que se haya recibido autorización apropiada;** **e) establecer que los listados de programas se deben mantener en un entorno seguro;** **f) conservar un registro de auditoría de todos los accesos a la librerías de fuentes de programas;** **g) mantener y copiar las bibliotecas de fuentes de programas a través de procedimientos estrictos de control de cambios.**	Se tiene el acceso restringido a códigos fuente, segregación de red, Políticas en el Manual de Seguridad de la Información. M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. Se tiene establecido mecanismos de gestión de códigos fuente y librerías dentro del repositorio de información establecido.
	A.10	**CRIPTOGRAFÍA**											
	A.10.1	**CONTROLES CRIPTOGRÁFICOS**	**Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.**										

10. CRIPTOGRAFÍA	A.10.1.1	**Políticas sobre el uso de controles criptográficos.**	**Control** **Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.**	SI	NO	Se adopta este control, puesto que se deben tener lineamientos para el uso de controles criptográficos en la Entidad.	X		X		**Se aplica cifrado en sistema de correo electrónico mediante appliance de seguridad para correo electrónico, de igual manera a través de Exchange, se cuenta con toquen bancarios, certificados de páginas web y cifrado de discos y/o capsulas.** **a) establecer el enfoque de la dirección con relación al uso de controles criptográficos en toda la organización, incluyendo los principios generales bajo los cuales se deben proteger la información del negocio;** **b) realizar una valoración de riesgos, que identifique el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de encriptación requerido.** **c) utilizar la encriptación para la protección de información transportada por dispositivos de encriptación móviles o removibles, o a través de líneas de comunicación;** **d) gestionar las llaves y los métodos para la protección de llaves criptográficas y la recuperación de información encriptada, en el caso de llaves perdidas, llaves cuya seguridad está comprometida, o que están dañadas;** **e) establecer roles y responsabilidades, quién es responsable por:** **1) la implementación de la política.** **2) la gestión de llaves, incluida la generación de llaves;** **f) establecer las normas que se van a adoptar para la implementación efectiva en toda la organización (procesos del negocio);** **g) definir el impacto de usar información encriptada en los controles que dependen de la inspección del contenido.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. E.F) P-A-GTI-08 CIFRADO DE ACHIVO CONFIDENCIAL O DE ACCESO RESTRINGIDO
	A.10.1.2	**Gestión de llaves.**	**Control** **Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.**	SI	NO	Se adopta este control, puesto que se deben tener lineamientos para la gestión de llaves criptográficas durante todo su ciclo de vida.	X		X		**a) generar llaves para diferentes sistemas criptográficos y diferentes aplicaciones;** **b) generar y obtener certificados de llaves públicas;** **c) distribuir llaves a las entidades previstas, incluyendo la forma de recibir y activar las llaves;** **d) almacenar las llaves, incluyendo la forma en que los usuarios autorizados obtienen acceso a ellas;** **e) cambiar o actualizar las llaves, incluyendo las reglas sobre cuándo se deben cambiar y cómo hacerlo;** **f) dar tratamiento a las llaves cuya seguridad está comprometida;**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-08 CIFRADO DE ACHIVO CONFIDENCIAL O DE ACCESO RESTRINGIDO
	A.11	**SEGURIDAD FÍSICA Y DEL ENTORNO**											
11. SEGURIDAD FÍSICA Y DEL ENTORNO	**A.11.1**	**ÁREAS SEGURAS**	**Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.**										
	A.11.1.1	**Perímetros de seguridad física.**	**Control** **Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.**	SI	NO	Se adopta este control, puesto que se debe prevenir el acceso físico no autorizado a las instalaciones de procesamiento de la información en la Entidad, definiendo perímetros de seguridad.			X		**a) definir los perímetros de seguridad, y el emplazamiento y fortaleza de cada uno de los perímetros deben depender de los requisitos de seguridad de los activos dentro del perímetro y de los resultados de una valoración de riesgos;** **b) establecer los perímetros de una edificación o sitio que contenga instalaciones de procesamiento de la información debe ser físicamente seguros; el techo exterior, las paredes y el material de los pisos del sitio deben ser de construcción sólida, y todas las paredes externas deben estar protegidas adecuadamente contra acceso no autorizado con mecanismos de control (barras, alarmas, cerraduras); las puertas y ventanas deben estar cerradas con llave cuando no hay supervisión, y se debe considerar protección externa para ventanas, particularmente al nivel del suelo;** **c) definir un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o edificación; el acceso a los sitios y edificaciones debe estar restringido únicamente para personal autorizado;** **d) establecer cuando sea aplicable y construir barreras físicas para impedir el acceso físico no autorizado y la contaminación ambiental;** **e) establecer que todas las puertas contra incendio en un perímetro de seguridad deben tener alarmas, estar monitoreadas y probadas junto con las paredes, para establecer el nivel requerido de resistencia de acuerdo con normas regionales, nacionales e internacionales adecuadas; deben funcionar de manera segura de acuerdo al código local de incendios;** **f) instalar sistemas adecuados para detección de intrusos de acuerdo con normas nacionales, regionales o internacionales y se deben probar regularmente para abarcar todas las puertas externas y ventanas accesibles; las áreas no ocupadas deben tener alarmas en todo momento; también deben abarcar otras áreas, tales como las salas de computo o las salas de comunicaciones;** **g) establecer que las instalaciones de procesamiento de información gestionadas por la organización deben estar separadas físicamente de las gestionadas por partes externas.**	M-A-GAC-01 Protocolo de Seguridad Ministerio de Ambiente y Desarrollo Sostenible. M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GAC-01 Protocolo de seguridad Minambiente
	A.11.1.2	**Controles de accesos físicos.**	**Control** **Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el ingreso a personal autorizado.**	SI	NO	Se adopta este control, puesto que solo debe ingresar el personal autorizado a las áreas seguras de la Entidad.	X		X		**a) tener un registro de la fecha y hora de entrada y salida de los visitantes, y todos los visitantes deben ser supervisados a menos que su acceso haya sido aprobado previamente; solo se les debe otorgar acceso para propósitos específicos autorizados y se deben emitir instrucciones sobre los requisitos de seguridad del área y de los propósitos de emergencia. La identidad de los visitantes se deben autenticar por los medios apropiados;** **b) establecer que el acceso a las áreas en las que se procesa o almacena información confidencial se debería restringir a los individuos autorizados solamente mediante la implementación de controles de acceso apropiados, (mediante la implementación de un mecanismo de autenticación de dos factores, tales como una tarjeta de acceso y un PIN secreto);** **c) mantener y hacer seguimiento de un libro de registro (physical log book) físico o un rastro de auditoría electrónica de todos los accesos;** **d) definir que todos los empleados, contratistas y partes externas deben portar algún tipo de identificación visible, y se deben notificar de inmediato al personal de seguridad si se encuentran visitantes no acompañados, y sin la identificación visible;** **e) establecer que el personal de servicio de soporte de la parte externa se le debería otorgar acceso restringido a áreas seguras o a instalaciones de procesamiento de información confidencial solo cuando se requiera; este acceso se deben autorizar y se le debe hacer seguimiento;** **f) definir los derechos de acceso a áreas seguras se deben revisar y actualizar regularmente, y revocar cuando sea necesario.**	M-A-GAC-01 Protocolo de Seguridad Ministerio de Ambiente y Desarrollo Sostenible. M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GAC-01 Protocolo de seguridad Minambiente
	A.11.1.3	**Seguridad de oficinas, recintos e instalaciones.**	**Control** **Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.**	SI	NO	Se adopta este control, puesto que se debe brindar seguridad a oficinas, recintos e instalaciones que impida el acceso público donde no esté permitido.			X		**a) establecer que las instalaciones clave deben estar ubicadas de manera que se impida el acceso del público;** **b) definir donde sea aplicable, las edificaciones deben ser discretas y dar un indicio mínimo de su propósito, sin señales obvias externas o internas, que identifiquen la presencia de actividades de procesamiento de información;** **c) establecer que las instalaciones deben estar configuradas para evitar que las actividades o información confidenciales sean visibles y audibles desde el exterior. El blindaje electromagnético también se debe ser el apropiado;** **d) definir los directorios y guías telefónicas internas que identifican los lugares de las instalaciones de procesamiento de información confidencial no deben ser accesibles a ninguna persona no autorizada.**	M-A-GAC-01 Protocolo de Seguridad Ministerio de Ambiente y Desarrollo Sostenible. M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GAC-01 Protocolo de seguridad Minambiente
	A.11.1.4	**Protección contra amenazas externas y ambientales.**	**Control** **Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.**	SI	NO	Se adopta este control, puesto que se debe evitar daños a causa de incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o causados por el hombre.			X	X	**De acuerdo a la NIST deben identificarse los elementos de resiliencia para soportar la entrega de los servicios críticos de la entidad.**	M-A-GAC-01 Protocolo de Seguridad Ministerio de Ambiente y Desarrollo Sostenible. M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GAC-01 Protocolo de seguridad Minambiente M-A-GTI-02 MANUAL GENERAL DE OPERACIONES DE INFRAESTRUCTURA DE TI (ANEXO 5. Manual de operaciones de solución antivirus)
	A.11.1.5	**Trabajo en áreas seguras.**	**Control** **Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.**	SI	NO	Se adopta este control, puesto que deben existir lineamientos para trabajar en áreas seguras.			X		**a) establecer que el personal solo debe conocer de la existencia de un área segura o de actividades dentro de un área segura, con base en lo que necesita conocer;** **b) definir que el trabajo no supervisado en áreas seguras se debe evitar tanto por razones de seguridad como para evitar oportunidades para actividades malintencionadas;** **c) establecer que las áreas seguras vacías deben estar cerradas con llave y se revisan periódicamente;** **d) no se permite el ingreso y uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello.**	M-A-GAC-01 Protocolo de Seguridad Ministerio de Ambiente y Desarrollo Sostenible. M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GAC-01 Protocolo de seguridad Minambiente
	A.11.1.6	**Áreas de despacho y carga.**	**Control: 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 el acceso no autorizado.**	SI	NO	Se adopta este control, puesto que deben existir lineamientos para evitar que en las áreas de despacho y carga ingresen personas no autorizadas.	X		X		**a) establecer que el acceso al área de despacho y de carga desde el exterior de la edificación se debería restringir al personal identificado y autorizado;** **b) definir que el área de despacho y carga se debe diseñar de manera que los suministros se puedan cargar y descargar sin que el personal de despacho tenga acceso a otras partes de la edificación;** **c) establecer que las puertas externas de un área de despacho y carga se aseguran cuando las puertas internas están abiertas;** **d) definir que el material que ingresa se inspecciona y examina para determinar la presencia de explosivos, químicos u otros materiales peligrosos, antes de que se retiren del área de despacho y carga;** **e) establecer que el material que ingresa se registra de acuerdo con los procedimientos de gestión de activos al entrar al sitio;** **f) definir que los despachos entrantes y salientes se están separados físicamente, en donde sea posible;** **g) establecer que el material entrante se inspecciona para determinar evidencia de manipulación durante el viaje. Si se descubre esta manipulación, se debería reportar de inmediato al personal de seguridad.**	M-A-GAC-01 Protocolo de Seguridad Ministerio de Ambiente y Desarrollo Sostenible. M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GAC-01 Protocolo de seguridad Minambiente
	A.11.2	**EQUIPOS**	**Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización.**										
	A.11.2.1	**Ubicación y protección de los equipos.**	**Control** **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	NO	Se adopta este control, puesto que se debe reducir el riesgo de que personas no autorizadas puedan acceder a los equipos.			X		**a) establecer que los equipos están ubicados de manera que se minimice el acceso innecesario a las áreas de trabajo;** **b) definir que las instalaciones de procesamiento de la información que manejan datos sensibles están ubicadas cuidadosamente para reducir el riesgo de que personas no autorizadas puedan ver la información durante su uso;** **c) establecer que las instalaciones de almacenamiento se aseguran para evitar el acceso no autorizado;** **d) definir que los elementos que requieren protección especial se salvaguardan para reducir el nivel general de protección requerida;** **e) establecer los controles para minimizar el riesgo de amenazas físicas y ambientales, (robo, incendio, explosivos, humo, agua (o falla en el suministro de agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo);** **f) establecer directrices acerca de comer, consumir líquidos y fumar en cercanías de las instalaciones de procesamiento de información;** **g) hacer seguimiento de las condiciones ambientales tales como temperatura y humedad, para determinar las condiciones que puedan afectar adversamente las instalaciones de procesamiento de información;** **h) proteger contra descargas eléctricas atmosféricas se debe aplicar a todas las edificaciones y se deben colocar filtros a todas las líneas de comunicaciones y de potencia entrantes, para la protección contra dichas descargas;** **i) considerar el uso de métodos de protección especial, tales como membranas para teclados, para equipos en ambientes industriales;** **j) proteger los equipos para procesamiento de información confidencial para minimizar el riesgo de fuga de información debido a emanaciones electromagnéticas.**	M-A-GAC-01 Protocolo de Seguridad Ministerio de Ambiente y Desarrollo Sostenible. M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información.

	A.11.2.2	**Servicio de suministro.**	**Control** **Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.**	SI	NO	Se adopta este control, puesto que las fallas en los servicios de suministro pueden causar pérdida o daño a la información.			X	X	**a) cumplir con las especificaciones de los fabricantes de equipos y con los requisitos legales locales;** **b) evaluar regularmente en cuanto a su capacidad para estar al ritmo del crecimiento e interacciones del negocio con otros servicios de soporte;** **c) inspeccionar y probar regularmente para asegurar su funcionamiento apropiado;** **d) si es necesario, contar con alarmas para detectar mal funcionamiento;** **e) si es necesario, tener múltiples alimentaciones con diverso enrutado físico.**	M-A-GAC-01 Protocolo de Seguridad Ministerio de Ambiente y Desarrollo Sostenible. M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información.
	A.11.2.3	**Seguridad de cableado.**	**Control** **El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debería estar protegido contra interceptación, interferencia o daño.**	SI	NO	Se adopta este control, puesto que se deben reducir los riesgos de interceptación, interferencia o daño en las redes de cableado de la Entidad.			X		**a) establecer que las líneas de potencia y de telecomunicaciones que entran a instalaciones de procesamiento de información deben ser subterráneas en donde sea posible, o deben contar con una protección alternativa adecuada;** **b) establecer que los cables de potencia están separados de los cables de comunicaciones para evitar interferencia;** **c) definir para sistemas sensibles o críticos los controles adicionales que se deben considerar incluyen:** **1) la instalación de conduit apantallado y recintos o cajas con llave en los puntos de inspección y de terminación;** **2) el uso de blindaje electromagnético para proteger los cables;** **3) el inicio de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se conectan a los cables**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI
	A.11.2.4	**Mantenimiento de equipos.**	**Control** **Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.**	SI	NO	Se adopta este control, puesto que es necesario mantener la disponibilidad de la información en la Entidad, se deben mantener adecuadamente los equipos.			X	X	**a) mantener los equipos de acuerdo con los intervalos y especificaciones de servicio recomendados por el proveedor;** **b) establecer que solo el personal de mantenimiento autorizado debería llevar a cabo las reparaciones y el servicio a los equipos;** **c) llevar registros de todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo y correctivo;** **d) implementar los controles apropiados cuando el equipo está programado para mantenimiento, teniendo en cuenta si éste lo lleva a cabo el personal en el sitio o personal externo a la organización; en donde sea necesario, la información confidencial se debe borrar del equipo, o el personal de mantenimiento debería retirarse (cleared) lo suficientemente de la información;** **e) cumplir todos los requisitos de mantenimiento impuestos por las políticas de seguros;** **f) establecer que antes de volver a poner el equipo en operación después de mantenimiento, se debería inspeccionar para asegurarse de que no ha sido alterado y que su funcionamiento es adecuado.**	P-A-GAC-01 - Elaborar y ejecutar el plan de mantenimiento preventivo P-A-GAC-02 - Efectuar mantenimiento correctivo F-A-GAC-03 - Cronograma de Mantenimiento F-A-GTI-06 - Plan de mantenimiento de infraestructura tecnológica M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI P-A-GTI-04 - Gestión de cambios
	A.11.2.5	**Retiro de activos.**	**Control** **Los equipos, información o software no se deben retirar de su sitio sin autorización previa.**	SI	NO	Se adopta este control, puesto que se debe controlar el retiro de los equipos de las oficinas e instalaciones de la Entidad.			X		**a) mantener los equipos de acuerdo con los intervalos y especificaciones de servicio recomendados por el proveedor;** **b) establecer que solo el personal de mantenimiento autorizado debería llevar a cabo las reparaciones y el servicio a los equipos;** **c) llevar registros de todas las fallas reales o sospechadas, y de todo el mantenimiento preventivo y correctivo;** **d) implementar los controles apropiados cuando el equipo está programado para mantenimiento, teniendo en cuenta si éste lo lleva a cabo el personal en el sitio o personal externo a la organización; en donde sea necesario, la información confidencial se debe borrar del equipo, o el personal de mantenimiento debería retirarse (cleared) lo suficientemente de la información;** **e) cumplir todos los requisitos de mantenimiento impuestos por las políticas de seguros;** **f) establecer que antes de volver a poner el equipo en operación después de mantenimiento, se debería inspeccionar para asegurarse de que no ha sido alterado y que su funcionamiento es adecuado.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GAC-01 Protocolo de Seguridad Minambiente F-A-GAC-02 - Autorización salida de elementos F-A-GTI-08 - Hoja de vida de equipos F-A-GAC-04 - Hoja de vida equipos
	A.11.2.6	**Seguridad de los equipos y activos fuera de las instalaciones.**	**Control** **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	NO	Se adopta este control, puesto que el uso de cualquier equipo de almacenamiento y procesamiento de información por fuera de las instalaciones de la Entidad, debe ser aprobado.			X	X	**a) establecer que los equipos y medios retirados de las instalaciones no se deben dejar sin vigilancia en lugares públicos;** **b) seguir en todo momento las instrucciones del fabricante para proteger los equipos, (contra exposición a campos electromagnéticos fuertes);** **c) controlar los lugares fuera de las instalaciones, tales como trabajo en la casa, teletrabajo y sitios temporales se deben determinar mediante una valoración de riesgos y se deben aplicar los controles adecuados según sean apropiados, (gabinetes de archivo con llave, política de escritorio limpio, controles de acceso para computadores y comunicación segura con la oficina);** **d) establecer que cuando el equipo que se encuentra afuera de las instalaciones es transferido entre diferentes individuos y partes externas, llevar un registro que defina la cadena de custodia para el equipo, que incluya al menos los nombres y las organizaciones de los responsables del equipo.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GAC-01 Protocolo de Seguridad Minambiente F-A-GAC-02 - Autorización salida de elementos F-A-GTI-08 - Hoja de vida de equipos F-A-GAC-04 - Hoja de vida equipos
	A.11.2.7	**Disposición segura o reutilización de equipos.**	**Control** **Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.**	SI	NO	Se adopta este control, puesto que antes de la disposición o reúso de los equipos, se debe verificar que estos no contengan información sensible para la Entidad.	X		X		**Se verifica los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. G-A-GTI-04 - Borrado seguro P-A-GAC-12 - Baja y enajenación de bienes del inventario F-A-GTI-08 - Hoja de vida de equipos F-A-GAC-04 - Hoja de vida equipos
	A.11.2.8	**Equipos de usuario desatendido.**	**Control** **Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.**	SI	NO	Se adopta este control, puesto que todos los usuarios deben tomar conciencia de los requisitos y procedimientos de seguridad para proteger los equipos desatendidos.			X		**a) establecer que se cierren las sesiones activas cuando hayan terminado, a menos que se puedan asegurar mediante un mecanismo de bloqueo apropiado (un protector de pantalla protegido con contraseña);** **b) establecer que es obligatorio salir de las aplicaciones o servicios de red cuando ya no los necesiten;** **c) asegurar que los computadores o dispositivos móviles contra uso no autorizado mediante el bloqueo de teclas o un control equivalente (acceso con contraseña, cuando no están en uso).**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. G-E-GET-41 Plan de sensibilización y comunicaciones en seguridad de la información Se implementó política GPO para bloqueo de equipos, tras 5 minutos de inactividad.
	A.11.2.9	**Política de escritorio limpio y pantalla despejada.**	**Control** **Se debería 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	NO	Se adopta este control, puesto que se deben minimizar los riesgos de fuga, robo o daño de la información durante y por fuera de las horas laborales.			X		**a) establecer que la información sensible o crítica del negocio, (sobre papel o en un medio de almacenamiento electrónico), se guarda bajo llave (idealmente, en una caja fuerte o en un gabinete u otro mueble de seguridad) cuando no se requiera, especialmente cuando la oficina esté desocupada.** **b) definir un procedimiento para la gestión de equipos desatendidos; los computadores y terminales deben estar fuera del sistema y estar protegidos con un sistema de bloqueo de la pantalla y el teclado, controlado por una contraseña, token o mecanismo similar de autenticación de usuario, y deben estar protegidos por bloqueo de teclas u otros controles, cuando no están en uso;** **c) evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (escáneres, cámaras digitales);** **d) establecer que los medios que contienen información sensible o clasificada se deben retirar de las impresoras inmediatamente.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información.
	A.12	**SEGURIDAD FÍSICA Y DEL ENTORNO**										
	A.12.1	**PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES**	**Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.**									
	A.12.1.1	**Procedimiento de operación documentados.**	**Control** **Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.**	SI	NO	Se adopta este control, puesto que se deben generar procedimientos para las actividades operacionales asociadas con las instalaciones de procesamiento y comunicación.			X		**a) instalar y configurar sistemas;** **b) establecer el procesamiento y manejo de información, tanto automático como manual;** **c) establecer la gestión de las copias de respaldo;** **d) definir los requisitos de programación, incluidas las interdependencias con otros sistemas, los tiempos de finalización del primer y último trabajos;** **e) establecer las instrucciones para manejo de errores u otras condiciones excepcionales que podrían surgir durante la ejecución del trabajo, incluidas las restricciones sobre el uso de sistemas utilitarios;** **f) definir contactos de apoyo y de una instancia superior, incluidos los contactos de soporte externo, en el caso de dificultades operacionales o técnicas inesperadas;** **g) establecer las instrucciones sobre manejo de medios y elementos de salida, tales como el uso de papelería especial o la gestión de elementos de salida confidenciales, incluidos procedimientos para la disposición segura de elementos de salida de trabajos fallidos;** **h) definir los procedimientos de reinicio y recuperación del sistema para uso en el caso de falla del sistema;** **i) definir la gestión de la información de rastros de auditoria y de información del log del sistema;** **j) establecer los procedimientos de seguimiento.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI Documentación del Proceso GTI y GTE relativa a las operaciones publicados y oficializados en SOMOSIG
	A.12.1.2	**Gestión de cambios.**	**Control** **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	NO	Se adopta este control, puesto que debe existir responsables y procedimientos de gestión formales para asegurar el control satisfactorio de todos los cambios, evitando fallas en el sistema o en la seguridad.			X	X	**a) Identificar y registrar los cambios significativos;** **b) Planificar y puesta a prueba de los cambios;** **c) Valorar los impactos potenciales, incluidos los impactos de estos cambios en la seguridad de la información;** **d) Tener un procedimiento de aprobación formal para los cambios propuestos;** **e) Verificar que se han cumplido los requisitos de seguridad de la información;** **f) Comunicar todos los detalles de los cambios a todas las personas pertinentes;** **g) Tener un procedimiento de apoyo, incluidos procedimientos y responsabilidades para abortar cambios no exitosos y recuperarse de ellos, y eventos no previstos;** **h) Contar con un suministro de un proceso de cambio de emergencia que posibilite la implementación rápida y controlada de los cambios necesarios para resolver un incidente.**	P-A-GTI-04 Procedimiento de Gestión de Cambios M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información.
	A.12.1.3	**Gestión de capacidad.**	**Control** **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	NO	Se adopta este control, puesto que los requisitos de capacidad se deben identificar teniendo en cuenta la criticidad del sistema involucrado, asegurando el desempeño requerido.			X	X	**a) eliminar datos obsoletos (espacio en disco);** **b) realizar cierre definitivo de aplicaciones, sistemas, bases de datos o ambientes;** **c) optimizar cronogramas y procesos de lotes;** **d) optimizar las consultas de bases de datos o lógicas de las aplicaciones;** **e) realizar una negación o restricción de ancho de banda a servicios ávidos de recursos, si estos no son críticos para el negocio (por ejemplo, video en tiempo real).**	P-A-GTI-06 Gestión de la Capacidad M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información.

12. SEGURIDAD DE LAS OPERACIONES	A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación.	**Control** **Se deben separar los ambientes de desarrollo, prueba y producción, para reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.**	SI	NO	Se adopta este control, con el fin de minimizar riesgos en la operación, es necesario implementar la separación de los ambientes de desarrollo, pruebas y producción.			X		**a) definir y documentar las reglas para la transferencia de software del estatus de desarrollo al de operaciones.** **b) establecer que el software de desarrollo y de operaciones debe funcionar en diferentes sistemas o procesadores de computador y en diferentes dominios o directorios;** **c) definir que los cambios en los sistemas operativos y aplicaciones se deben probar en un entorno de pruebas antes de aplicarlos a los sistemas operacionales;** **d) definir que solo en circunstancias excepcionales, las pruebas no se deben llevar a cabo en los sistemas operacionales;** **e) establecer que los compiladores, editores y otras herramientas de desarrollo o utilitarios del sistema no debe ser accesibles desde sistemas operacionales cuando no se requiere;** **f) establecer que los usuarios deben usar diferentes perfiles de usuario para sistemas operacionales y de pruebas, y los menús deben desplegar mensajes de identificación apropiados para reducir el riesgo de error;** **g) definir que los datos sensibles no se debe copiar en el ambiente del sistema de pruebas, a menos que se suministren controles equivalentes para el sistema de pruebas**	M-E-GET-04 Manual de Políticas Especificas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI P-E-GET-12 GESTIONAR PROYECTOS DE TI G-E-GET-42 - Arquitectura de referencia para sistemas de información P-A-GTI-03 - Desarrollar y Mantener Sistemas de Información y Componentes de Software
	A.12.2	**PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS**	**Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos**									
	A.12.2.1	Controles contra códigos maliciosos	**Control** **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	NO	Se adopta este control, puesto que se deben minimizar los riesgos asociados con la obtención de archivos y software que pueda contener código malicioso.			X		**a) establecer una política formal que prohiba el uso de software no autorizado;** **b) implementar controles para evitar o detectar el uso de software no autorizado (listas blancas de aplicaciones);** **b) implementar controles para evitar o detectar el uso de sitios web malicioso o que se sospecha que lo son (listas negras);** **d) establecer una política formal para proteger contra riesgos asociados con la obtención de archivos y de software ya sea mediante redes externas o cualquier otro medio, indicando qué medidas externas se deben tomar;** **e) reducir las vulnerabilidades de las que pueda aprovecharse el software malicioso, (medio de la gestión de la vulnerabilidad técnica);** **f) llevar a cabo revisiones regulares del software y del contenido de datos de los sistemas que apoyan los procesos críticos del negocio; se debería investigar formalmente la presencia de archivos no aprobados o de enmiendas no autorizadas;** **g) instalar y actualizar software de detección y reparación del software malicioso en los computadores y medios como una medida de control, en forma rutinaria**	M-E-GET-04 Manual de Políticas Especificas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI
	A.12.3	**COPIAS DE RESPALDO**	**Objetivo: Proteger contra la pérdida de datos.**									
	A.12.3.1	Respaldo de la información.	**Control** **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	NO	Se adopta este control, puesto que deben existir lineamientos para definir los requisitos de la Entidad para las copias de respaldo de información, software y sistemas.			X	X	**a) producir registros exactos y completos de las copias de respaldo, y procedimientos de restauración documentados;** **b) establecer la cobertura (copias de respaldo completas o diferenciales) y la frecuencia con que se hagan las copias de respaldo debe reflejar los requisitos del negocio de la organización, los requisitos de la seguridad de la información involucrada, y la criticidad de la información para la operación continua de la organización;** **c) definir las copias de respaldo se debe almacenar en un lugar remoto, a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en el sitio principal;** **d) establecer la información de respaldo y un nivel apropiado de protección física y del entorno, de coherencia con las normas aplicadas en el sitio principal;** **e) definir los medios de respaldo se debe poner a prueba regularmente para asegurar que se puede depender de ellos para uso de emergencia en caso necesario; esto se debería combinar con una prueba de los procedimientos de restauración, y se debe verificar contra el tiempo de restauración requerido.** **f) definir las situaciones en las que la confidencialidad tiene importancia, las copias de respaldo deben estar protegidas por medio de encriptación.**	I-A-GTI-02 Instructivo para la generación de copias de respaldo BACK-UP P-A-GTI-05 Procedimiento de Respaldo (back-up) M-E-GET-04 Manual de Políticas Especificas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI
	A.12.4	**REGISTRO (LOGGING) Y SEGUIMIENTO**	**Objetivo: Registro de eventos y generar evidencia.**									
	A.12.4.1	Registro de eventos.	**Control** **Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.**	SI	NO	Se adopta este control, puesto que es necesario monitorear las actividades de usuario, excepciones, fallas y eventos de seguridad con el fin de generar alertas sobre la seguridad del sistema y poder tomar acciones correspondientes.			X		**a) identificar los usuarios;** **b) establecer las actividades del sistema;** **c) definir las fechas, horas y detalles de los eventos clave, (entrada y salida);** **d)identificar el dispositivo o ubicación, si es posible, e identificador del sistema;** **e) tener registros de intentos de acceso al sistema exitosos y rechazados;** **e) definir registros de datos exitosos y rechazados y otros intentos de acceso a recursos;** **g) establecer los cambios a la configuración del sistema;** **h) definir el uso de privilegios;** **i) establecer el uso de utilitarios y aplicaciones del sistema;** **j) definir los archivos a los que se tuvo acceso, y el tipo de acceso;** **k) establecer las direcciones y protocolos de red;** **l) definir las alarmas accionadas por el sistema de control de acceso;** **m) activar y desactivar los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusión;** **n) registrar las transacciones ejecutadas por los usuarios en las aplicaciones.**	M-E-GET-04 Manual de Políticas Especificas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI
	A.12.4.2	Protección de la información de registro.	**Control** **Los sistemas de gestión de registros (Logging Facilities) y la información de registro (Log Información) se deben proteger contra alteración y acceso no autorizado.**	SI	NO	Se adopta este control, puesto que es necesario proteger los sistemas contra los cambios no autorizados de la información de registro.			X		**a) verificar todas las alteraciones a los tipos de mensaje que se registran;** **b) establecer los archivos log que son editados o eliminados;** **c) verificar cuando se excede la capacidad de almacenamiento del medio de archivo log, lo que da como resultado falla en el registro de eventos, o sobre escritura de eventos pasados registrados.**	M-E-GET-04 Manual de Políticas Especificas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI
	A.12.4.3	Registros del administrador y operador.	**Control** **Las actividades del administrador y del operador del sistema se deben registrar (Logged), y los registros (Logs) se deben proteger y revisar con regularidad.**	SI	NO	Se adopta este control, puesto que los titulares de cuenta de usuario con privilegios, pueden estar en capacidad de manipular los registros en los sistemas bajo su control, por ello es necesario proteger y revisar los registros para mantener la integridad de los registros que pueden ser modificados por usuarios con privilegios.			X		**Revisar los registros de las actividades del administrador y del operador del sistema, los registros se deben proteger y revisar con regularidad.**	M-E-GET-04 Manual de Políticas Especificas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI
	A.12.4.4	Sincronización de relojes.	**Control** **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	NO	Se adopta este control, puesto que se debe documentar e implementar el enfoque de la Entidad para obtener un tiempo de referencia de una sola fuente y sincronizar confiablemente los relojes internos de los sistemas.			X	X	**Se deben sincronizar los relojes con una única fuente de referencia de tiempo 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.**	M-E-GET-04 Manual de Políticas Especificas de Seguridad de la Información. Se cuenta con servidor NTP para sincronización de relojes.
	A.12.5	**CONTROL DE SOFTWARE OPERACIONAL**	**Objetivo: Asegurar la integridad de los sistemas operativos (Operational Systems)**									
	A.12.5.1	**12.5.1 Instalación de software en sistemas operativos (Operational Systems)**	**Control** **Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos (Operational Systems**	SI	NO	Se adopta este control, puesto que se deben controlar los cambios de software en los sistemas operativos para minimizar riesgos de seguridad.			X		**a) actualizar el software operacional, aplicaciones y bibliotecas de programas solo la debe llevar a cabo administradores entrenados, con autorización apropiada de la dirección;** **b) definir que los sistemas operacionales solo debe contener códigos ejecutables aprobados, no el código de desarrollo o compiladores;** **c) establecer que las aplicaciones y el software del sistema operativo solo se debe implementar después de pruebas extensas y exitosas; los ensayos deben abarcar la usabilidad, la seguridad, los efectos sobre otros sistemas y la facilidad de uso, y se debe llevar a cabo en sistemas separados; se debe asegurar que todas las bibliotecas de fuentes de programas correspondientes hayan sido actualizadas;** **d) usar un sistema de control de la configuración para mantener el control de todo el software implementado, al igual que la documentación del sistema;** **e) establecer una estrategia de retroceso (rollback) antes de implementar los cambios;** **f) mantener un log de auditoría de todas las actualizaciones de las bibliotecas de programas operacionales;** **g) definir las versiones anteriores del software de aplicación se deben conservar como una medida de contingencia;** **h) establecer que las versiones de software anteriores se deben llevar al archivo permanente, junto con toda la información y parámetros, procedimientos, detalles de configuración y software de soporte anteriores, en tanto los datos permanezcan en el archivo permanente.**	M-E-GET-04 Manual de Políticas Especificas de Seguridad de la Información.
	A.12.6	**GESTIÓN DE LA VULNERABILIDAD TÉCNICA**	**Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.**									
	A.12.6.1	**Gestión de las vulnerabilidades técnicas**	**Control** **Se debería 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	NO	Se adopta este control, puesto que se deben tomar acciones apropiadas y oportunas en respuesta a la identificación de vulnerabilidades técnicas potenciales.			X		**a) definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, la colocación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida;** **b) definir los recursos de información que se usarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la toma de conciencia acerca de ellos se debe identificar para el software y otra tecnología;** **c) una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas pertinentes potencialmente;** **d) establecer que una vez que se haya identificado una vulnerabilidad técnica potencial, la organización debería identificar los riesgos asociados y las acciones por tomar; esta acción puede involucrar la colocación de parches de sistemas vulnerables o la aplicación de otros controles; Si no es posible colocar controles se deben documentar en los riesgos de acuerdo a su probabilidad e impacto y colocarlo como riesgo aceptado.** **e) definir dependiendo de la urgencia con la que se necesite tratar una vulnerabilidad técnica, la acción tomada se debería llevar a cabo de acuerdo con los controles relacionados con la gestión de cambios, o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información;** **f) establecer, si está disponible un parche de una fuente legítima, se debe valorar los riesgos asociados con la instalación del parche (los riesgos que acarrea la vulnerabilidad se debe comparar con el riesgo de instalar el parche);** **g) establecer que los parches se deben probar y evaluar antes de su instalación, para asegurarse de que son eficaces y no producen efectos secundarios que no se puedan tolerar; si no hay parches disponibles,**	P-A-GTI-10 - Análisis Periódico de Vulnerabilidades M-E-GET-04 Manual de Políticas Especificas de Seguridad de la Información.
	A.12.6.2	**Restricciones sobre la instalación de software**	**Control** **Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios**	SI	NO	Se adopta este control, puesto que es necesario tener lineamientos respecto del software que pueden instalar los usuarios.			X		**Revisar las restricciones y las reglas para la instalación de software por parte de los usuarios.**	M-E-GET-04 Manual de Políticas Especificas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI. Se tienen implementadas políticas GPO desde el Directorio Activo para evitar la instalación y desinstalación de software.
	A.12.7	**GESTIÓN DE LA VULNERABILIDAD TÉCNICA**	**Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos(Operational Systems)**	SI	NO							
	A.12.7.1	**Controles sobre auditorías de sistemas de información**	**Control** **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	NO	Se adopta este control, puesto que los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos de la Entidad.			X		**a) establecer los requisitos de auditoría para acceso a sistemas y a datos se debe acordar con la dirección apropiada;** **b) definir el alcance de las pruebas técnicas de auditoría se debe acordar y controlar;** **c) establecer las pruebas de auditoría se debe limitar a acceso a software y datos únicamente para lectura;** **d) definir el acceso diferente al de solo lectura solamente se debe prever para copias aisladas de los archivos del sistema, que se deben borrar una vez que la auditoría haya finalizado, o se debe proporcionar información apropiada si hay obligación de mantener estos archivos bajo los requisitos de documentación de auditoría;** **e) definir los requisitos para procesos especiales y adicionales se debe identificar y acordar;** **f) establecer las pruebas de auditoría que puedan afectar la disponibilidad del sistema se deben realizar fuera de horas laborales;** **g) hacer seguimiento de todos los accesos y logged para producir un rastro de referencia.**	M-E-GET-04 Manual de Políticas Especificas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI.
	A.13	**SEGURIDAD DE LAS COMUNICACIONES**										
	A.13.1	**GESTIÓN DE LA SEGURIDAD DE LAS REDES**	**Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.**									

13. SEGURIDAD DE LAS COMUNICACIONES	**A.13.1.1**	**Controles de redes**	**Control.** **Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones**	SI	NO	Se adopta este control, puesto que se deben implementar controles para asegurar la seguridad de la información en las redes y la protección de servicios relacionados contra el acceso no autorizado.			X	**a) establecer las responsabilidades y procedimientos para la gestión de equipos de redes;** **b) definir la responsabilidad operacional por las redes se debería separar de las operaciones informáticas, en donde sea apropiado;** **c) establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan sobre redes públicas o sobre redes inalámbricas, y para proteger los sistemas y aplicaciones conectados;** **d) gestionar el acceso remoto** **d) aplicar logging y seguimiento adecuados para posibilitar el registro y detección de acciones que pueden afectar, o son pertinentes a la seguridad de la información;** **e) definir las actividades de gestión a coordinar estrechamente tanto para optimizar el servicio de la organización, como para asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información;** **f) establecer los sistemas en la red que se autenticar;** **g) restringir la conexión de los sistemas a la red.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI.
	A.13.1.2	**Seguridad de los servicios de red**	**Control.** **Se debe 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 servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.**	SI	NO	Se adopta este control, puesto que es necesario verificar la seguridad de los servicios de red, identificando los acuerdos, niveles de servicio y requisitos de gestión.			X	**a) establecer la tecnología aplicada a la seguridad de servicios de red, tales como autenticación, encriptación y controles de conexión de red;** **b) definir los parámetros técnicos requeridos para la conexión segura con los servicios de red de acuerdo con las reglas de conexión de seguridad y de red;** **c) establecer los procedimientos para el uso de servicios de red para restringir el acceso a los servicios o aplicaciones de red, cuando sea necesario.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI.
	A.13.1.3	**Separación en las redes**	**Control.** **Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.**	SI	NO	Se adopta este control, puesto que es necesario realizar una buena gestión de seguridad de las redes, definiendo los segmentos de red y su correspondiente control de acceso de usuarios.			X	**De acuerdo a NIST se debe proteger la integridad de las redes incorporando segregación donde se requiera.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI.
	A.13.2	**TRANSFERENCIA DE INFORMACIÓN**	**Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.**								
	A.13.2.1	**Políticas y procedimientos de transferencia de información**	**Control.** **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 comunicación.**	SI	NO	Se adopta este control, puesto que deben existir lineamientos para proteger la información transferida contra interceptación, copiado, modificación y destrucción.	X	X	X	**a) definir los procedimientos diseñados para proteger la información transferida contra interceptación, copiado, modificación, enrutado y destrucción;** **b) definir los procedimientos para la detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas;** **c) definir los procedimientos para proteger información electrónica sensible comunicada que están como adjuntos;** **d) establecer la política o directrices que presentan el uso aceptable de las instalaciones de comunicación;** **e) definir las responsabilidades del personal, las partes externas y cualquier otro usuario no comprometer a la organización, (por difamación, acoso, suplantación, envío de cadenas, compras no autorizadas, etc.);** **f) establecer el uso de técnicas criptográficas, (proteger la confidencialidad, la integridad y la autenticidad de la información).** **g) establecer las directrices sobre retención y disposición para toda la correspondencia del negocio, incluidos mensajes, de acuerdo con la legislación y reglamentaciones locales y nacionales;** **h) definir los controles y restricciones asociadas con las instalaciones de comunicación, (el reenvío automático de correo electrónico a direcciones de correo externas);** **i) brindar asesoría al personal para que tome las precauciones apropiadas acerca de no revelar información confidencial;** **j) no dejar mensajes que contengan información confidencial, en las máquinas contestadoras, ya que éstos pueden ser escuchados por personas no autorizadas, almacenados en sistemas comunales o almacenados incorrectamente como resultado de una marcación incorrecta;**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información.
	A.13.2.2	**Acuerdos sobre transferencia de información**	**Control.** **Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.**	SI	NO	Se adopta este control, puesto que deben definir lineamientos y acuerdos entre la Entidad y partes externas para la transferencia segura de la información.	X	X	X	**a) establecer las responsabilidades de la dirección para controlar y notificar la transmisión, despacho y recibo;** **b) definir los procedimientos para asegurar trazabilidad y no repudio;** **c) definir los estándares técnicos mínimos para empaquetado y transmisión;** **d) tener certificados de depósito de títulos en garantía;** **e) establecer los estándares de identificación de mensajería;** **f) definir las responsabilidades y obligaciones en el caso de incidentes de seguridad de la información, tales como pérdidas de datos;** **g) establecer el uso de un sistema de etiquetado acordado para información sensible o crítica, que asegure que el significado de la etiqueta se entiende de inmediato, y que la información está protegida apropiadamente;** **h) definir las normas técnicas para registro y lectura de información y software;** **i) cualquier control especial que se requiera para proteger elementos críticos, tales como criptografía;** **j) mantener una cadena de custodia para la información mientras está en tránsito;** **k) definir los niveles aceptables de control de acceso.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-09 Gestión de incidentes de seguridad y privacidad de la información. F-A-GTI-10 Valoración de incidentes de seguridad y privacidad de la información.
	A.13.2.3	**Mensajería electrónica**	**Control** **Se debe proteger adecuadamente la información incluida en la mensajería electrónica.**	SI	NO	Se adopta este control, puesto que se deben implementar controles para asegurar la información que se envía a través de mensajería electrónica.	X		X	**a) definir la protección de mensajes contra acceso no autorizado, modificación o denegación del servicio proporcionales al esquema de clasificación adoptado por la organización;** **b) asegurar el direccionamiento y transporte correctos del mensaje;** **c) establecer la confiabilidad y disponibilidad del servicio;** **d) definir las consideraciones legales, (los requisitos para firmas electrónicas;** **e) establecer la obtención de aprobación antes de usar servicios públicos externos como mensajería instantánea, redes sociales o intercambio de información);** **f) definir niveles más fuertes de autenticación para control del acceso desde redes accesibles públicamente.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información.
	A.13.2.4	**Acuerdos de confidencialidad o de no divulgación**	**Control** **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	NO	Se adopta este control, puesto que debe existir un acuerdo de confidencialidad para funcionarios, contratistas o terceros que tengan acceso a la información de la Entidad, el cual debe tener en cuenta los requisitos para proteger la información confidencial y las premisas frente a su divulgación.	X	X	X	**a) definir la información que se va a proteger (información confidencial);** **b) determinar la duración esperada de un acuerdo, incluidos los casos en los que podría ser necesario mantener la confidencialidad indefinidamente;** **c) establecer las acciones requeridas cuando termina el acuerdo;** **d) definir las responsabilidades y acciones de los firmantes para evitar la divulgación no autorizada de información;** **e) definir la propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de información confidencial;** **f) definir el uso permitido de información confidencial y los derechos del firmante para usar la información;** **g) establecer el derecho a actividades de auditoría y de seguimiento que involucran información confidencial;** **h) definir el proceso de notificación y reporte de divulgación no autorizada o fuga de información confidencial;** **i) definir los plazos para que la información sea devuelta o destruida al cesar el acuerdo;** **j) establecer las acciones que se espera tomar en caso de violación del acuerdo.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-CTR-01 Manual de contratación F-A-CTR-36 Acta de compromiso de confidencialidad
	A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**									
	A.14.1	**REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN**	**Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.**								
	A.14.1.1	**Análisis y especificación de requisitos de seguridad de la información**	**Control** **Los requisitos relacionados con seguridad de la información se debe incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.**	SI	NO	Se adopta este control, puesto que los requisitos de seguridad de la información se deben identificar e incluir en los requisitos para nuevos sistemas teniendo en cuenta las políticas y directrices de la Entidad.	**X**		**X**	**a) establecer el nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario.** **b) definir los procesos de suministro de acceso y de autorización para usuarios del negocio, al igual que para usuarios privilegiados o técnicos;** **c) informar a los usuarios y operadores sobre sus deberes y responsabilidades;** **d) definir las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad, integridad;** **e) definir los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso y seguimiento, y de no repudio;** **f) establecer los requisitos exigidos por otros controles de seguridad, (interfaces con el ingreso o seguimiento, o los sistemas de detección de fuga de datos).**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI. I-E-GET-02 Metodología para la identificación gestión y clasificación de activos de información
	A.14.1.2	**Seguridad de servicios de las aplicaciones en redes públicas**	**Control.** **La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.**	SI	NO	Se adopta este control, puesto que se debe mantener la confidencialidad, integridad y disponibilidad de la información, cuando esta pasa a través de redes públicas.		X	X	X	**a) definir el nivel de confianza que cada parte requiere con relación a la identidad declarada por la otra parte, (por medio de autenticación);** **b) establecer los procesos de autorización asociados con quien puede aprobar el contenido o expedir o firmar documentos transaccionales clave;** **c) asegurar que los socios de comunicación estén completamente informados de sus autorizaciones para suministro o uso del servicio;** **d) determinar y cumplir los requisitos para confidencialidad, integridad, prueba de despacho y recibo de documentos clave y el no repudio de los contratos, (asociados con procesos de ofertas y contratos);** **e) definir el nivel de confianza requerido en la integridad de los documentos clave;** **f) establecer los requisitos de protección de cualquier información confidencial;** **g) definir la confidencialidad e integridad de cualquier transacción de pedidos, información de pagos, detalles de la dirección de entrega y confirmación de recibos;** **h) definir el grado de verificación apropiado de la información de pago suministrada por un cliente;** **i) seleccionar la forma de arreglo de pago más apropiado para protegerse contra fraude;** **j) definir el nivel de protección requerido para mantener la confidencialidad e integridad de la información del pedido;** **k) evitar la pérdida o duplicación de información de la transacción;** **l) definir la responsabilidad civil asociada con cualquier transacción fraudulenta;** **m) establecer los requisitos de seguros.** **n) De acuerdo a NIST se deben usar mecanismos de chequeo de las integridad para verificar la integridad del software, firmware, e información**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI. I-E-GET-02 Metodología para la identificación gestión y clasificación de activos de información
	A.14.1.3	**Protección de transacciones de los servicios de las aplicaciones (Application Services)**	**Control.** **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	NO	Se adopta este control, puesto que es necesario considerar controles de seguridad para la información involucrada en las transacciones de los servicios de las aplicaciones y protegerla para evitar la transmisión incompleta, divulgación no autorizada, entre otros.	X		X	**a) definir el uso de firmas electrónicas por cada una de las partes involucradas en la transacción;** **b) establecer todos los aspectos de la transacción, es decir, asegurar que:** **1) definir la información de autenticación secreta de usuario, de todas las partes, se valide y verifique;** **2) definir a transacción permanezca confidencial;** **3) mantener la privacidad asociada con todas las partes involucradas;** **c) definir la trayectoria de las comunicaciones entre todas las partes involucradas esté encriptada;** **d) definir los protocolos usados para comunicarse entre todas las partes involucradas estén asegurados;** **e) asegurar que el almacenamiento de los detalles de la transacción esté afuera de cualquier entorno accesible públicamente, (en una plataforma de almacenamiento existente en la intranet de la organización, y no retenido ni expuesto en un medio de almacenamiento accesible directamente desde Internet);** **f) utilizar una autoridad confiable (para los propósitos de emitir y mantener firmas digitales o certificados digitales), la seguridad está integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. M-A-GTI-02 Manual general de operaciones de infraestructura de TI.
	A.14.2	**SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE**	**Objetivo: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.**								
	A.14.2.1	**Política de desarrollo seguro**	**Control** **Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.**	SI	NO	Se adopta este control, puesto que se deben tener lineamientos para desarrollo de software o sistemas dentro de la Entidad.	X		X	**a) definir la seguridad del ambiente de desarrollo;** **b) orientar la seguridad en el ciclo de vida de desarrollo del software:** **1) definir la seguridad en la metodología de desarrollo de software;** **2) establecer las directrices de codificación seguras para cada lenguaje de programación usado;** **c) definir los requisitos de seguridad en la fase diseño;** **d) definir los puntos de chequeo de seguridad dentro de los hitos del proyecto;** **e) establecer los depósitos seguros;** **f) definir la seguridad en el control de la versión;** **g) establecer el conocimiento requerido sobre seguridad de la aplicación;** **h) definir la capacidad de los desarrolladores para evitar, encontrar y resolver las vulnerabilidades.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-03 Desarrollar y Mantener Sistemas de Información y Componentes de Software I-A-GTI-03 Instructivo Para la Elaboración de Arquitecturas de Software I-A-GTI-06 Instructivo de historias de usuario I-A-GTI-05 Instructivo de Casos de Prueba I-A-GTI-08 Instructivo Informe de Ejecución de Casos de Prueba I-A-GTI-04 Instructivo para la elaboración de manuales de despliegue

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	A.14.2.2	**Procedimientos de control de cambios en sistemas**	**Control** **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	NO	Se adopta este control, puesto que se requiere implementar procedimientos formales de control de cambios.	X		X		**a) llevar un registro de los niveles de autorización acordados;** **b) asegurar que los cambios se presenten a los usuarios autorizados;** **c) revisar los controles y procedimientos de integridad para asegurar que no se vean comprometidos por los cambios;** **d) identificar todo el software, información, entidades de bases de datos y hardware que requieren corrección;** **e) identificar y verificar el código crítico de seguridad para minimizar la posibilidad de debilidades de seguridad conocidas;** **f) obtener aprobación formal para propuestas detalladas antes de que el trabajo comience;** **g) revisar antes de la implementación, asegurar que los usuarios autorizados aceptan los cambios;** **h) asegurar que el conjunto de documentación del sistema está actualizado al completar cada cambio, y que la documentación antigua se lleva al archivo permanente, o se dispone de ella;** **i) mantener un control de versiones para todas las actualizaciones de software;** **j) mantener un rastro de auditoría de todas las solicitudes de cambio;** **k) asegurar que la documentación de operación y los procedimientos de los usuarios experimenten los cambios que les permitan seguir siendo apropiados;** **l) asegurar que la implementación de los cambios ocurre en el momento correcto y no afecta los procesos de negocio involucrados.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-04 Procedimiento de gestión de cambios P-A-GTI-03 Desarrollar y Mantener Sistemas de Información y Componentes de Software I-A-GTI-03 Instructivo Para la Elaboración de Arquitecturas de Software I-A-GTI-06 Instructivo de historias de usuario I-A-GTI-05 Instructivo de Casos de Prueba I-A-GTI-08 Instructivo Informe de Ejecución de Casos de Prueba I-A-GTI-04 Instructivo para la elaboración de manuales de despliegue
	A.14.2.3	**Revisión técnica de las aplicaciones después de cambios en la plataforma de operación**	**Control** **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	NO	Se adopta este control, para garantizar la adecuada gestión de cambios en las plataformas.	X		X		**a) revisar los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones;** **b) asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación;** **c) asegurar que se hacen cambios apropiados en los planes de continuidad del negocio.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-04 Procedimiento de gestión de cambios P-A-GTI-03 Desarrollar y Mantener Sistemas de Información y Componentes de Software I-A-GTI-03 Instructivo Para la Elaboración de Arquitecturas de Software I-A-GTI-06 Instructivo de historias de usuario I-A-GTI-05 Instructivo de Casos de Prueba I-A-GTI-08 Instructivo Informe de Ejecución de Casos de Prueba I-A-GTI-04 Instructivo para la elaboración de manuales de despliegue P-E-GET-12 Gestionar Proyectos de TI
	A.14.2.4	**Restricciones en los cambios a los paquetes de software**	**Control** **Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente**	SI	NO	Se adopta este control, puesto que es necesario usar paquetes de software suministrados directamente por el proveedor o fabricante garantizando que no hayan sufrido modificaciones.	X		X		**a) definir el riesgo de que los procesos de integridad y los controles incluidos se vean comprometidos;** **b) obtener el consentimiento del vendedor;** **c) obtener del vendedor los cambios requeridos, a medida que se actualiza el programa estándar;** **d) evaluar el impacto, si la organización llega a ser responsable del mantenimiento futuro del software como resultado de los cambios;** **e) definir la compatibilidad con otro software en uso.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-04 Procedimiento de gestión de cambios P-A-GTI-03 Desarrollar y Mantener Sistemas de Información y Componentes de Software I-A-GTI-03 Instructivo Para la Elaboración de Arquitecturas de Software I-A-GTI-06 Instructivo de historias de usuario I-A-GTI-05 Instructivo de Casos de Prueba I-A-GTI-08 Instructivo Informe de Ejecución de Casos de Prueba I-A-GTI-04 Instructivo para la elaboración de manuales de despliegue P-E-GET-12 Gestionar Proyectos de TI
	A.14.2.5	**Principios de construcción de sistemas seguros**	**Control** **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	NO	Se adopta este control, puesto que deben existir lineamientos para la construcción segura de sistemas de información.	X		X		**Revisar la documentación y los principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-04 Procedimiento de gestión de cambios P-A-GTI-03 Desarrollar y Mantener Sistemas de Información y Componentes de Software I-A-GTI-03 Instructivo Para la Elaboración de Arquitecturas de Software I-A-GTI-06 Instructivo de historias de usuario I-A-GTI-05 Instructivo de Casos de Prueba I-A-GTI-08 Instructivo Informe de Ejecución de Casos de Prueba I-A-GTI-04 Instructivo para la elaboración de manuales de despliegue P-E-GET-12 Gestionar Proyectos de TI
	A.14.2.6	**Ambiente de desarrollo seguro**	**Control** **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	NO	Se adopta este control, puesto que se debe mantener y proteger los ambientes de desarrollo.	X		X		**a) carácter sensible de los datos que el sistema va a procesar, almacenar y transmitir;** **b) definir los requisitos externos e internos aplicables, (reglamentaciones o políticas);** **c) definir los controles de seguridad ya implementados por la organización, que brindan soportar al desarrollo del sistema;** **d) establecer la confiabilidad del personal que trabaja en el ambiente;** **e) definir el grado de contratación externa asociado con el desarrollo del sistema;** **f) definir la necesidad de separación entre diferentes ambientes de desarrollo;** **g) definir el control de acceso al ambiente de desarrollo;** **h) establecer el seguimiento de los cambios en el ambiente y en los códigos almacenados ahí;** **i) definir las copias de respaldo se almacenan en lugares seguros fuera del sitio;** **j) definir el control sobre el movimiento de datos desde y hacia el ambiente.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-04 Procedimiento de gestión de cambios P-A-GTI-03 Desarrollar y Mantener Sistemas de Información y Componentes de Software I-A-GTI-03 Instructivo Para la Elaboración de Arquitecturas de Software I-A-GTI-06 Instructivo de historias de usuario I-A-GTI-05 Instructivo de Casos de Prueba I-A-GTI-08 Instructivo Informe de Ejecución de Casos de Prueba I-A-GTI-04 Instructivo para la elaboración de manuales de despliegue P-E-GET-12 Gestionar Proyectos de TI
	A.14.2.7	**Desarrollo contratado externamente**	**Control** **La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.**	SI	NO	Se adopta este control, para el desarrollos contratados externamente, por lo cual se deben considerar aspectos de seguridad en toda la cadena de suministro.	X		X		**a) definir los acuerdos de licenciamiento, propiedad de los códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente;** **b) establecer los requisitos contractuales para prácticas seguras de diseño, codificación y pruebas;** **c) definir el suministro del modelo de amenaza aprobado, al desarrollador externo;** **d) realizar los ensayos de aceptación para determinar la calidad y exactitud de los entregables;** **e) definir la evidencia de que se usaron umbrales de seguridad para establecer niveles mínimos aceptables de calidad de la seguridad y de la privacidad;** **f) definir la evidencia de que se han hecho pruebas suficientes para proteger contra contenido malicioso intencional y no intencional en el momento de la entrega;** **g) definir la evidencia de que se han hecho pruebas suficientes para proteger contra la presencia de vulnerabilidades conocidas;** **h) definir los certificados de depósito de títulos en garantía; (el código fuente ya no está disponible);** **i) establecer el derecho contractual con relación a procesos y controles de desarrollo de auditorías;** **j) documentar eficaz del ambiente de construcción usado para crear entregables;** **k) establecer que la organización es responsable de la conformidad con las leyes aplicables y con la verificación de la eficiencia del control.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-04 Procedimiento de gestión de cambios P-A-GTI-03 Desarrollar y Mantener Sistemas de Información y Componentes de Software I-A-GTI-03 Instructivo Para la Elaboración de Arquitecturas de Software I-A-GTI-06 Instructivo de historias de usuario I-A-GTI-05 Instructivo de Casos de Prueba I-A-GTI-08 Instructivo Informe de Ejecución de Casos de Prueba I-A-GTI-04 Instructivo para la elaboración de manuales de despliegue P-E-GET-12 Gestionar Proyectos de TI
	A.14.2.8	**Pruebas de seguridad de sistemas**	**Control** **Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad**	SI	NO	Se adopta este control, puesto que los desarrollos requieren pruebas de funcionalidad y de seguridad durante el ciclo de desarrollo.	X		X		**Para pasar a producción los desarrollos se realizan pruebas de seguridad. También verifique que los procesos de detección de incidentes son probados periódicamente.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-04 Procedimiento de gestión de cambios P-A-GTI-03 Desarrollar y Mantener Sistemas de Información y Componentes de Software I-A-GTI-03 Instructivo Para la Elaboración de Arquitecturas de Software I-A-GTI-06 Instructivo de historias de usuario I-A-GTI-05 Instructivo de Casos de Prueba I-A-GTI-08 Instructivo Informe de Ejecución de Casos de Prueba I-A-GTI-04 Instructivo para la elaboración de manuales de despliegue P-E-GET-12 Gestionar Proyectos de TI
	A.14.2.9	**Prueba de aceptación de sistemas**	**Control** **Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.**	SI	NO	Se adopta este control, puesto que se requiere definir los criterios de aceptación y pruebas de los sistemas de información.	X	X	X		**Revisar las pruebas de aceptación de sistemas, para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-04 Procedimiento de gestión de cambios P-A-GTI-03 Desarrollar y Mantener Sistemas de Información y Componentes de Software I-A-GTI-03 Instructivo Para la Elaboración de Arquitecturas de Software I-A-GTI-06 Instructivo de historias de usuario I-A-GTI-05 Instructivo de Casos de Prueba I-A-GTI-08 Instructivo Informe de Ejecución de Casos de Prueba I-A-GTI-04 Instructivo para la elaboración de manuales de despliegue P-E-GET-12 Gestionar Proyectos de TI
	A.14.3	**DATOS DE PRUEBA**	**Objetivo: Asegurar la protección de los datos usados para pruebas**									
	A.14.3.1	**Protección de datos de prueba**	**Control** **Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente**	SI	NO	Se adopta este control, puesto que se requiere que los datos de prueba se seleccionen, protejan y controlen cuidadosamente.		X	X		**a) establecer los procedimientos de control de acceso, que se aplican a los sistemas de aplicación operacionales, se debe aplicar también a los sistemas de aplicación de pruebas;** **b) tener una autorización separada cada vez que se copia información operacional a un ambiente de pruebas;** **c) definir que la información operacional se debe borrar del ambiente de pruebas inmediatamente después de finalizar las pruebas;** **d) establecer que el copiado y uso de la información operacional se debe logged para suministrar un rastro de auditoría.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-04 Procedimiento de gestión de cambios P-A-GTI-03 Desarrollar y Mantener Sistemas de Información y Componentes de Software I-A-GTI-03 Instructivo Para la Elaboración de Arquitecturas de Software I-A-GTI-06 Instructivo de historias de usuario I-A-GTI-05 Instructivo de Casos de Prueba I-A-GTI-08 Instructivo Informe de Ejecución de Casos de Prueba I-A-GTI-04 Instructivo para la elaboración de manuales de despliegue P-E-GET-12 Gestionar Proyectos de TI
	A. 15	**RELACIONES CON LOS PROVEEDORES**										
	A.15.1	**SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES**	**Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores**									

15. RELACIONES CON LOS PROVEEDORES	A.15.1.1	**Política de seguridad de la información para las relaciones con proveedore**	**Control** **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	NO	Se adopta este control, puesto que se deben definir lineamientos en los que se identifique y exija controles de seguridad de la información para el acceso de los proveedores a la información de la Entidad.	X	X	X		**1) Verifique la política de seguridad de la información para las relaciones con los proveedores, que indique los requisitos de SI para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización, esta política debe reflejarse en los acuerdos con los proveedores que deben estar documentados.** **2) Verifique en la muestra de proveedores con acceso a los activos de información (no necesariamente son proveedores de tecnología de la información, por ejemplo pueden ser proveedores que tengan por ejemplo un proceso de nomina en outsourcing), se hayan suscrito acuerdos (ANS) formales donde se establezcan y acuerden todos los requisitos de seguridad de la información pertinentes con cada proveedor.** **3) Verifique para los proveedores si se tiene en cuenta los riesgos de SI asociados a la cadena de suministro, por ejemplo para los proveedores en la nube es muy común que se apoyen en otros proveedores para proporcionar las instalaciones y se deben manejar los riesgos asociados a este tercero con el cual la entidad no tiene una relación comercial directa. Solicite que le indiquen como identifican para cada proveedor su cadena de suministro y obtenga evidencia de este hecho.**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información F-A-CTR-36 Acta de compromiso de confidencialidad F-A-CTR-55 Informe Periódico de supervisión. P-A-GTI-04 procedimiento de gestión de cambios F-A-CTR-21 Modelo Contrato Prestación de Servicios F-A-CTR-64 Estudios Previos F-A-CTR-52 Estudio previo contrato de prestación de servicios F-A-CTR-56 Informe de presunto incumplimiento F-A-CTR-69 Requerimiento por presunto incumplimiento del contrato F-A-CTR-27 Ficha técnica
	A.15.1.2	**Tratamiento de la seguridad dentro de los acuerdos con proveedores**	**Control** **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	NO	Se adopta este control, puesto que de requiere acordar con los proveedores lo concerniente a la cadena de suministro de componentes o infraestructura de TI.	X	X	X		**1) Indague y solicite evidencia en una muestra de proveedores seleccionada, como la entidad hace seguimiento, revisa y audita con regularidad de acuerdo a la política la prestación de servicios de los proveedores y el cumplimiento de los compromisos respecto a la seguridad de la información.** **2) Indague y evidencie como se gestionan 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, los incidentes de seguridad de la información y la revaloración de los riesgos.**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información F-A-CTR-36 Acta de compromiso de confidencialidad F-A-CTR-55 Informe Periódico de supervisión. P-A-GTI-04 procedimiento de gestión de cambios F-A-CTR-21 Modelo Contrato Prestación de Servicios F-A-CTR-64 Estudios Previos F-A-CTR-52 Estudio previo contrato de prestación de servicios F-A-CTR-56 Informe de presunto incumplimiento F-A-CTR-69 Requerimiento por presunto incumplimiento del contrato F-A-CTR-27 Ficha técnica
	A.15.1.3	**Cadena de suministro de tecnología de información y comunicación.**	**Control** **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	NO	Se adopta este control, puesto que se deben incluir requisitos para tratar los riesgos de seguridad de la información derivados de la cadena de suministro de servicios y componentes de TI.	X	X	X		**a) definir los requisitos de seguridad de la información para aplicar a la adquisición de productos o servicios de tecnología de la información y de comunicaciones, además de los requisitos generales de seguridad de la información para las relaciones con los proveedores;** **b) para los servicios de tecnología de información y de comunicaciones, exigir que los proveedores divulguen los requisitos de seguridad de la organización a lo largo de la cadena de suministro, si los proveedores contratan externamente partes del servicio de tecnología de la información y comunicaciones que suministran a la organización;** **c) para los productos de tecnología de información y comunicaciones, exigir que los proveedores divulguen prácticas de seguridad adecuadas a lo largo de la cadena de suministro, si estos productos incluyen componentes comprados a otros proveedores;** **d) implementar un proceso de seguimiento y métodos aceptables para validar que los productos y servicios de tecnología de información y comunicación cumplan los requisitos de seguridad establecidos;** **e) implementar un proceso para identificar los componentes de los productos o servicios que son críticos para mantener la funcionalidad, y por tanto, requieren una mayor atención y escrutinio cuando se construyen por fuera de la organización, especialmente si el proveedor en el nivel superior contrata externamente aspectos de componentes de productos o servicios a otros proveedores;** **f) obtener la seguridad de que los componentes críticos y su origen se pueden rastrear a todo lo largo de la cadena de suministro;**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información F-A-CTR-36 Acta de compromiso de confidencialidad F-A-CTR-55 Informe Periódico de supervisión. P-A-GTI-04 procedimiento de gestión de cambios F-A-CTR-21 Modelo Contrato Prestación de Servicios F-A-CTR-64 Estudios Previos F-A-CTR-52 Estudio previo contrato de prestación de servicios F-A-CTR-56 Informe de presunto incumplimiento F-A-CTR-69 Requerimiento por presunto incumplimiento del contrato F-A-CTR-27 Ficha técnica
	A.15.2	**GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DE PROVEEDORES**	**Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.**									
	A.15.2.1	**Seguimiento y revisión de los servicios de los proveedores.**	**Control** **Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.**	SI	NO	Se adopta este control, puesto que se debe hacer seguimiento y revisión de los servicios de los proveedores.	X	X	X		**a) hacer seguimiento de los niveles de desempeño de servicio para verificar el cumplimiento de los acuerdos;** **b) revisar los reportes de servicio elaborados por el proveedor, y concertar reuniones de avance regulares, según se exija en los acuerdos;** **c) llevar a cabo auditorías de los proveedores, junto con la revisión de reportes de auditores independientes, si están disponibles, y seguimiento a las cuestiones identificadas;** **d) suministrar información acerca de incidentes de seguridad de la información y revisar esta información según se exija en los acuerdos y en cualquier directriz y procedimiento de soporte;** **e) revisar los rastros de auditoría (Audit Trails) del proveedor, y los registros de eventos de seguridad de la información, problemas operacionales, fallas, rastreo de fallas e interrupciones relacionadas con el servicio entregado;** **f) resolver y gestionar cualquier problema identificado;** **g) revisar los aspectos de seguridad de la información de las relaciones de los proveedores con sus propios proveedores;** **h) asegurar que el proveedor mantenga una capacidad de servicio suficiente, junto con planes ejecutables destinados a asegurar que se mantienen los niveles de continuidad del servicio acordados, después de fallas considerables en el servicio, o después de un desastre**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información F-A-CTR-36 Acta de compromiso de confidencialidad F-A-CTR-55 Informe Periódico de supervisión. P-A-GTI-09 - Procedimiento Gestión de Incidentes de la Información F-A-GTI-10 Formato Reporte de Incidentes DS-E-GET-03 Contacto con las Autoridades y Grupos de Interés Especial P-A-GTI-04 Procedimiento de gestión de cambios F-E-GET-16 Solicitud de Cambios de Proyectos de TI
	A.15.2.2	**Gestión de cambios en los servicios de los proveedores.**	**Control** **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 revaloración de los riesgos.**	SI	NO	Se adopta este control, puesto que todos los cambios en el suministro de servicios por parte de los proveedores se deben gestionar de manera eficiente y segura.	X	X	X		**Se deberían considerar los siguientes aspectos:** **a) los cambios en los acuerdos con los proveedores;** **b) los cambios hechos por la organización para implementar:** **1) las mejoras a los servicios ofrecidos en la actualidad;** **2) el desarrollo de nuevas aplicaciones y sistemas;** **3) las modificaciones o actualizaciones a las políticas y procedimientos de la organización;** **4) los controles nuevos o modificados para resolver incidentes de seguridad de la información y mejorar la seguridad;** **c) los cambios en los servicios de los proveedores para implementar:** **1) cambios y mejoras en las redes;** **2) el uso de nuevas tecnologías;** **3) la adopción de nuevos productos o versiones/ediciones más recientes;** **4) nuevas herramientas y ambientes de desarrollo;** **5) cambios en las ubicaciones físicas de las instalaciones de servicio;** **6) cambio de proveedores;** **7) contratación externa de otros proveedores.**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información F-A-CTR-36 Acta de compromiso de confidencialidad F-A-CTR-55 Informe Periódico de supervisión. P-A-GTI-09 Procedimiento Gestión de Incidentes de la Información F-A-GTI-10 Formato Reporte de Incidentes DS-E-GET-03 Contacto con las Autoridades y Grupos de Interés Especial P-A-GTI-04 Procedimiento de gestión de cambios F-E-GET-16 Solicitud de Cambios de Proyectos de TI
	A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**										
	A.16.1	**GESTIÓN DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN**	**Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.**									
	A.16.1.1	**Responsabilidades y procedimientos.**	**Control** **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	NO	Se adopta este control, puesto que deben existir en la Entidad responsabilidades y procedimientos de gestión de incidentes de seguridad de la información.			X		**a) establecer las responsabilidades de gestión, para asegurar que los siguientes procedimientos se desarrollan y comunican adecuadamente dentro de la organización:** **1) los procedimientos para la planificación y preparación de respuesta a incidentes;** **2) los procedimientos para seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información;** **3) los procedimientos para logging las actividades de gestión de incidentes;** **4) los procedimientos para el manejo de evidencia forense;** **5) los procedimientos para la valoración y toma de decisiones sobre eventos de seguridad de la información y la valoración de debilidades de seguridad de la información;** **6) los procedimientos para respuesta, incluyendo aquellos para llevar el asunto a una instancia superior, recuperación controlada de un incidente y comunicación a personas u organizaciones internas y externas;** **b) establecer los procedimientos para asegurar que:** **1) el personal competente maneje las cuestiones relacionadas con incidentes de seguridad de la información dentro de la organización;** **2) se implemente un punto de contacto para la detección y reporte de incidentes de seguridad;** **3) se mantengan contactos apropiados con las autoridades, grupos de interés o foros externos que manejen las cuestiones relacionadas con incidentes de seguridad de la información;** **c) definir el reporte de procedimientos debería incluir:** **1) la preparación de formatos de reporte de eventos de seguridad de la información para apoyar la acción de reporte y ayudar a la persona que reporta a recordar todas las acciones necesarias en caso de un evento de seguridad de la información;** **2) el procedimiento que se va a seguir en el caso de un evento de seguridad de la información, (tomar nota inmediatamente de todos los detalles, tales como el tipo de no conformidad o violación, mal funcionamiento, mensajes en la pantalla y reporte inmediato al punto de contacto y realizar solamente acciones coordinadas);** **3) referencia a un proceso disciplinario formal establecido para ocuparse de los empleados que cometen violaciones a la seguridad;** **4) los procesos de retroalimentación adecuados para asegurar que las personas que reportan eventos de seguridad de la información sean notificadas de los resultados después de que la cuestión haya sido tratada y cerrada.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-09 - Procedimiento de gestión de incidentes F-A-GTI-10 Formato Reporte de Incidentes DS-E-GET-03 Contacto con las Autoridades y Grupos de Interés Especial G-A-GTI-06 Guía para la recolección de evidencia digital
	A.16.1.2	**Reporte de eventos de seguridad de la información.**	**Control** **Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible**	SI	NO	Se adopta este control, puesto que todos los funcionarios y contratistas deben tomar conciencia de su responsabilidad de reportar eventos de seguridad de la información tan pronto como sea posible.			X	X	**a) establecer un control de seguridad ineficaz;** **b) definir la violación de la integridad, confidencialidad o expectativas de disponibilidad de la información;** **c) definir los errores humanos;** **d) definir las no conformidades con políticas o directrices;** **e) definir las violaciones de acuerdos de seguridad física;** **f) establecer los cambios no controlados en el sistema;** **g) definir mal funcionamiento en el software o hardware;** **h) definir violaciones de acceso.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-09 - Procedimiento de gestión de incidentes F-A-GTI-10 Formato Reporte de Incidentes DS-E-GET-03 Contacto con las Autoridades y Grupos de Interés Especial G-A-GTI-06 Guía para la recolección de evidencia digital
	A.16.1.3	**Reporte de debilidades de seguridad de la información.**	**Control** **Se debería 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	NO	Se adopta este control, puesto que todos los funcionarios y contratistas deben reportar las debilidades de seguridad de la información que conozcan, para evitar la materialización de incidentes.			X	X	**Validar si los eventos son reportados de forma consistente en toda la entidad de acuerdo a los criterios establecidos.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-09 Procedimiento de gestión de incidentes F-A-GTI-10 Formato Reporte de Incidentes DS-E-GET-03 Contacto con las Autoridades y Grupos de Interés Especial G-A-GTI-06 Guía para la recolección de evidencia digital
	A.16.1.4	**Evaluación de eventos de seguridad de la información y decisiones sobre ellos.**	**Control** **Los eventos de seguridad de la información se deben evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.**	SI	NO	Se adopta este control, puesto que es necesario evaluar los eventos de seguridad de la información y decidir si es necesario clasificarlos como incidente de seguridad de la información.			X	X	**Validar si los eventos de SI detectados son analizados para determinar si constituyen un incidentes de seguridad de la información y entender los objetivos del ataque y sus métodos.** **Evidencia si los incidentes son categorizados y se cuenta con planes de respuesta para cada categoría.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-09 Procedimiento de gestión de incidentes F-A-GTI-10 Formato Reporte de Incidentes DS-E-GET-03 Contacto con las Autoridades y Grupos de Interés Especial G-A-GTI-06 Guía para la recolección de evidencia digital

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	A.16.1.5	**Respuesta a incidentes de seguridad de la información.**	**Control** **Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados**	SI	NO	Se adopta este control, puesto que es necesario gestionar los incidentes de seguridad de la información conforme al procedimiento.			X	X	**a) Los incidentes son contenidos y la probabilidad de que vuelvan a ocurrir mitigada.** **b) Se debe contar con un plan de recuperación de incidentes durante o después del mismo.** **b) recolectar evidencia lo más pronto posible después de que ocurra el incidente;** **c) llevar a cabo análisis forense de seguridad de la información, según se requiera** **d) llevar el asunto a una instancia superior, según se requiera;** **e) asegurar que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior;** **f) comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo;** **g) tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente;** **g) establecer que una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto.** **h) de acuerdo a la NIST se deben investigar las notificaciones de los sistemas de detección.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-09 Procedimiento de gestión de incidentes F-A-GTI-10 Formato Reporte de Incidentes DS-E-GET-03 Contacto con las Autoridades y Grupos de Interés Especial G-A-GTI-06 Guía para la recolección de evidencia digital
	A.16.1.6	**Aprendizaje obtenido de los incidentes de seguridad de la información.**	**Control** **El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.**	SI	NO	Se adopta este control, puesto que se debe contar con mecanismos que permitan cuantificar y hacer el seguimiento de los incidentes de seguridad de la información.			X	X	**De acuerdo a la NIST se debe entender cual fue el impacto del incidente. Las lecciones aprendidas deben ser usadas para actualizar los planes de respuesta a los incidentes de SI.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-09 Procedimiento de gestión de incidentes F-A-GTI-10 Formato Reporte de Incidentes DS-E-GET-03 Contacto con las Autoridades y Grupos de Interés Especial G-A-GTI-06 Guía para la recolección de evidencia digital
	A.16.1.7	**Recolección de evidencia.**	**Control** **La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia**	SI	NO	Se adopta este control, puesto que se debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.			X	X	**a) definir la cadena de custodia;** **b) establecer la seguridad de la evidencia;** **c) definir la seguridad del personal;** **d) definir los roles y responsabilidades del personal involucrado;** **e) establecer la competencia del personal;** **f) realizar la documentación;** **g) definir las sesiones informativas.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. P-A-GTI-09 Procedimiento de gestión de incidentes F-A-GTI-10 Formato Reporte de Incidentes DS-E-GET-03 Contacto con las Autoridades y Grupos de Interés Especial G-A-GTI-06 Guía para la recolección de evidencia digital
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	**A.17**	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**										
	A.17.1	**CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN**	**Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.**									
	A.17.1.1	**Planificación de la continuidad de la seguridad de la información.**	**Control** **La organización debería 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	NO	Se adopta este control, puesto que se debe determinar los requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad en situaciones adversas.			X	X	**Indagar si la Entidad cuenta con un BCP (Bussines Continuity Plan) o DRP (Disaster Recovery Plan).** **Determine si aplica para procesos críticos solamente o se han incluido otros procesos o por lo menos se ha reconocido la necesidad de ampliarlo a otros procesos (para determinar el nivel de madurez)** **Evalúe si se ha incluido en estos planes y procedimientos los requisitos de seguridad de la información.** **Tenga en cuenta que en ausencia de una planificación formal de continuidad de negocio y recuperación de desastres, la dirección de seguridad de la información debería suponer que los requisitos de seguridad de la información siguen siendo los mismos en situaciones adversas, en comparación con las condiciones operacionales normales. Como alternativa, una organización puede llevar a cabo un análisis de impacto en el negocio de los aspectos de seguridad de la información, para determinar los requisitos de seguridad de la información aplicables a situaciones adversas.** **De acuerdo a la NIST también se deben tener planes de respuesta a incidentes y recuperación de incidentes.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. DS-E-GET-24 Política de Continuidad de Negocio
	A.17.1.2	**Implementación de la continuidad de la seguridad de la información.**	**Control** **La organización debería 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	NO	Se adopta este control, puesto que es necesario asegurar el nivel de continuidad requerido en la Entidad, para la seguridad de la información ante situaciones adversas.			X	X	**Verifique si la entidad cuenta con** **a) Una estructura organizacional adecuada para prepararse, mitigar y responder a un evento contingente, usando personal con la autoridad, experiencia y competencia necesarias.** **b) Personal formalmente asignado de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información.** **c) Planes aprobados, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como la organización gestionará un evento contingente y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información aprobados por la dirección.** **Revise si los controles de seguridad de la información que se han implementado continúan operando durante un evento contingente. Si los controles de seguridad no están en capacidad de seguir brindando seguridad a la información, se la Entidad debe establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información.
	A.17.1.3	**Verificación, revisión y evaluación de la continuidad de la seguridad de la información.**	**Control** **La organización debería 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	NO	Se adopta este control, puesto que es necesario realizar la verificación, revisión y evaluación de la continuidad de la seguridad de la información debido a posibles cambios organizacionales, técnicos, procedimentales y de proceso.			X	X	**Indague y solicite evidencias de la realización de pruebas de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que son coherentes con los objetivos de continuidad de la seguridad de la información;** **Tenga en cuenta que la verificación de los controles de continuidad de la seguridad de la información es diferente de las pruebas y verificación generales de seguridad de la información. Si es posible, es preferible integrar la verificación de los controles de continuidad de negocio de seguridad de la información con las pruebas de recuperación de desastres y de continuidad de negocio de la organización.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. DS-E-GET-24 Política de Continuidad de Negocio
	A.17.2	**REDUNDANCIAS**	**Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.**									
	A.17.2.1	**Disponibilidad de instalaciones de procesamiento de información.**	**Control** **Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.**	SI	NO	Se adopta este control, puesto que las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad			X	X	**Verifique si la Entidad cuenta con arquitecturas redundantes, ya sea un centro de cómputo principal y otro alterno o componentes redundantes en el único centro de cómputo.** **Indague como se han definido las necesidades de los procesos para seleccionar que elementos deben ser redundantes.** **Solicite si aplica las pruebas aplicadas para asegurar que un componente redundante funciona de la forma prevista durante una emergencia o falla.**	M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. DS-E-GET-24 Política de Continuidad de Negocio M-A-GTI-02 MANUAL GENERAL DE OPERACIONES DE INFRAESTRUCTURA DE TI - 6.1 ANEXO 2 Manual de operaciones de firewall de perímetro M-A-GTI-02 MANUAL GENERAL DE OPERACIONES DE INFRAESTRUCTURA DE TI La entidad cuenta con diferentes componentes redundantes implementados en la arquitectura de la infraestructura tecnológica. Actualmente cuenta con 2 Firewall, 2 WAF, 2 Switch CORE, 2 nodos hyperconvergentes, soluciones de backups en HA, 3 nodos de Nutanix, HA LAN (Redundancia en capa de acceso). En cuanto a los enlaces físicos se tienen implementadas soluciones de fibras renundantes LACP para la interconexión de los equipos.
	A.18	**CUMPLIMIENTO**										
	A.18.1	**CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES**	**Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.**									
	A.18.1.1	**Identificación de la legislación aplicable y de los requisitos contractuales.**	**Control** **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	NO	Se adopta este control, puesto que es necesario identificar toda la legislación aplicable a la Entidad para cumplir con los requisitos de seguridad de la información.	X	X	X		**Solicite la relación de requisitos legales, reglamentarios, estatutarios, que le aplican a la Entidad (Normograma).** **Indague si existe un responsable de identificarlos y se definen los responsables para su cumplimiento.**	F-E-SIG-08 Actualización de normograma P-E-SIG-06 Ingreso actualización del normograma M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. La entidad cuenta con el normograma documentado y actualizado, cada proceso es responsable respecto a su actualización.
	A.18.1.2	**Derechos de propiedad intelectual.**	**Control** **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	NO	Se adopta este control, puesto que se debe asegurar el cumplimiento de los requisitos legales relacionados con los derechos de propiedad intelectual.	X	X	X		**1) Solicite los procedimientos para el cumplimiento de los requisitos y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.** **2) Verifique si la Entidad cuenta con una política publicada sobre el cumplimiento de derechos de propiedad intelectual que defina el uso legal del software y de productos informáticos. Esta política debe estar orientada no solo al software, si no también a documentos gráficos, libros, etc.** **3) Indague como se controla que no se instale software ilegal.** **4) Indague si se tiene un inventario de software instalado y se compara con el número de licencias adquiridas para asegurar que no se incumplen los derechos de propiedad intelectual. Tenga en cuenta los controles que deben existir para asegurar que no se exceda ningún número máximo de usuarios permitido dentro de la licencia.**	F-E-SIG-08 Actualización de normograma P-E-SIG-06 Ingreso actualización del normograma M-E-GET-04 Manual de Políticas Específicas de Seguridad de la Información. 1) Dentro del documento M-E-GET-04 Manual de políticas especificas de seguridad y privacidad de la información se encuentran definidos los requisitos relacionados con los derechos de propiedad intelectual. 2) Dentro del documento M-E-GET-04 Manual de políticas especificas de seguridad y privacidad de la información, se encuentran definidos los lineamientos relacionados con los derechos de propiedad intelectual. 3) La instalación de software ilegal se controla con la aplicación de las políticas en el directorio activo. 4) Con al herramienta de gestión de servicios GEMA y el soporte del equipo de mesa de ayuda se registra la información del Software instalado vs las licencias adquiridas por la entidad.
	A.18.1.3	**Protección de registros.**	**Control** **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	NO	Se adopta este control, puesto que se deben proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.			X		**Revise si la Entidad cuenta con tablas de retención documental que especifiquen los registros y el periodo por el cual se deberían retener, además del almacenamiento, manejo y destrucción. Posibles tipos de registros pueden ser registros contables, registros de bases de datos, logs de transacciones, logs de auditoría y procedimientos operacionales, los medios de almacenamiento permitidos pueden ser papel, microfichas, medios magnéticos, medios ópticos etc.**	La entidad cuenta con las tablas de retención documental publicadas en el link: https://www.minambiente.gov.co/categoria-gd/tablas-de-retencion-documental/ F-A-DOC-55 Matriz de valoración documental para TRD y TVD F-A-GR-DC-02 Marcación de cajas, F-A-GR-DC-06 Consulta de documentos, F-A-GR-DC-07 Inventario Documental F-A-GR- DC-08 Ficha préstamo de documentos.
	A.18.1.4	**Privacidad y protección de información de datos personales.**	**Control** **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	NO	Se adopta este control, puesto que deben existir lineamientos para el manejo de los datos personales en la Entidad.	X		X		**Indague sobre las disposiciones que ha definido la Entidad para cumplir con la legislación de privacidad de los datos personales, ley estatutaria 1581 de 2012 y decreto 1377 que reglamenta la ley de 2013.** **1) Revise si existe una política para cumplir con la ley** **2) Si están definidos los responsables** **3) Si se tienen identificados los repositorios de datos personales** **4) Si se ha solicitado consentimiento al titular para tratar los datos personales y se guarda registro de este hecho.** **5) Si se adoptan las medidas técnicas necesarias para proteger las bases de datos donde reposan estos datos.**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información. DS-E-GET-01 Política de tratamiento y protección de datos personales https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/ F-E-GET-10 Bases de datos personales
	A.18.1.5	**Reglamentación de controles criptográficos.**	**Control** **Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.**	SI	NO	Se adopta este control, puesto que deben existir lineamientos para el uso de controles criptográficos en la Entidad.			X		**Se deberían considerar los siguientes aspectos para el cumplimiento con los acuerdos, leyes y reglamentaciones:** **a) las restricciones sobre importación o exportación de hardware y software, para la realización de funciones criptográficas;** **b) las restricciones sobre importación o exportación de hardware y software que está diseñado para la adición de funciones criptográficas;** **c) las restricciones sobre el uso de criptografía;** **d) los métodos obligatorios o discrecionales de acceso por parte de las autoridades de los países a información cifrada mediante software o hardware para brindar confidencialidad al contenido.**	N/A

	A.18.2	**REVISIONES DE SEGURIDAD DE LA INFORMACIÓN**	Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales									
	A.18.2.1	**Revisión independiente de la seguridad de la información**	**Control** **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	NO	Se adopta este control, puesto que el sistema de seguridad de la información se debe revisar de forma independiente para asegurar la conveniencia, la adecuación y la eficacia del sistema.	X		X		**Investigue la forma como se realizan revisiones independientes (por personas diferentes o no vinculadas a un proceso o área que se revisa), de la conveniencia, la adecuación y la eficacia continuas de la gestionar la seguridad de la información.** **Para esto solicite:** **1) El plan de auditorias del año** **2) El resultado de las auditorias del año** **3) Las oportunidades de mejora o cambios en la seguridad de la información identificados.**	P-C-EIN-01 Evaluación independiente, P-E-SIG-07 Auditora Interna del Sistema Integrado de Gestión M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información. F-E-SIG-10 Plan de mejoramiento
	A.18.2.2	**Cumplimiento con las políticas y normas de seguridad.**	**Control** **Los gerentes 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	NO	Se adopta este control, puesto que se debe identificar cómo se cumplen los requisitos de seguridad de la información definidos en las políticas de la Entidad.	X		X		**1) Verifique si los gerentes aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento de las políticas y estándares de seguridad.** **2) Verifique la revisión periódica del cumplimiento del centro de cómputo con las políticas y normas de seguridad establecidas.** **3) Verifique si los sistemas de información son revisados regularmente para asegurar el cumplimiento de las normas de seguridad de la información**	M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información. F-A-GTI-09 Lista de chequeo estado de centros de cableado
	A.18.2.3	**Revisión del cumplimiento.**	**Control** **Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.**	SI	NO	Se adopta este control, puesto que el cumplimiento técnico se debe revisar, generando informes técnicos, determinando el cumplimiento de las políticas de seguridad de la información de la Entidad.	X		X		**Verifique si se realizan evaluaciones de seguridad técnicas por o bajo la supervisión de personal autorizado, apoyado en herramientas automáticas o con revisiones manuales realizadas por especialistas.** **Solicite evidencia de las últimas pruebas realizadas, sus resultados y seguimiento para asegurar que las brechas de seguridad fueron solucionadas.**	P-A-GTI-10 Análisis Periódico de Vulnerabilidades M-E-GET-04 Manual de políticas específicas de seguridad y privacidad de la información. Informe de análisis de vulnerabilidades realizado en 2023 De igual forma se genera el plan de remediación con el respectivo seguimiento en las siguiente vigencia.