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

CONTROLES ISO 27001			CONTROLES ACTUALES	Justificación de exclusión	Justificación de inclusión	Selección Controles y Razón de la selección				Comentario / Descripción General del Control
						RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**								
Políticas de Seguridad de la Información	**A.5.1**	**Política de Seguridad de la Información.**								
		Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.								
	A.5.1.1	Políticas de Seguridad de la Información.	Se cuenta con Política documentada del SGSI en el documento "M-E-GIC-01 Manual de Seguridad de la Información". Se cuenta con política especificas en el documento "Manual de Seguridad de la Información" Numeral 7.		Se implementan políticas de seguridad de la información para dar cumplimiento a los requisitos de ISO 27001:2013, al modelo de Seguridad y Privacidad de la información de Gobierno en Línea y sus decretos relacionados, al cumplimiento de lo dispuesto en la ley 1581 y sus decretos relacionados. De igual manera se implementa como mejor práctica para mantener directrices de TI, de Seguridad de la información y tener herramientas que justifiquen y comuniquen a l interior del Ministerio buenas prácticas para la disminución de riesgos. Se revisan periódicamente.	X		X		
	A.5.1.2	Revisión de las Política de Seguridad de la Información.				X		X		
	A.6.1	**Organización Interna** **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.	Manual de Funciones del Ministerio de Ambiente y Desarrollo Sostenible (MADS). Manual de Seguridad de la Información en el Numeral 6. Grupo Operativo de Seguridad de la Información. Justificación de necesidades de contratistas.		Se han definido roles y responsabilidades a través de las diferentes herramientas y cumplimiento normativo del Ministerio. Ante el crecimiento de las necesidades de Seguridad de la Información del Ministerio y de las directrices de Min Tic.	X	X	X		
	A.6.1.2	Separación de deberes.	En cada proceso se han definido mediante el Manual de Funciones del MADS y en el Numeral 6. Grupo Operativo de Seguridad de la Información del documento M-E-GIC-01 Manual de Seguridad de la Información. También, se han asignado propietarios a los activos de información en la matriz de riesgos.		La separación de deberes y gestión de roles y permisos se realiza de acuerdo a las funciones especificas documentadas. Se tiene criterios de auditoria de seguridad, requerimientos legales, buenas prácticas y arquitectura empresarial.	X	X	X		
	A.6.1.3	Contacto con las Autoridades.	P-E-GIC-05 Procedimiento Gestión de Incidentes de Seguridad de la Información. G-A-ATH-03 Guía de emergencias y contingencia, identificación, calificación y análisis de amenazas, vulnerabilidad y riesgo.		Por la naturaleza pública de la organización se mantiene comunicación constante con autoridades. Se tienen contactos específicos y de igual manera se tienen documentados para posibles contactos ante posibles incidentes. Se mantiene el contacto tanto para acciones preventivas como correctivas	X		X		
	A.6.1.4	Contacto con Grupos de Interés Especiales.	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.			X		

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

CONTROLES ISO 27001			CONTROLES ACTUALES	Justificación de exclusión	Justificación de inclusión	Selección Controles y Razón de la selección				Comentario / Descripción General del Control
						RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**								
	A.6.1.5	Seguridad de la Información en la gestión de proyectos.	El Ministerio incluye en los contratos clausulas de confidencialidad y cumplimiento en lo exigido por la norma ISO27001. Se cuenta con un proceso de gestión de proyectos ante nuevos requerimientos como ante un cambio de alta magnitud. Se cuenta con un modelo de arquitectura empresarial y un Plan Estratégico de TI.		Se tienen criterios de seguridad en la gestión de proyectos con el fin de garantizar la continuidad y mejora continua de la Seguridad de la Información de acuerdo con los controles implementados.			X		
	A.6.2	**Dispositivos móviles y teletrabajo.**								
		Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.								
	A.6.2.1	Política para dispositivos móviles.	El Ministerio cuenta con una política específica documentada en el Numeral 8 del documento "M-E-GIC-01 Manual de Seguridad de la Información". La entidad tiene implementado control para comunicaciones de dispositivos móviles mediante la plataforma Aruba. Se cuenta con control de red únicamente para dispositivos móviles y aplicativo Aranda para dispositivos relevantes del Ministerio.		El Ministerio implementa controles y herramienta con el fin de mantener gobierno sobre la información y disminuir la probabilidad de materialización de Riesgos.			X	X	
	A.6.2.2	Teletrabajo.	Únicamente soporte de servidores tiene acceso remoto). Se encuentra en el Numeral "8.4 Control de Acceso" del documento "M-E-GIC-01 Manual de Seguridad de la Información". De igual manera para tele trabajadores se han definido controles tecnológicos y se han realizado pruebas piloto.		Se implementa control como requerimiento legal de acuerdo al libro blanco de teletrabajo de mintic, al acuerdo Minambiente - Mintic por el teletrabajo y como mejor práctica para realizar una gestión eficaz de la información.	X		X		
Seguridad de los Recursos Humanos	**A.7,1**	**Responsabilidad por los Activos.**								
		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.	Se encuentra en: "C-A-ATH-01 caracterización de proceso de administración de Talento Humano" y "Procedimiento Vinculación y Desvinculación de Personal P-A-ATH-08". Procesos definidos en el Manual de Contratación del Ministerio de Ambiente y desarrollo Sostenible		La aplicación de estos controles es un requerimiento legal y se justifica y aplica en los términos y condiciones de ley.	X				
	A.7.1.2	Términos y condiciones de empleo.	Resolución 0677 de 2012 y Resolución 0766 de 2012 Manual de Funciones. Documento M-E-GIC-01 Manual de Seguridad de la Información. Los contemplados en la Ley 734 de 2002 y demás normatividad vigente relacionada para servidores público. Estudios previos de contratistas, minutas de contratos, justificación de necesidades.			X				
	A.7.2	**Durante la ejecución del empleo.**								
		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.	Acta de aprobación política de SIG e incorporación del SGSI al SIG del 03 de dic de 2013 . Numeral 6. Grupo Operativo de Seguridad de la Información descrito en el documento M-E-GIC-01 Manual de Seguridad de la Información. Resolución Sistema Integrado de Gestión.		Mediante comité de desarrollo administrativo institucional, los comités de gerencia, el jefe asesor de tics, la oficina asesora de planeación a través del Sistema integrado de gestión, procedimientos de revisión por la dirección y cumplimiento de directrices de gobierno en línea son algunos de los requisitos por los cuales se incluye y gestión el presente control.	X		X		

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

CONTROLES ISO 27001			CONTROLES ACTUALES	Justificación de exclusión	Justificación de inclusión	Selección Controles y Razón de la selección				Comentario / Descripción General del Control
						RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**								
	A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	La entidad realiza capacitaciones a funcionarios en temáticas relacionadas a seguridad de la información. De igual manera se programa como mínimo una sensibilización al año. Se tienen mecanismos de sensibilización permanente tales como el uso de vídeos en las pantallas institucionales, wallpapers, popups entre otros.		Se realizan sensibilizaciones a los funcionarios teniendo en cuenta rotación de personal y recordación constante con el fin de disminuir la probabilidad de riesgos e incluir y cumplir con mejores prácticas			X	X	
	A.7.2.3	Proceso disciplinario.	Ver procedimientos: P-A-GR-DI-01 Indagación Preliminar, P-A-GR-DI-02 Investigación Disciplinaria, P-A-GR-DI-03 Juzgamiento (Pliego de Cargos), P-A-GR-DI-04 Segunda Instancia, P-A-GR-DI-05 Disciplinario Verbal. Ley 734 de 2002.		Se aplica de acuerdo a requisitos de ley en cumplimiento con la normativa nacional.	X	X			
	A.7.3	**Terminación y cambio de empleo.**								
		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.	"F-A-ATH-06 Control de Retiro del Servicio". Procedimientos de Talento Humano y requisitos de diferentes áreas en cuanto a responsabilidades.		Se aplica de acuerdo a requisitos de ley en cumplimiento con la normativa nacional.	X	X			
Gestión de activos	**8.1**	**Responsabilidad por los activos.**								
		Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.								
	A.8.1.1	Inventario de activos.	G-A-GTI-03 guía metodológica para la identificación y clasificación de activos y F-A-GTI-04 formato de identificación y clasificación de activos del SGSI.		Se implementa como cumplimiento de los estándares de ISO 27001:2013 y se realiza un trabajo conjunto para dar cumplimiento a requerimientos y alineación con gestión documental y criterios de retención, activos de arquitectura empresarial y flujos de información, Ley de transparencia y publicación de información.	X		X		
	A.8.1.2	Propiedad de los activos.				X		X		
	A.8.1.3	Uso aceptable de los activos.	Numeral 7 del documento "M-E-GIC-01 Manual de Seguridad de la Información"		Se implementan de acuerdo a normativa legal vigente y buenas prácticas de seguridad de la información.	X	X	X		
	A.8.1.4	Devolución de Activos.	"F-A-ATH-06 Control de Retiro del Servicio". Procedimientos de Talento Humano y requisitos de diferentes áreas en cuanto a responsabilidades.			X	X	X		
	8.2	**Clasificación de la información.**								
		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.	G-A-GTI-03 guía metodológica para la identificación y clasificación de activos y F-A-GTI-04 formato de identificación y clasificación de activos del SGSI. P-E-GIC-06 Procedimiento Clasificación y Etiquetado de Información		Se implementa como cumplimiento de los estándares de ISO 27001:2013 y se realiza un trabajo conjunto para dar cumplimiento a requerimientos y alineación con gestión documental y criterios de retención, activos de arquitectura empresarial y flujos de información, Ley de transparencia y publicación de información.	X		X		
	A.8.2.2	Etiquetado de la información.				X		X		
	A.8.2.3	Manejo de activos.	"M-E-GIC-01 Manual de Seguridad de la Información"					X		
	8.3	**Manejo de medios.**								
		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.	Política de gestión de medios removibles, del documento "M-E-GIC-01 Manual de Seguridad de la Información" y se controla a través de la consola de antivirus Kaspersky.		Se implementa como buena práctica, salvaguardando la necesidad institucional, la naturaleza pública, el principio de buena fe y la autorización de uso de dicho tipo de medios			X		
	A.8.3.2	Disposición de los medios.	El grupo de sistemas 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.		Se implementa como buena práctica para garantizar una adecuada disposición de medios.			X		

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

CONTROLES ISO 27001			CONTROLES ACTUALES	Justificación de exclusión	Justificación de inclusión	Selección Controles y Razón de la selección				Comentario / Descripción General del Control
						RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**								
	A.8.3.3	Transferencia de medios físicos.	El Ministerio cuenta con contrato de transporte y servicios de mensajería con la empresa 4 72.		Se implementa como buena práctica para garantizar una adecuada disposición de medios y como requisito normativo por la naturaleza pública de la entidad y la necesidad de comunicar y tener un flujo constante de información hacía la ciudadanía.	X		X		
Control de acceso	**A.9.1**	**Control de acceso.**								
		Limitar el acceso a información y a instalaciones de procesamiento de información.								
	A.9.1.1	Política de control de acceso.	Documento "M-E-GIC-01 Manual de Seguridad de la Información" se realiza la gestión de control de acceso mediante el Directorio Activo.		Se gestiona el uso y autorización de acceso a los sistemas de información del ministerio, carpetas compartidas y redes mediante procesos de autorización explícitos y desactivación automática con el fin de salvaguardar la información del Ministerio.		X	X		
	A.9.1.2	Acceso a redes y servicios de red.	Administrado por Infraestructura, memoria del MAC en switches. Internet inalámbrico, cambio de contraseña con frecuencia programada.					X		
	A.9.2	**Gestión de acceso de usuarios.**								
		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.	Mediante la información que suministra el proceso de talento humano sobre el perfil del funcionario o contratista realiza el registro y creación de los usuarios para los sistemas de información mediante la Herramienta de Mesa de Ayuda ARANDA . La cancelación se realiza mediante formato "Control de Retiro del Servicio" Código: F-A-ATH-06 y mediante programación automática		Cómo mejor práctica y política institucional se regula el acceso y retiro a los sistemas de información. Se deja registro en el aplicativo Aranda de la necesidad y de igual forma mediante directorio activo se programa la desactivación para contratistas y mediante formatos se controla la de servidores públicos provisionales y de carrera con el fin de gobierno y control sobre la información del Ministerio.			X		
	9.2.2	Suministro de acceso de usuarios.	Mediante la Herramienta de Mesa de Ayuda ARANDA o correo electrónico la coordinación del grupo de sistemas en casos específicos.					X		
	9.2.3	Gestión de derechos de acceso privilegiado.	La asignación de privilegios está ligada al perfil de cargo del servidor público. Para el acceso a los activos de TI (infraestructura) del Ministerio se tiene acuerdo de confidencialidad con el contratista para los roles DBA, Redes y Servidores. El acceso a las aplicaciones se controla mediante solicitud y autorización escrita de los jefes de cada dependencia y el nivel de acceso. En el caso de los contratistas las cuentas del Directorio Activo se configuran desde su creación para su bloqueo con la fecha de finalización del contrato.		Se aplica control como mejor práctica para gestionar requisitos contractuales, niveles de acceso y privilegios para mantener y controlar los sistemas de información del Ministerio.			X	X		
	9.2.4	Gestión de información de autenticación secreta de usuarios.	Se cuenta con políticas definidas en "M-E-GIC-01 Manual de Seguridad de la Información" y con Directorio Activo y controles a nivel de base de datos		Se aplica control como mejor práctica para tener control y una trazabilidad total del uso, revisión y eliminación de los derechos de acceso asignados.			X		
	9.2.5	Revisión de los derechos de acceso de usuarios.						X		
	9.2.6	Retiro o ajuste de los derechos de acceso.	En caso de retiro la cancelación se realza mediante formato "Control de Retiro del Servicio" Código: F-A-ATH-06. En caso de ajuste de derechos de acceso se solicita mediante correo o memorando.					X		
	A.9.3	**Responsabilidad de los usuarios.**								
		Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.								
	A.9.3.1	Uso de información de autenticación secreta.	Políticas de uso en "M-E-GIC-01 Manual de Seguridad de la Información". Políticas aplicadas en Directorio Activo.		Se aplican y divulgan políticas con el fin de mantener el no repudio en los sistemas de información del Ministerio.			X		

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

CONTROLES ISO 27001			CONTROLES ACTUALES	Justificación de exclusión	Justificación de inclusión	Selección Controles y Razón de la selección				Comentario / Descripción General del Control
						RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**								
	A.9.4	**Control de acceso a sistemas y aplicaciones.**								
		Evitar el acceso no autorizado a sistemas y aplicaciones.								
	A.9.4.1	Restricción de acceso a la información.	Políticas y Directrices en el capitulo 7 de "M-E-GIC-01 Manual de Seguridad de la Información" se realiza la gestión de control de acceso mediante el Directorio Activo. El acceso a las aplicaciones se controla mediante solicitud y autorización escrita de los jefes de cada dependencia y el nivel de acceso.		Los privilegios de acceso a la información se encuentran limitados a usuarios que requieren se uso, el acceso es limitado y gestionado como mejor práctica para evitar la materialización de riesgos asociados.			X		
	A.9.4.2	Procedimiento de ingreso seguro.	Se encuentran políticas y directrices en el documento "M-E-GIC-01 Manual de Seguridad de la Información"					X		
	A.9.4.3	Sistemas de gestión de contraseñas.						X		
	A.9.4.4	Uso de programas utilitarios privilegiados.						X		
	A.9.4.5	Control de acceso a códigos fuente de programas.	Existen políticas y controles técnicos aplicados en el Manual "M-E-GIC-01 Manual de Seguridad de la Información"					X		
Criptografía	**A.10.1**	**Controles Criptográficos.**								
		Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.								
	A.10.1.1	Políticas sobre el uso de controles criptográficos.	Se incluyen políticas en el numeral 7 del "M-E-GIC-01 Manual de Seguridad de la Información". 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.		Se implementan como mejor práctica y requerimiento legal con el fin de garantizar confidencialidad y/o autenticidad de la información.	X		X		
	A.10.1.2	Gestión de llaves.	El Ministerio pone en práctica las Políticas de Operación del sistema financiero SIIF exigidas por el Ministerio de Hacienda y protege en cajas fuertes dispositivos como Toquen. Se cuenta con firmas digitales para el sistema de gestión documental Sigma.			X		X		
	A.11.1	**Áreas seguras.**								
		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.	Las áreas físicas que contienen información y medios de procesamiento de información poseen perímetros de seguridad física compuestos principalmente por puertas de ingreso controlado y recepcionistas que administran el ingreso de las personas a los diferentes pisos del edificio. Protocolo de Ingreso y acceso físico.		Con el fin de mantener y controlar la seguridad física en las instalaciones se definen áreas seguras , se controla mediante CCTV, se tienen políticas y protocolos definidos, y personal de seguridad. Se aplica control como mejor práctica y como requerimiento legal.			X		
	A.11.1.2	Controles de accesos físicos.	Para el acceso a áreas que comprometen la seguridad de la información se cuenta con personal de seguridad que realiza el control del acceso. Además se cuenta con puertas de seguridad que solo pueden ser abiertas por personal autorizado, monitoreo de cámaras y alarmas. Ver Numeral 8.4 del documento "M-E-GIC-01 Manual de Seguridad de la Información" "Protocolo de ingreso y control de acceso físico"			X		X		

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

CONTROLES ISO 27001			CONTROLES ACTUALES	Justificación de exclusión	Justificación de inclusión	Selección Controles y Razón de la selección				Comentario / Descripción General del Control
						RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**								
Seguridad física y del entorno	A.11.1.3	Seguridad de oficinas, recintos e instalaciones.	Para la seguridad de oficinas, recintos e instalaciones se cuenta con personal de seguridad que monitorea la seguridad a través de cámaras.					X		
	A.11.1.4	Protección contra amenazas externas y ambientales.	Existen control contra amenazas de incendios en áreas restringidas, el DataCenter. Al interior del Ministerio existen diferentes controles, tales como extintores para salvaguardar la información.		Se implementan con el fin de minimizar los riesgos de pérdida de información por amenazas ambientales. Se implementan buenas prácticas para el cuidado de los activos.			X	X	
	A.11.1.5	Trabajo en áreas seguras.	Además de las medidas presentes en los Controles de Acceso Físico no se permite la presencia de equipos de fotografía, vídeo, audio u otras formas de registro salvo autorización especial al Data Center.		Con el fin de tener especial cuidado en ciertas zonas y advertir al personal de seguridad sobre la importancia de estás, se documentan y difunden con los encargados.			X		
	A.11.1.6	Áreas de despacho y carga.	Para el acceso a áreas que comprometen la seguridad de la información se cuenta con personal de seguridad que realiza el control del acceso. Además se cuenta con puertas de seguridad que solo pueden ser abiertas por personal autorizado, monitoreo de cámaras y alarmas. Ver Numeral 8.4 del documento "M-E-GIC-01 Manual de Seguridad de la Información". "Procedimiento Control Acceso Físico P-A-GAF-16". Se define la puerta central norte y rampa hacia piso -2 como área de despacho y carga.		Como buena práctica y para que las actividades de cargue y descargue no impliquen riesgo de falla en los controles de acceso físico o riesgo para los activos.			X		
	A.11.2	**Equipos.**								
		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.	Políticas en "M-E-GIC-01 Manual de Seguridad de la Información" El ministerio cuenta con buena ubicación de los equipos de cómputo. Mesa de Ayuda asume responsabilidad en la buena ubicación de equipos.		Como buena práctica para salvaguardar la información contenida en los equipos, así como los mismos equipos en sí, se cuenta con escritorios diseñados para tal fin y se designa a mesa de ayuda para ejercer dicho control.			X		
	A.11.2.2	Servicio de suministro.	Se cuenta con UPS para el edificio - corriente regulada. 1 Planta eléctrica de 380 KVA con aproximadamente 24 horas de autonomía. Canal de Internet con alta disponibilidad.		Para mantener la continuidad de los servicios de suministro y/o evitar el menor impacto ante daños o interrupciones, se cuenta con dispositivos y controles diseñados para tal fin.			X	X	Resultado de análisis de riesgos se compró nueva UPS.
	A.11.2.3	Seguridad de cableado.	Política en "M-E-GIC-01 Manual de Seguridad de la Información"		El cableado estructurado es certificado, de igual manera se tienen políticas para el mismo, esto con el fin de tener una red en optimas condiciones para prestar servicios tecnológicos.			X		
	A.11.2.4	Mantenimiento de equipos.	Procedimientos de Mantenimiento: P-A-GAF-01 y P-A-GAF-02		Se programa mantenimientos con fines preventivos y correctivos para mantener el buen estado de los equipos.			X	X	
	A.11.2.5	Retiro de activos.	Procedimiento Control Acceso Físico P-A-GAF-16		Para velar por la información del Ministerio y el respectivo cuidado de los equipos, se implementan procedimientos y formatos para el retiro de activos.			X		
	A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.	Numeral 7.6 del documento "M-E-GIC-01 Manual de Seguridad de la Información". El Ministerio cuenta con póliza de empresa aseguradora que protege bienes de la entidad.		Se establecen políticas para velar por el buen uso de los activos y el respectivo cuidado fuera de las instalaciones si se considera necesario.			X	X	
	A.11.2.7	Disposición segura o reutilización de equipos.	Se realiza en la bodega del Almacén del Ministerio mediante confirmación de equipos para baja de acuerdo al procedimiento "Guía de borrado seguro" vigente en MADS.		Se tienen acuerdos y protocolos para la disposición final con el ánimo de salvaguardar la información.	X		X		

			CONTROLES ACTUALES	Justificación de exclusión	Justificación de inclusión	Selección Controles y Razón de la selección				Comentario / Descripción General del Control
						RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**								
	A.11.2.8	Equipos de usuario desatendido.	Numeral 8.4 del documento "M-E-GIC-01 Manual de Seguridad de la Información". Políticas implementadas en Directorio Activo.		Cómo mejor práctica y con el ánimo de cambiar y mantener la cultura en seguridad de la información, así como la disminución de riesgos, se implementan los controles relacionados.			X		
	A.11.2.9	Política de escritorio limpio y pantalla despejada.						X		
	A.12.1	**Procedimiento operacionales y responsabilidades.**								
		Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.								
	A.12.1.1	Procedimiento de operación documentados.	M-E-DE-MC-01 Manual Administración de Documentos SIG. Procedimientos de TI documentados. Al igual que procedimientos de todas las áreas de MADS. Cargados y actualizados a través de MADSIGestión.		En conjunto con Sistema de Gestión de Calidad, se tienen documentados todos los procedimientos para buscar la continuidad de las operaciones.			X		Existen manuales de operación de equipos de seguridad, de red, manuales de los cursos sobre elementos de la infraestructura y actividades a realizar.
	A.12.1.2	Gestión de cambios.	Procedimiento de Gestión de Cambios.		Con el fin de mantener la disponibilidad y mitigar y gestionar los riesgos se implementa proceso de gestión de cambios.			X	X	
	A.12.1.3	Gestión de capacidad.	Procedimiento de Gestión de Capacidad		Como mejor práctica y como mecanismo para gestionar e identificar de manera temprana riesgos de disponibilidad procesos de gestión de capacidad.			X	X	
	A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación.	El Ministerio de Ambiente y Desarrollo Sostenible cuenta con separación de las instalaciones de desarrollo, pruebas y producción.		Como mejor práctica y de acuerdo a políticas de seguridad, desarrollo y gestión de tic, el ministerio tiene ambientes específicos a las actividades necesarias para cada escenario y/o necesidad.			X		
	A.12.2	**Protección contra códigos maliciosos.**								
		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	Se cuenta con consola centralizada del antivirus Kaspersky, la cual es monitoreada por el grupo de Sistemas.		Cómo una de las principales medidas preventivas se tiene consola de antivirus.			X		
	A.12.3	**Copias de respaldo.**								
		Proteger contra la pérdida de datos.								
		Respaldo de la información.	Procedimiento de Respaldo. Herramientas de backup Symantec		El Ministerio cuenta con herramienta de BackUps, procedimientos y políticas de retención y restauración.			X	X	
	A.12.4	**Registro y seguimiento.**								
		Registro de eventos y generar evidencia.								
	A.12.4.1	Registro de eventos.	Logs de Servidores, SIEM, FortiDB, Fortiweb, Fortisanbox.		Se tienen configurados logs y herramientas de registro y monitoreo de infraestructura y eventos en general.			X		
	A.12.4.2	Protección de la información de registro.	Directorio Activo. Permisos y usuarios servidores y bases de datos.		El acceso a los logs se encuentra restringido mediante roles y permisos. De igual manera se realiza backup diario de los mismos.			X		
	A.12.4.3	Registros del administrador y operador.	En el MADS las actividades de administradores y usuarios se registran en algunos sistemas de información de modo que se evidencia su trazabilidad.					X		
	A.12.4.4	Sincronización de relojes.	Se cuenta con servidor NTP para sincronización de relojes.		Los relojes del ministerio se encuentran sincronizados con el centro nacional de meteorología para facilitar procesos forenses.			X	X	
	A.12.5	**Control de software operacional.**			de aplicación como de infraestructura.					

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

CONTROLES ISO 27001			CONTROLES ACTUALES	Justificación de exclusión	Justificación de inclusión	Selección Controles y Razón de la selección				Comentario / Descripción General del Control
						RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**								
Relaciones con los proveedores	A.15.1.3	Cadena de suministro de tecnología de información y comunicación.	El Ministerio cuenta con suministro de internet con una disponibilidad alta.		cada tipo buscando una sinergia entre las mejores prácticas, el cumplimiento legal y los requisitos contractuales.	X	X	X		
	A.15.2	**Gestión de la prestación de servicios de proveedores.**								
		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.	Políticas documentadas en "M-E-GIC-01 Manual de Seguridad de la Información"		Se implementan acuerdos de confidencialidad, políticas de seguridad y requerimientos técnicos de acuerdo a cada tipo de contratación estatal y en la medida que la normatividad vigente lo permite, se implementan diferentes tipos de acuerdos para cada tipo buscando una sinergia entre las mejores prácticas, el cumplimiento legal y los requisitos contractuales.	X	X	X		
	A.15.2.2	Gestión de cambios en los servicios de los proveedores.	P-A-TIC-04 Procedimiento de Gestión de cambios. P-A-TIC-03 Procedimiento Gestión de proyectos de Sistemas de información Manual de contratación y Manual de políticas de Seguridad de la Información .			X	X	X		
Gestión de incidentes de seguridad de la información	**A.16.1**	**Gestión de incidentes y mejoras en la seguridad de la información.**								
		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.	P-E-GIC-05 Procedimiento de Gestión de Incidentes de Seguridad , Manual de Seguridad de la Información, Procedimiento de atención de solicitudes de Soporte, Herramienta ARANDA		En el Manual de Seguridad de la información y el procedimiento de gestión de incidentes se establecen responsabilidades para cumplir con las mejores prácticas y disminuir la probabilidad y/o impacto de riesgos			X	X	
	A.16.1.2	Reporte de eventos de seguridad de la información.			Se incluye control como mejor práctica para el registro de eventos e incidentes, la priorización, seguimiento y cierre, así como mantener la información actualizada e incrementar la base de conocimiento de lecciones aprendidas.			X	X	
	A.16.1.3	Reporte de debilidades de seguridad de la información.			Se han definido criterios con el fin de optimizar la atención, realizar un procedimiento adecuado, llevar un seguimiento y responder de manera oportuna y eficaz, se han establecido procedimientos y herramientas a manera de buenas prácticas para evitar materialización de riesgos y correcta aplicación de buenas prácticas.			X	X	
	A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.						X	X	
	A.16.1.5	Respuesta a incidentes de seguridad de la información.						X	X	
	A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.						X	X	
	A.16.1.7	Recolección de evidencia.						X	X	
Aspectos de seguridad de la información de la gestión de continuidad de negocio	**A.17.1**	**Continuidad de seguridad de la información.**								
		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.	G-E-GIC-02 Plan de Continuidad de Negocio Manual de Políticas de Seguridad de la Información		Se implementan planes y políticas con el fin de que ante cualquier cambio en la Continuidad, mantenga los niveles de Seguridad de la información.			X	X	
	A,17.1.2	Implementación de la continuidad de la seguridad de la información.						X	X	
	A,17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.						X	X	
	A.17.2	**Redundancias.**								
		Asegurar la disponibilidad de instalaciones de procesamiento de información.								

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

			CONTROLES ACTUALES	Justificación de exclusión	Justificación de inclusión	Selección Controles y Razón de la selección				Comentario / Descripción General del Control
						RL	OC	RN/MP	RER	
CLAUSULA	**Sec**	**Objetivo de Control**								
	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	El Ministerio contiene planeando a largo plazo adelantar procesos de contratación para DataCenter alterno y/o acuerdos administrativos		Como una buena práctica y como principal riesgo se incluye para realizar el proceso adecuado y llevar a niveles óptimos de madurez.			X	X	Se maneja y gestiona como un riesgo, se tienen acuerdos con entidades del sector como control compensatorio
Cumplimiento	**A.18.1**	**Cumplimiento de requisitos legales y contractuales.**								
		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.	Numeral 3 del documento "M-E-GIC-01 Manual de Seguridad de la Información"		Para la aplicación de normativa legal y vigente, así como la identificación en materia de seguridad de la información y políticas de privacidad y protección de datos personales, cumplimiento de ley 1581 y decretos relacionados, se han establecido procesos y procedimientos, se justifica la inclusión bajo mejores prácticas y cumplimiento normativo.	X		X		
	A.18.1.2	Derechos de propiedad intelectual.	Contratos funcionarios y contratistas.			X	X	X		
	A.18.1.3	Protección de registros.	Se cuenta con: F-A-GR-DC-02 Marcación de cajas, F-A-GR-DC-06 Consulta de documentos, F-A-GR-DC-07 Inventario Documental y F-A-GR-DC-08 Ficha préstamo de Documentos. Además de estar en los ficheros de la oficina de Talento Humano					X		
	A.18.1.4	Privacidad y protección de información de datos personales.	Ficheros de oficina de Talento Humano. Nomograma de la Entidad ley 1581			X		X		
	A.18.1.5	Reglamentación de controles criptográficos.	Numeral 8.5 del documento "M-E-GIC-01 Manual de Seguridad de la Información"					X		
	A.18.2	**Revisiones de seguridad de la información.**								
		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.	P-C-EIN-01 Evaluación independiente, P-C-EIN-02 Procedimiento de Auditorías internas		Se realiza por entes de control, control interno y auditorias externas	X		X		
	A.18.2.2	Cumplimiento con las políticas y normas de seguridad.	Contratos funcionarios y contratistas.		Por naturaleza pública se cumple con todos los requisitos normativos y se gestionan con las mejores prácticas.	X		X		
	A.18.2.3	Revisión del cumplimiento.	P-C-EIN-02 Procedimiento de Auditorías internas			X		X		