Declaración de Aplicabilidad

Contralor de Bogotá
Julián Mauricio Ruiz Rodriguez

Contralor Auxiliar
Javier Tomas Reyes Bustamante

Elaborado por:
Ana Milena Contreras Cifuentes
Alvaro Fernando Vallejo Morán
Henry Linares Castañeda
Profesionales Especializados, Dirección de Tecnologías de la Información y las Comunicaciones.

Revisado por:
Carlos Andrés Prada Durán
Director de Tecnologías de la Información y las Comunicaciones (E)
Jorge Orlando Murcia Sequeda,
Subdirector de Gestión de la Información.

Fecha:
Diciembre, 2024

Tabla de Contenido

1. INTRODUCCIÓN

La Declaración de Aplicabilidad es el documento mediante el cual la Contraloría de Bogotá D.C., define los controles de seguridad de la información aplicados por la entidad, en el desarrollo del Sistema de Gestión Seguridad de la Información SGSI, éste se fundamenta en el conjunto de controles y objetivos establecidos en el Anexo A de la Norma ISO/IEC 27001:2013 y en el Modelo de Seguridad y Privacidad expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones, mediante resolución 500 de 2021.

2. OBJETIVO

2.1 OBJETIVO GENERAL

Definir los controles de seguridad de la información aplicados por la Contraloría de Bogotá D.C., en el marco del Sistema de Gestión de Seguridad de la Información – SGSI, así como los procesos responsables de su gestión, aplicación y actualización dentro de la entidad.

2.2 OBJETIVOS ESPECIFICOS

- Establecer la aceptación o exclusión de los controles establecidos en el Anexo A de la Norma ISO/IEC 27001:2013, para su implementación por medio del Sistema de Seguridad de la Información de la Contraloría de Bogotá D.C.
- Fortalecer la seguridad de la información en la de Contraloría de Bogotá D.C., mediante la aplicación de controles para la proteger la información institucional, buscando mantener su integridad, confidencialidad y disponibilidad.

3. DECLARACIÓN DE APLICABILIDAD

La presente declaración de aplicabilidad es basada en los resultados y conclusiones de los procesos de evaluación y tratamiento de riesgos, los requisitos legales o reglamentarios, las obligaciones contractuales y/o cambios significativos de la plataforma tecnológica y/o de personal o cualquier otra situación que impacte el Sistema de Seguridad de la Información de la Contraloría de Bogotá D.C., que sea evidenciado por los procesos responsables de la implementación y gestión de los controles.

Este documento y su contenido, será sujeto de revisión en las instancias del Comité PG-DIGITAL o quien haga sus veces, cuando se requiera o en los periodos convenidos para su actualización (mínimo una vez al año).

Dominio/Control 27001:2013			Aplicabilidad del control	Justificación	APLICABILIAD / EVIDENCIAS			Responsables
					ACTIVIDAD / DOCUMENTO	POLITICAS	DOCUMENTACION SIG	
5 - Políticas de la seguridad de la información	**A.5.1 - Orientación de la dirección para la gestión de la seguridad de la información**							
	A.5.1.1 Políticas para la seguridad de la información	Control: Se debe 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	Se establece para dar cumplimento de la norma 27001 y asegurar la integridad de la información que maneja la Contraloría de Bogotá, D.C. Cumplimiento a la norma 27001:2013, MSPI de Mintic	RR 012 DE 2021	PDE-10 POLÍTICAS INSTITUCIONALES	PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL	DIRECCIONAMIENTO ESTRATEGICO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.5.1.2 Revisión de las políticas para la seguridad de la información	Control: Las políticas para seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	SI	Para hacer el adecuado control y seguimiento enfocado a posibles mejoras Cumplimiento a la norma 27001:2013, MSPI de Mintic	RR 012 DE 2021		PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL ACTA DE COMITÉ PG-DIGITAL	DIRECCIONAMIENTO ESTRATEGICO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN COMITÉ PG-DIGITAL
6. Organización de la seguridad de la información	**A.6.1 - Organización interna**							
	A.6.1.1 Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	SI	Para toma de decisiones y asignación de responsabilidades relacionadas con Seguridad de la Información Cumplimiento a la norma	R.R.046 DE 2019 R.R.031 DE 2019		PDE-02 MANUAL DEL SISTEMA INTEGRADO DE GESTION-SIG	COMITÉ PG-DIGITAL DIRECCIONAMIENTO ESTRATEGICO GESTIÓN TALENTO HUMANO GESTIÓN DE TECNOLOGIAS DE LA INFORMACION

				27001:2013, MSPI de Mintic				
	A.6.1.2. Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	SI	Garantizar la confidencialidad e integridad de la información de la entidad. Cumplimiento a la norma 27001:2013, MSPI de Mintic	R.R.046 DE 2019 R.R.031 DE 2019 R.R. 003 DE 2021 (modificada por la R.R 019 de 2023, 012 de 2023 y 009 de 2024)			COMITÉ PG-DIGITAL DIRECCIONAMIENTO ESTRATEGICO GESTIÓN TALENTO HUMANO GESTIÓN DE TECNOLOGIAS DE LA INFORMACION
	A.6.1.3. Contacto con las autoridades	Control: Se debe mantener los contactos apropiados con las autoridades pertinentes	SI	Para reportar de manera oportuna los incidentes de seguridad que puedan afectar la continuidad de la operación. Cumplimiento a la norma 27001:2013, MSPI de Mintic	DIRECTORIO DE AUTORIDADES Y GRUPOS DE EMERGENCIA DE SEGURIDAD DE LA INFORMACIÓN			COMITÉ PG-DIGITAL DIRECCIONAMIENTO ESTRATEGICO PARTICIPACIÓN CIUDADANA Y COMUNICACIÓN CON PARTES INTERESADAS
	A.6.1.4. Contacto con grupos de interés especial	Control: Se debe mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información y asociaciones de profesionales.	SI	La entidad requiere estar adscrita y/o tener contacto con grupos, asociaciones y entidades que presten asesoría en el ámbito de seguridad e intercambiar información sobre cuestiones de seguridad. Cumplimiento a la norma	MATRIZ DE IDENTIFICACIÓN PARTES INTERESADAS		PDE-02 MANUAL DEL SISTEMA INTEGRADO DE GESTION-SIG	DIRECCIONAMIENTO ESTRATEGICO PARTICIPACIÓN CIUDADANA Y COMUNICACIÓN CON PARTES INTERESADAS

				27001:2013, MSPI de Mintic				
	A.6.1.5 Seguridad de la información en gestión de proyectos	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	SI	Para gestionar la coordinación de los procesos, las herramientas, miembros del equipo y las habilidades para entregar proyectos en tiempo y con el cumplimiento de los objetivos planteados. Cumplimiento a la norma 27001:2013, MSPI de Mintic			PDE-06 PROCEDIMIENTO PARA LA GESTION DE LOS PROYECTOS DE INVERSIÓN PGTI-18 PROCEDIMIENTO GESTIÓN DE PROYECTOS CON COMPONENTE DE TI	DIRECCIONAMIENTO ESTRATEGICO GESTIÓN DE TECNOLOGIAS DE LA INFORMACION
	A.6.2 Dispositivos móviles y teletrabajo							
	A.6.2.1 Política para dispositivos móviles	Control: Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	SI	Reducir los riesgos de conexión de dispositivos móviles a la red de la CGN y/o perdida Cumplimiento a la norma 27001:2013, MSPI de Mintic		8.2. DISPOSITIVOS MÓVILES (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)		DIRECCIONAMIENTO ESTRATEGICO GESTIÓN DE TECNOLOGIAS DE LA INFORMACION
	A.6.2.2 Teletrabajo	Control: Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o	SI	La entidad ha establecido las disposiciones necesarias para dar cumplimiento a los lineamientos de teletrabajo. Cumplimiento a la norma	R.R. 014/2024	7.2. TELETRABAJO (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)		DIRECCIONAMIENTO ESTRATEGICO COMITÉ PG-DIGITAL GESTIÓN TALENTO HUMANO

		almacenada en los lugares en los que se realiza teletrabajo.		27001:2013, MSPI de Mintic				
A.7 Seguridad de los recursos humanos	**A.7.1 Antes de asumir el empleo**							
	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, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic y demás leyes aplicables a la gestión de talento humano.			PGTH-04 PROCEDIMIENTO PROVISIÓN DE EMPLEOS VACANTES DE LA PLANTA DE PERSONAL	GESTIÓN DE TALENTO HUMANO
	A.7.1.2 Términos y condiciones del 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	Cumplimiento a la norma 27001:2013, MSPI de Mintic y demás leyes aplicables a la gestión de talento humano.		7.9. PRIVACIDAD Y CONFIDENCIALIDAD (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)	PGTH-04 PROCEDIMIENTO PARA LA PROVISIÓN DE EMPLEOS EN VACANCIA DE LA PLANTA DE PERSONAL PGTH-04-06 ACUERDO DE CONFIDENCIALIDAD PGAF-08 – PROCEDIMIENTO PARA LA GESTIÓN CONTRACTUAL	GESTIÓN DE TALENTO HUMANO GESTIÓN ADMINISTRATIVA Y FINANCIERA
	A.7.2 Durante la ejecución del empleo							

	A.7.2.1 Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PDE-02 MANUAL DEL SISTEMA INTEGRADO DE GESTION-SIG	COMITÉ DIRECTIVO COMITÉ PG-DIGITAL DIRECCIONAMIENTO ESTRATEGICO
	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 pertinentes para su cargo.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTH-11 PLAN INSTITUCIONAL DE CAPACITACIÓN - PIC PGTI-12 PLAN DE SEGURIDAD DE LA INFORMACION	GESTIÓN DE TALENTO HUMANO GESTIÓN DE TECNOLOGIAS DE LA INFORMACION
	A.7.2.3 Proceso disciplinario	Control: Se debe contar con un proceso disciplinario formal el cual debe ser comunicado, para emprender acciones contra empleados hayan cometido una violación a la seguridad de la información.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		7.8. NO REPUDIO (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)	PGTH-20 PROCEDIMIENTO PARA EL TRÁMITE DEL PROCESO DISCIPLINARIO	GESTIÓN DE TALENTO HUMANO
	A.7.3 Terminación o cambio 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 validos después de la terminación o cambio de contrato se debe definir, comunicar al empleado o contratista y hacer cumplir.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic y demás leyes aplicables a la gestión de talento humano.			PGTH-10 RETIRO DEL SERVICIO DE LOS SERVIDORES PÚBLICOS PGTH-21 PROCEDIMIENTO ENTREGA DEL PUESTO DE TRABAJO PGAF-08 GESTIÓN CONTRACTUAL	GESTIÓN DE TALENTO HUMANO GESTIÓN ADMINISTRATIVA Y FINANCIERA
A.8 Gestión de activos	**A.8.1 Responsabilidad por los activos**							
	A.8.1.1 Inventario de activos	Control: Se debe identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se deber elaborar y mantener un inventario de estos activos.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		7.7. GESTIÓN DE ACTIVOS (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)	PGD-08 PROCEDIMIENTO PARA LA ACTUALIZACIÓN DE LOS INSTRUMENTOS DE GESTIÓN DE INFORMACIÓN PÚBLICA	GESTIÓN DOCUMENTAL
	A.8.1.2 Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		7.7. GESTIÓN DE ACTIVOS (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)	PGD-08 PROCEDIMIENTO PARA LA ACTUALIZACIÓN DE LOS INSTRUMENTOS DE GESTIÓN DE INFORMACIÓN PÚBLICA	GESTIÓN DOCUMENTAL

	A.8.1.3 Uso aceptable de los activos	Control: Se debe identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		8.6. USO DE LOS RECURSOS TECNOLÓGICOS (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)	PGAF-10 - PROCEDIMIENTO PARA LA GESTIÓN DE BIENES PROPIEDAD, PLANTA Y EQUIPO	GESTIÓN ADMINISTRATIVA Y FINANCIERA GESTIÓN DE TECNOLOGIAS DE LA INFORMACION
	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	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGAF-10 - PROCEDIMIENTO PARA LA GESTIÓN DE BIENES PROPIEDAD, PLANTA Y EQUIPO PGTH-21 PROCEDIMIENTO ENTREGA DEL PUESTO DE TRABAJO PGTH-10 PROCEDIMIENTO PARA EL RETIRO DEL SERVICIO DE LOS SERVIDORES PÚBLICOS	GESTIÓN ADMINISTRATIVA Y FINANCIERA GESTIÓN DE TALENTO HUMANO
	A.8.2 Clasificación de la información							
	A.8.2.1 Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		7.10. INTEGRIDAD (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)	PGD -08 PROCEDIMIENTO PARA LA ACTUALIZACIÓN DE LOS INSTRUMENTOS DE GESTIÓN DE INFORMACIÓN PÚBLICA	GESTIÓN DOCUMENTAL

	A.8.2.2 Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGD -08 PROCEDIMIENTO PARA LA ACTUALIZACIÓN DE LOS INSTRUMENTOS DE GESTIÓN DE INFORMACIÓN PÚBLICA	GESTIÓN DOCUMENTAL
	A.8.2.3 Manejo de activos	Control: Se debe desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGD -08 PROCEDIMIENTO PARA LA ACTUALIZACIÓN DE LOS INSTRUMENTOS DE GESTIÓN DE INFORMACIÓN PÚBLICA PGTH-10 PROCEDIMIENTO PARA EL RETIRO DEL SERVICIO DE LOS SERVIDORES PÚBLICOS PGTH-21 PROCEDIMIENTO ENTREGA DEL PUESTO DE TRABAJO PGAF-10 PROCEDIMIENTO PARA LA GESTIÓN DE BIENES PROPIEDAD, PLANTA Y EQUIPO	GESTIÓN ADMINISTRATIVA Y FINANCIERA GESTIÓN DOCUMENTAL GESTIÓN DE TALENTO HUMANO
	A.8.3. Manejo de medios							

	A.8.3.1 Gestión de medios removibles	Control: Se debe implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-05 PROCEDIMIENTO GESTIÓN DE RECURSOS Y SERVICIOS TECNOLÓGICOS	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.8.3.2 Disposición de los medios	Control: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic	R.R.009 DE 2020 - ESTRATEGIA CERO PAPEL PLAN INSTITUCIONAL DE GESTIÓN AMBIENTAL – PIGA		PGTI-05 PROCEDIMIENTO GESTIÓN DE RECURSOS Y SERVICIOS TECNOLÓGICOS PGAF-10 PROCEDIMIENTO PARA LA GESTIÓN DE BIENES PROPIEDAD, PLANTA Y EQUIPO PGAF-16 PROCEDIMIENTO MANEJO INTEGRAL DE RESIDUOS	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN GESTIÓN ADMINISTRATIVA Y FINANCIERA

	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	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-05 GESTIÓN DE RECURSOS Y SERVICIOS TECNOLÓGICOS PGTI-06 PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMÁTICA Y LAS COMUNICACIONES PGD-03 PROCEDIMIENTO PARA LA ACTUALIZACION Y APLICACION DE TABLAS DE RETENCION DOCUMENTAL TRD PGD-05 PROCEDIMIENTO PARA LA PRODUCCIÓN, ORGANIZACIÓN Y CONSERVACIÓN DE DOCUMENTOS	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN GESTIÓN DOCUMENTAL
A.9 Control de acceso	**A.9.1 Requisitos del negocio para control de acceso**							
	A.9.1.1 Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		8.1. CONTROL DE ACCESO LÓGICO Y FÍSICO (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.9.1.2 Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		8.4. USO DE INTERNET Y REDES SOCIALES (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y	PGTI-07 PROCEDIMIENTO CONTROL DE ACCESO USUARIO	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

		sido autorizados específicamente.				SEGURIDAD DIGITAL)		
	A.9.2 Gestión de acceso de usuarios							
	A.9.2.1 Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de usuarios, para posibilitar la asignación de los derechos de acceso.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTH-04 PROCEDIMIENTO PROVISIÓN DE EMPLEOS VACANTES DE LA PLANTA DE PERSONAL PGTH-02 PROCEDIMIENTO PARA GESTIONAR SITUACIONES ADMINISTRATIVAS PGTH-03 PROCEDIMIENTO PARA MOVIMIENTOS DE PERSONAL PGTH-21 PROCEDIMIENTO ENTREGA DEL PUESTO DE TRABAJO PGTI-07 PROCEDIMIENTO CONTROL DE ACCESO USUARIOS	GESTIÓN DE TALENTO HUMANO GESTIÓN DE TECNOLOGIAS DE LA INFORMACION
	A.9.2.2 Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTH-04 PROCEDIMIENTO PROVISIÓN DE EMPLEOS VACANTES DE LA PLANTA DE PERSONAL PGTH-02 PROCEDIMIENTO PARA GESTIONAR SITUACIONES ADMINISTRATIVAS PGTH-03	GESTIÓN DE TALENTO HUMANO GESTIÓN DE TECNOLOGIAS DE LA INFORMACION

							PROCEDIMIENTO PARA MOVIMIENTOS DE PERSONAL PGTH-21 PROCEDIMIENTO ENTREGA DEL PUESTO DE TRABAJO PGTI-07 PROCEDIMIENTO CONTROL DE ACCESO USUARIOS	
	A.9.2.3 Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		7.9. PRIVACIDAD Y CONFIDENCIALIDAD (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)	PGTI-07 PROCEDIMIENTO CONTROL DE ACCESO USUARIOS	GESTIÓN DE TECNOLOGIAS DE LA INFORMACION
	A.9.2.4 Gestión de información de autenticación secreta de usuarios	Control: La asignación de la información secreta se debe controlar por medio de un proceso de gestión formal.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-07 PROCEDIMIENTO CONTROL DE ACCESO USUARIOS	GESTIÓN DE TECNOLOGIAS DE LA INFORMACION
	A.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	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-07 PROCEDIMIENTO CONTROL DE ACCESO USUARIOS	GESTIÓN DE TECNOLOGIAS DE LA INFORMACION
	A.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	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTH-03 PROCEDIMIENTO PARA MOVIMIENTOS DE PERSONAL PGTH-21 PROCEDIMIENTO ENTREGA DEL PUESTO DE	GESTIÓN DE TALENTO HUMANO GESTIÓN DE TECNOLOGIAS DE LA INFORMACION

		deben retirar al terminar su empleo, contrato o acuerdo, o se debe ajustar cuando se hagan cambios.					TRABAJO PGTI-07 PROCEDIMIENTO CONTROL DE ACCESO USUARIO	
	A.9.3 Responsabilidades de los usuarios							
	A.9.3.1 Uso de la información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		7.9. PRIVACIDAD Y CONFIDENCIALIDAD (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)	PGTI-06 PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMÁTICA Y LAS COMUNICACIONES PGTI-07 PROCEDIMIENTO CONTROL DE ACCESO USUARIOS	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.9.4 Control de acceso a sistemas y aplicaciones							
	A.9.4.1 Restricción de acceso Información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se deben restringir de acuerdo con la política de control de acceso.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-07 PROCEDIMIENTO CONTROL DE ACCESO USUARIOS	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	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 debe controlar mediante un proceso de ingreso seguro.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-07 PROCEDIMIENTO CONTROL DE ACCESO USUARIOS	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.9.4.3 Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-07 PROCEDIMIENTO CONTROL DE ACCESO USUARIOS	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

		interactivos y deben asegurar la calidad de las contraseñas						
	A.9.4.4 Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-07 PROCEDIMIENTO CONTROL DE ACCESO USUARIOS	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.9.4.5 Control de acceso a códigos fuente de programas	Control: Se deben restringir el acceso a los códigos fuente de los programas.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-07 PROCEDIMIENTO CONTROL DE ACCESO USUARIOS	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
A.10 Criptografía	**A.10.1 Controles criptográficos**							
	A.10.1.1 Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		7.3. CONTROLES CRIPTOGRÁFICOS (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.10.1.2 Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		7.3. CONTROLES CRIPTOGRÁFICOS (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.11.1 Áreas seguras							

A.11 Seguridad física y del entorno	A.11.1.1 Perímetro de seguridad física	Control: Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGAF-20 PROCEDIMIENTO SEGURIDAD FÍSICA Y DEL ENTORNO	GESTIÓN ADMINISTRATIVA Y FINANCIERA
	A.11.1.2 Controles de Acceso físicos	Control: Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGAF-20 PROCEDIMIENTO SEGURIDAD FÍSICA Y DEL ENTORNO	GESTIÓN ADMINISTRATIVA Y FINANCIERA
	A.11.1.3 Seguridad de oficinas, recintos e instalaciones	Control: Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGAF-20 PROCEDIMIENTO SEGURIDAD FÍSICA Y DEL ENTORNO	GESTIÓN ADMINISTRATIVA Y FINANCIERA
	A.11.1.4 Protección contra amenazas externas y ambientales	Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic	PLAN DE PREVENCION, PREPARACION Y RESPUESTA ANTE EMERGENCIAS		PGAF-13 PROCEDIMIENTO IDENTIFICACIÓN DE ASPECTOS AMBIENTALES PGAF-20 PROCEDIMIENTO SEGURIDAD FÍSICA Y DEL ENTORNO	GESTIÓN DE TALENTO HUMANO GESTIÓN ADMINISTRATIVA Y FINANCIERA
	A.11.1.5 Trabajo en áreas seguras	Control: Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGAF-20 PROCEDIMIENTO SEGURIDAD FÍSICA Y DEL ENTORNO	GESTIÓN DE TALENTO HUMANO GESTIÓN ADMINISTRATIVA Y FINANCIERA
	A.11.1.6 Áreas de despacho y carga	Control: Se debe controlar los puntos de acceso tales como áreas de	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGAF-20 PROCEDIMIENTO SEGURIDAD FÍSICA Y DEL ENTORNO	GESTIÓN ADMINISTRATIVA Y FINANCIERA

		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.						
	A.11.2 Equipos							
	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 oportunidades para acceso no autorizado.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic				GESTIÓN ADMINISTRATIVA Y FINANCIERA
	A.11.2.2 Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic				GESTIÓN ADMINISTRATIVA Y FINANCIERA
	A.11.2.3 Seguridad del cableado	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debe estar protegido contra interceptación, interferencia o daño	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-05 PROCEDIMIENTO GESTIÓN DE RECURSOS Y SERVICIOS TECNOLÓGICOS	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN

	A.11.2.4 Mantenimiento de equipos	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-05 PROCEDIMIENTO GESTIÓN DE RECURSOS Y SERVICIOS TECNOLÓGICOS PGAF-17 PROCEDIMIENTO PARA EL MANTENIMIENTO INTEGRAL DE LOS INMUEBLES Y MUEBLES DE LA ENTIDAD	GESTIÓN ADMINISTRATIVA Y FINANCIERA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.11.2.5 Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGAF-10 PROCEDIMIENTO PARA EL MANEJO Y CONTROL DE ALMACÉN E INVENTARIOS	GESTIÓN ADMINISTRATIVA Y FINANCIERA
	A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones	Control: Se debe 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	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-05 PROCEDIMIENTO GESTIÓN DE RECURSOS Y SERVICIOS TECNOLÓGICOS	GESTIÓN ADMINISTRATIVA Y FINANCIERA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.11.2.7 Disposición segura o reutilización de equipos	Control: Se debe verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-05 PROCEDIMIENTO GESTIÓN DE RECURSOS Y SERVICIOS TECNOLÓGICOS PGAF-10 PROCEDIMIENTO PARA EL MANEJO Y CONTROL DE	GESTIÓN ADMINISTRATIVA Y FINANCIERA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

		sobrescrito en forma segura antes de su disposición o reutilización.					ALMACÉN E INVENTARIOS	
	A.11.2.8. Equipos de usuario desatendidos	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic	DIRECTIVA EN SERVIDOR CENTRAL - BLOQUEO DE SESIÓN	8.9. USO DE DISPOSITIVOS PROPIOS DE FUNCIONARIOS O CONTRATISTAS (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.11.2.9 Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		8.3. ESCRITORIO Y PANTALLA LIMPIOS (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
A.12 Seguridad de las operaciones	**A.12.1 Procedimientos operacionales y responsabilidades**							
	A.12.1.1 Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGD-02 PROCEDIMIENTO PARA MANTENER LA INFORMACIÓN DOCUMENTADA DEL SISTEMA INTEGRADO DE GESTIÓN - SIG	TODOS LOS PROCESOS RELACIONADOS EN ROLES Y RESPONSABILIDADES DEL SIG
	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	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-08 PROCEDIMIENTO PARA LA GESTIÓN CAMBIOS Y CAPACIDAD TECNOLÓGICA	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

		procesamiento de información que afectan la seguridad de la información.						
	A.12.1.3 Gestión de capacidad	Control: Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-08 PROCEDIMIENTO PARA LA GESTIÓN CAMBIOS Y CAPACIDAD TECNOLÓGICA	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.12.1.4 Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.12.2 Protección 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	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-06 PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMÁTICA Y LAS COMUNICACIONES	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.12.3 Copias de respaldo							

	A.12.3.1 Respaldo de información	Control: Se deben hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		7.4. COPIAS DE RESPALDO Y 8.7. POLÍTICA DE GESTIÓN DE ALMACENAMIENTO (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)	PGTI-03 PROCEDIMIENTO PARA LA GESTIÓN DE COPIAS DE RESPALDO	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.12.4 Registro y seguimiento								
	A.12.4.1 Registro de eventos	Control: Se debe elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-04 REGISTRO Y ATENCIÓN DE REQUERIMIENTOS DE SOPORTE A LOS SISTEMAS DE INFORMACIÓN Y EQUIPOS INFORMÁTICOS PGTI-10 PROCEDIMIENTO GESTIÓN INCIDENTES DE SEGURIDAD	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.12.4.2 Protección de la información de registro	Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-07 PROCEDIMIENTO DE CONTROL DE ACCESO USUARIOS	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.12.4.3 Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-06 PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMÁTICA Y LAS COMUNICACIONES	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN

	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 deberían sincronizar con una única fuente de referencia de tiempo	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic	CONFIGURACION EN SERVIDOR CENTRAL - SINCRONIZACIÓN HORA LEGAL SERVIDORES			GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.12.5 Control de software operacional							
	A.12.5.1 Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-04 PROCEDIMIENTO DE REGISTRO Y ATENCIÓN DE REQUERIMIENTOS DE SOPORTE PGTI-05 PROCEDIMIENTO DE GESTIÓN DE RECURSOS Y SERVICIOS TECNOLÓGICOS	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.12.6 Gestión de la vulnerabilidad técnica							

	A.12.6.1 Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-06 PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMÁTICA Y LAS COMUNICACIONES	GESTIÓN DE TECNOLOGIAS 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	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-05 PROCEDIMIENTO GESTIÓN DE RECURSOS Y SERVICIOS TECNOLÓGICOS PGTI-04 PROCEDIMIENTO REGISTRO Y ATENCIÓN DE REQUERIMIENTOS DE SOPORTE A LOS SISTEMAS DE INFORMACIÓN Y EQUIPOS INFORMÁTICOS PGTI-07 PROCEDIMIENTO DE CONTROL DE ACCESO A USUARIOS	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.12.7 Consideraciones sobre auditorias de sistemas de información							

	A.12.7.1 Información controles de auditoría de sistemas	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	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
A.13 Seguridad de las comunicaciones	**A.13.1 Gestión de la seguridad de las redes**							
	A.13.1.1 Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-06 PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMÁTICA Y LAS COMUNICACIONES	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.13.1.2 Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-06 PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMÁTICA Y LAS COMUNICACIONES	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN

	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	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-06 PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMÁTICA Y LAS COMUNICACIONES	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.13.2 Transferencia de información							
	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	Cumplimiento a la norma 27001:2013, MSPI de Mintic		7.13. TRANSFERENCIA DE LA INFORMACIÓN (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)		GESTIÓN DOCUMENTAL GESTIÓN DE TECNOLOGÍAS 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	Cumplimiento a la norma 27001:2013, MSPI de Mintic	CLÁUSULAS DE CUMPLIMIENTO INCLUIDAS DENTRO DE LOS CONTRATOS CON PROVEEDORES	7.13. TRANSFERENCIA DE LA INFORMACIÓN (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)		GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN GESTION ADMINISTRATIVA Y FINANCIERA
	A.13.2.3 Mensajería electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic	AVISO LEGAL (DISCLAIMER) INCLUIDO DESDE EL SERVIDOR CENTRAL EN CORREOS ELECTRONICOS	8.5. USO CORREO ELECTRONICO (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)		GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.13.2.4 Acuerdos de confidencialidad o de no divulgación	Control: Se debe identificar, revisar regularmente y documentar los requisitos para los acuerdos de	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		7.9. PRIVACIDAD Y CONFIDENCIALIDAD (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y	PGTH-04-13 ACUERDO DE CONFIDENCIALIDAD	GESTIÓN DE TALENTO HUMANO GESTIÓN ADMINISTRATIVA Y FINANCIERA

		confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.				SEGURIDAD DIGITAL)		
A.14 Adquisición, desarrollo y mantenimientos de sistemas	**A.14.1.1 Requisitos de seguridad de los sistemas de información**							
	A.14.1.1 Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		8.8. USO DE LOS SISTEMAS O HERRAMIENTAS DE INFORMACIÓN (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)	PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.14.1.2 Seguridad de servicios de las aplicaciones en redes publicas	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	Cumplimiento a la norma 27001:2013, MSPI de Mintic	CERTIFICADO SSL IMPLEMENTADO			GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.14.1.3 Protección de transacciones de los servicios de las aplicaciones	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic	CERTIFICADO SSL IMPLEMENTADO			GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN

		deben 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.						
	A.14.2 Seguridad en los procesos de desarrollo y soporte							
	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	Cumplimiento a la norma 27001:2013, MSPI de Mintic		7.5. DESARROLLO SEGURO (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)		GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	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	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-08 GESTIÓN CAMBIOS Y CAPACIDAD PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-08 GESTIÓN CAMBIOS Y CAPACIDAD PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN

		no haya impacto adverso en las operaciones o seguridad de la organización.					DE SISTEMAS DE INFORMACIÓN	
	A.14.2.4 Restricciones en los cambios a los paquetes de software	Control: Se debe 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	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-08 GESTIÓN CAMBIOS Y CAPACIDAD PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.14.2.5 Principios de construcción de sistemas seguros	Control: Se debe establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.14.2.6 Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN

		ciclo de vida de desarrollo de sistemas.						
	A.14.2.7 Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	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	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.14.2.9 Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.14.3 Datos de prueba							
	A.14.3.1 Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN

							MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	
A.15 Relación con los proveedores	**A.15.1 Seguridad de la información en las relaciones con los proveedores**							
	A.15.1.1 Política de seguridad de la información para las relaciones con proveedores	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	Cumplimiento a la norma 27001:2013, MSPI de Mintic		7.6. RELACIONES CON LOS PROVEEDORES (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)	PGAF-08 PROCEDIMIENTO PARA LA GESTIÓN CONTRACTUAL	GESTIÓN ADMINISTRATIVA Y FINANCIERA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se debe 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	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGAF-08 PROCEDIMIENTO PARA LA GESTIÓN CONTRACTUAL	GESTIÓN ADMINISTRATIVA Y FINANCIERA
	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	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGAF-08 PROCEDIMIENTO PARA LA GESTIÓN CONTRACTUAL	GESTIÓN ADMINISTRATIVA Y FINANCIERA

		suministro de productos y servicios de tecnología de información y comunicación.						
	A.15.2 Gestión de la prestación de servicios 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	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGAF-08 PROCEDIMIENTO PARA LA GESTIÓN CONTRACTUAL	GESTIÓN ADMINISTRATIVA Y FINANCIERA
	A.15.2.2 Gestión de cambios en los servicios de proveedores	Control: Se debe 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	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGAF-08 PROCEDIMIENTO PARA LA GESTIÓN CONTRACTUAL PGTI-08 GESTIÓN CAMBIOS Y CAPACIDAD	GESTIÓN ADMINISTRATIVA Y FINANCIERA GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.16.1 Gestión de incidentes y mejoras en la seguridad de la información							

A.16 Gestión de incidentes de seguridad de la información	A.16.1.1 Responsabilidades y procedimientos	Control: Se debe establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic	R.R.046 DE 2019 R.R.031 DE 2019	7.11. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)	PDE-02 MANUAL DEL SISTEMA INTEGRADO DE GESTION-SIG	COMITÉ PG-DIGITAL DIRECCIONAMIENTO ESTRATEGICO GESTIÓN TALENTO HUMANO GESTIÓN DE TECNOLOGIAS DE LA INFORMACION
	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	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-04 REGISTRO Y ATENCIÓN DE REQUERIMIENTOS DE SOPORTE A LOS SISTEMAS DE INFORMACIÓN Y EQUIPOS INFORMÁTICOS PGTI-10 PROCEDIMIENTO GESTIÓN INCIDENTES DE SEGURIDAD	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.16.1.3 Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-04 REGISTRO Y ATENCIÓN DE REQUERIMIENTOS DE SOPORTE A LOS SISTEMAS DE INFORMACIÓN Y EQUIPOS INFORMÁTICOS PGTI-10 PROCEDIMIENTO GESTIÓN INCIDENTES DE SEGURIDAD	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN

		sistemas o servicios.						
	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 deben decidir si se van a clasificar como incidentes de seguridad de la información.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-04 REGISTRO Y ATENCIÓN DE REQUERIMIENTOS DE SOPORTE A LOS SISTEMAS DE INFORMACIÓN Y EQUIPOS INFORMÁTICOS PGTI-10 PROCEDIMIENTO GESTIÓN INCIDENTES DE SEGURIDAD	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.16.1.5 Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-10 PROCEDIMIENTO GESTIÓN INCIDENTES DE SEGURIDAD	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	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 debe usar para reducir la posibilidad o el impacto de incidentes futuros.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-04 REGISTRO Y ATENCIÓN DE REQUERIMIENTOS DE SOPORTE A LOS SISTEMAS DE INFORMACIÓN Y EQUIPOS INFORMÁTICOS PGTI-10 PROCEDIMIENTO GESTIÓN INCIDENTES DE SEGURIDAD	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN

	A.16.1.7 Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-10 PROCEDIMIENTO GESTIÓN INCIDENTES DE SEGURIDAD	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio	**A.17.1 Continuidad de seguridad de la información**							
	A.17.1.1 Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		7.14. CONTINUIDAD DE OPERACIÓN INSTITUCIONAL (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)	PGTI 15 - PLAN DE CONTINGENCIAS DE TI PGTI-03 GESTIÓN DE COPIAS DE RESPALDO	COMITÉ PG-DIGITAL DIRECCIONAMIENTO ESTRATEGICO
	A.17.1.2 Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		8.10. USO DE HERRAMIENTAS OFIMATICAS Y COLABORATIVAS EN ENTORNOS VUCA (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)	PGTI 15 - PLAN DE CONTINGENCIAS DE TI PGTI-03 GESTIÓN DE COPIAS DE RESPALDO	COMITÉ PG-DIGITAL DIRECCIONAMIENTO ESTRATEGICO GESTION DE TECNOLOGIAS DE LA INFORMACION

	A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI 15 - PLAN DE CONTINGENCIAS DE TI PGTI-03 GESTIÓN DE COPIAS DE RESPALDO	COMITÉ PG-DIGITAL DIRECCIONAMIENTO ESTRATEGICO GESTION DE TECNOLOGIAS DE LA INFORMACION
	A.17.2 Redundancias							
	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de información se debe implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI 15 - PLAN DE CONTINGENCIAS DE TI PGTI-03 GESTIÓN DE COPIAS DE RESPALDO	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
A.18 Cumplimiento	**A.18.1 Cumplimiento de requisitos legales y contractuales**							
	A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales	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	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic	MARCO LEGAL INCLUIDO EN LA DOCUMENTACION DEL SGSI Y SIG			DIRECCIONAMIENTO ESTRATEGICO TODOS LOS PROCESOS

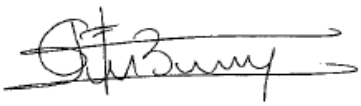
		información y para la organización.						
	A.18.1.2 Derechos de propiedad intelectual	Control: Se debe implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGTI-05 PROCEDIMIENTO GESTIÓN DE RECURSOS Y SERVICIOS TECNOLÓGICOS PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.18.1.3 Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PGD-03 PROCEDIMIENTO PARA LA ACTUALIZACIÓN Y APLICACIÓN DE TABLAS DE RETENCIÓN DOCUMENTAL TRD PGD -08 PROCEDIMIENTO PARA LA ACTUALIZACIÓN DE LOS INSTRUMENTOS DE GESTIÓN DE INFORMACIÓN PÚBLICA PGTI-03 PROCEDIMIENTO PARA LA GESTIÓN DE COPIAS DE RESPALDO	GESTIÓN DOCUMENTAL GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN

	A.18.1.4 Privacidad y protección de datos personales	Control: Cuando sea aplicable, se debe asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic	R.R.012 DE 2019	7.9. PRIVACIDAD Y CONFIDENCIALIDAD (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)	PDE-10 POLÍTICAS INSTITUCIONALES	DIRECCIONAMIENTO ESTRATEGICO
	A.18.1.5 Reglamentación de controles criptográficos	Control: se debe usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic		7.3. CONTROLES CRIPTOGRÁFICOS (PGTI-16 POLITICAS DE SEGURIDAD DE LA INFORMACION Y SEGURIDAD DIGITAL)		GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN
	A.18.2 Revisiones de seguridad de la información							
	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	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic	PROGRAMA ANUAL DE AUDITORÍAS INTERNAS PAAI		PEM-03 PROCEDIMIENTO PARA AUDITORÍA INTERNA AL SISTEMA INTEGRADO DE GESTIÓN - SIG	EVALUACION Y MEJORA

		cambios significativos.						
	A.18.2.2 Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic			PDE-08 REVISIÓN POR LA DIRECCIÓN	DIRECCIONAMIENTO ESTRATEGICO
	A.18.2.3 Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	SI	Cumplimiento a la norma 27001:2013, MSPI de Mintic	INDICADORES DEL SGSI		PGTI-06 PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMÁTICA Y LAS COMUNICACIONES PGTI-09 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGIAS DE LA INFORMACIÓN

CONTROL DE CAMBIOS

Versión	Acta Administrativo	Descripción de la Modificación
3.0	Acta No.2 de Comité PG-DIGITAL 05-dic-2023	Actualización de las evidencias de la implementación y/o evidencia de la aplicabilidad de los controles, adición de la columna de Justificación de la aplicabilidad del control y cambio al documento en formato accesible.
4.0	Acta No.02 de Comité PG-DIGITAL 06-dic-2024	Actualización de las evidencias de la implementación y/o evidencia de la aplicabilidad de los controles de seguridad de la información aplicados por la entidad y establecidos en el Anexo A de la Norma ISO/IEC 27001:2013.
5.0		

Responsable de Proceso que Aprueba	
Cargo	Director Técnico
Dependencia	Dirección de Tecnologías de la Información y las Comunicaciones
Nombre Completo	Carlos Andrés Prada Durán
Firma	
Director de Planeación que Realiza Revisión Técnica	
Nombre Completo	Sandra Patricia Bohorquez González
Firma	

Fecha publicación formato: 30/09/2024.