	Responsable del Proceso	**Dirección de Planeación**
	Aprobación	**Revisión Técnica**
Firma:		
Nombre:	CARLOS ANDRES PRADA DURAN	ANA MARÍA OCHOA VILLEGAS
Cargo:	Director Técnico (E)	Directora Técnica
Dependencia:	Dirección de Tecnologías de la Información y las Comunicaciones	Dirección de Planeación
Acta de Comité PGDIGITAL Nº 1 del 5 mayo 2022		Fecha publicación: 30 de junio de 2022

JULIÁN MAURICIO RUÍZ RODRÍGUEZ
Contralor de Bogotá, D.C.

CARLOS ORLANDO ACUÑA RUÍZ
Contralor Auxiliar

ANA MARÍA OCHOA VILLEGAS
Directora Técnica de Planeación

CARLOS ANDRES PRADA DURAN
Director Técnico de Tecnologías de la Información y las Comunicaciones (E)

Bogotá, D.C., junio de 2022

TABLA DE CONTENIDO

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.

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 dentro de la entidad.

OBJETIVOS ESPECÍFICOS

- Establecer la aceptación o exclusión de los controles establecidos en el Anexo A de la Norma ISO/IEC 27001:2013, para su implementación a través del Sistema de Seguridad de la Información de la Contraloría de Bogotá D.C.

- Fortalecer la seguridad de la información en la Contraloría de Bogotá D.C., mediante la aplicación de controles para la proteger la información institucional, buscando mantener su integridad, confidencialidad y disponibilidad.

DECLARACIÓN DE APLICABILIDAD

La presente declaración de aplicabilidad será revisada con base en los resultados de cada nuevo proceso de valoración de riesgos y/o ante cambios significativos de la plataforma tecnológica y/o de personal o cualquier otra que impacte el Sistema de Seguridad de la Información de la Contraloría de Bogotá D.C.

Esta información, será sujeta de verificación en los procesos de revisión por el Comité PG-DIGITAL o quien haga sus veces, cuando se requiera o en los periodos convenidos para su actualización.

Dominio/Control 27001:2013			Aplicabilidad del control	APLICABILIAD			Responsables
				ACTIVIDAD / DOCUMENTO	POLÍTICAS	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	RR 012 DE 2021	PDE-10 POLÍTICAS INSTITUCIONALES	PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	DIRECCIONAMIENTO ESTRATÉGICO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN GESTIÓN DE TALENTO HUMANO
	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	RR 012 DE 2021	PDE-10 POLÍTICAS INSTITUCIONALES	PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	DIRECCIONAMIENTO ESTRATÉGICO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN GESTIÓN DE TALENTO HUMANO COMITÉ PG-DIGITAL (o quien haga sus veces)
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	R.R.046 DE 2019 R.R.031 DE 2019		PDE-02 MANUAL DEL SISTEMA INTEGRADO DE GESTION-SIG	COMITÉ PG-DIGITAL (o quien haga sus veces) DIRECCIONAMIENTO ESTRATÉGICO GESTIÓN TALENTO HUMANO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	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	R.R.046 DE 2019 R.R.031 DE 2019 R.R. 003 DE 2021		MANUAL DE FUNCIONES Y DE COMPETENCIAS LABORALES	COMITÉ PG-DIGITAL (o quien haga sus veces) DIRECCIONAMIENTO ESTRATÉGICO GESTIÓN TALENTO HUMANO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

A.6.1.3. Contacto con las autoridades	Control: Se debe mantener los contactos apropiados con las autoridades pertinentes.	SI			PDE-02 MANUAL DEL SISTEMA INTEGRADO DE GESTION-SIG	COMITÉ PG-DIGITAL (o quien haga sus veces) DIRECCIONAMIENTO ESTRÁTEGICO 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			PDE-02 MANUAL DEL SISTEMA INTEGRADO DE GESTION-SIG	COMITÉ PG-DIGITAL (o quien haga sus veces) DIRECCIONAMIENTO ESTRATÉGICO PARTICIPACIÓN CIUDADANA Y COMUNICACIÓN CON PARTES INTERESADAS
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			PDE-06 PROCEDIMIENTO PARA LA GESTIÓN DE LOS PROYECTOS DE INVERSIÓN PGTI-18 PROCEDIMIENTO GESTIÓN DE PROYECTOS CON COMPONENTE DE TI	DIRECCIONAMIENTO ESTRATÉGICO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
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		8.2. DISPOSITIVOS MÓVILES (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)		DIRECCIONAMIENTO ESTRATÉGICO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
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 almacenada en los lugares en los que se realiza teletrabajo.	SI	R.R.014 DE 2019	7.2. TELETRABAJO (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)		DIRECCIONAMIENTO ESTRATÉGICO COMITÉ PG-DIGITAL (o quien haga sus veces) GESTIÓN TALENTO HUMANO

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			PGTH-04 PROCEDIMIENTO PROVISIÓN DE EMPLEOS VACANTES DE LA PLANTA DE PERSONAL PGAF-08 - GESTIÓN CONTRACTUAL	GESTIÓN DE TALENTO HUMANO GESTIÓN ADMINISTRATIVA Y FINANCIERA
	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		7.9. PRIVACIDAD Y CONFIDENCIALIDAD (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)	**PGTH-04** PROCEDIMIENTO PROVISIÓN DE EMPLEOS VACANTES DE LA PLANTA DE PERSONAL **PGTH-04-13** ACUERDO DE CONFIDENCIALIDAD PGAF-08 - 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			**PDE-02** MANUAL DEL SISTEMA INTEGRADO DE GESTIÓN-SIG	COMITÉ DIRECTIVO COMITÉ PG-DIGITAL (o quien haga sus veces) DIRECCIONAMIENTO ESTRATÉGICO
	A.7.2.2 Toma de conciencia, educación y formación en la	Control: Todos los empleados de la organización, y en donde sea pertinente, los	SI			**PGTH-11** PLAN INSTITUCIONAL DE CAPACITACIÓN - PIC	GESTIÓN DE TALENTO HUMANO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

	seguridad de la información	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.				PGTI-14 GESTIÓN DE CULTURA ORGANIZACIONAL EN EL SGSI	
	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		7.8. NO REPUDIO (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 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 deben definir, comunicar al empleado o contratista y hacer cumplir.	SI			**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	SERVIDOR INSTITUCIONAL DATACONTRABOG PLAN DE PRESERVACION DIGITAL	7.7. GESTIÓN DE ACTIVOS (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 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		7.7. GESTIÓN DE ACTIVOS (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)	**PGD-08** PROCEDIMIENTO PARA LA ACTUALIZACIÓN DE LOS INSTRUMENTOS DE GESTIÓN DE INFORMACIÓN PÚBLICA PGD-05 PROCEDIMIENTO PARA LA PRODUCCIÓN, ORGANIZACIÓN Y CONSERVACIÓN DE DOCUMENTOS	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		8.6. USO DE LOS RECURSOS TECNOLÓGICOS (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)	**PGAF-10** - PROCEDIMIENTO PARA LA GESTIÓN DE BIENES PROPIEDAD, PLANTA Y EQUIPO	GESTIÓN ADMINISTRATIVA Y FINANCIERA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
A.8.1.4 Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	SI			PGAF-10 - PROCEDIMIENTO PARA LA GESTIÓN DE BIENES PROPIEDAD, PLANTA Y EQUIPO PGAF-08 - GESTIÓN CONTRACTUAL 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	TABLAS DE RETENCIÓN DOCUMENTAL CUADRO DE CLASIFICACION DOCUMENTAL SISTEMA INTEGRADO DE CONSERVACIÓN	7.10. INTEGRIDAD (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 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			**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			**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	SISTEMA INTEGRADO DE CONSERVACIÓN PROGRAMA DE GESTIÓN DOCUMENTAL		**PGTI-05** PROCEDIMIENTO GESTIÓN DE RECURSOS Y SERVICIOS TECNOLÓGICOS GESTIÓN DOCUMENTAL	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	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	TABLAS DE CONTROL DE ACCESO HOJA DE CONTROL DE ACCESO		**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		8.1. CONTROL DE ACCESO LÓGICO Y FÍSICO (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 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 sido	SI	VPN (Virtual Private Network - Red privada virtual)	8.4. USO DE INTERNET Y REDES SOCIALES (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y	**PGTI-07** PROCEDIMIENTO CONTROL DE ACCESO USUARIO	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

	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			**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 PGAF-08 GESTIÓN CONTRACTUAL	GESTIÓN DE TALENTO HUMANO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN GESTIÓN ADMINISTRATIVA Y FINANCIERA
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			**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	GESTIÓN DE TALENTO HUMANO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN GESTIÓN ADMINISTRATIVA Y FINANCIERA

					PGTI-07 PROCEDIMIENTO CONTROL DE ACCESO USUARIOS PGAF-08 GESTIÓN CONTRACTUAL	
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		7.9. PRIVACIDAD Y CONFIDENCIALIDAD (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)	**PGTI-07** PROCEDIMIENTO CONTROL DE ACCESO USUARIOS	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
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			**PGTI-07** PROCEDIMIENTO CONTROL DE ACCESO USUARIOS	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
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			**PGTI-07** PROCEDIMIENTO CONTROL DE ACCESO USUARIOS	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
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 deben retirar al terminar su empleo, contrato o acuerdo, o se debe ajustar cuando se hagan cambios.	SI			**PGTH-03** PROCEDIMIENTO PARA MOVIMIENTOS DE PERSONAL **PGTH-21** PROCEDIMIENTO ENTREGA DEL PUESTO DE TRABAJO **PGTI-07** PROCEDIMIENTO CONTROL DE ACCESO USUARIO PGAF-08 GESTIÓN CONTRACTUAL	GESTIÓN DE TALENTO HUMANO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN GESTIÓN ADMINISTRATIVA Y FINANCIERA
A.9.3 Responsabilidades de los usuarios						
A.9.3.1 Uso de la información de	Control: Se debe exigir a los usuarios que cumplan las prácticas de la	SI		7.9. PRIVACIDAD Y CONFIDENCIALIDAD (PGTI-16	**PGTI-06** PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMÁTICA Y LAS	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

	autenticación secreta	organización para el uso de información de autenticación secreta.			POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)	COMUNICACIONES **PGTI-07** PROCEDIMIENTO CONTROL DE ACCESO USUARIOS	
	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 debe restringir de acuerdo con la política de control de acceso.	SI			**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			**PGTI-07** PROCEDIMIENTO CONTROL DE ACCESO USUARIOS PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.9.4.3 Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas	SI			**PGTI-07** PROCEDIMIENTO CONTROL DE ACCESO USUARIOS	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	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			**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			**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	Control: Se debe desarrollar e implementar una política sobre el uso	SI		7.3. CONTROLES CRIPTOGRÁFICOS (PGTI-16 POLÍTICAS DE		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

	controles criptográficos	de controles criptográficos para la protección de la información.			SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)		
	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		7.3. CONTROLES CRIPTOGRÁFICOS (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)		GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	**A.11.1 Áreas seguras**						
	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				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				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				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	PLAN DE PREVENCIÓN, PREPARACION Y RESPUESTA ANTE EMERGENCIAS		**PGAF-13** PROCEDIMIENTO IDENTIFICACIÓN DE ASPECTOS AMBIENTALES	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	POLÍTICA SG-SST			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 despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	SI				GESTIÓN ADMINISTRATIVA Y FINANCIERA
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				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				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			**PGTI-05** PROCEDIMIENTO GESTIÓN DE RECURSOS Y SERVICIOS TECNOLÓGICOS	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
A.11.2.4 Mantenimiento de equipos	Control: Los equipos se deberían mantener correctamente para	SI	CRONOGRAMA DE MANTENIMIENTO ANUAL DE		**PGTI-05** PROCEDIMIENTO GESTIÓN DE RECURSOS Y SERVICIOS TECNOLÓGICOS	GESTIÓN ADMINISTRATIVA Y FINANCIERA GESTIÓN DE

	asegurar su disponibilidad e integridad continuas.		EQUIPOS DE COMPUTO		**PGAF-17** PROCEDIMIENTO PARA EL MANTENIMIENTO INTEGRAL DE LOS INMUEBLES Y MUEBLES DE LA ENTIDAD	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			**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			**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 sobrescrito en forma segura antes de su disposición o reutilización.	SI			**PGTI-05** PROCEDIMIENTO GESTIÓN DE RECURSOS Y SERVICIOS TECNOLÓGICOS **PGAF-10** PROCEDIMIENTO PARA EL MANEJO Y CONTROL DE ALMACÉN E INVENTARIOS	GESTIÓN ADMINISTRATIVA Y FINANCIERA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
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	CONFIGURACION EN SERVIDOR CENTRAL - BLOQUEO DE SESIÓN	8.9. USO DE DISPOSITIVOS PROPIOS DE FUNCIONARIOS O CONTRATISTAS (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 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		8.3. ESCRITORIO Y PANTALLA LIMPIOS (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 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			**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 procesamiento de información que afectan la seguridad de la información.	SI			**PGTI-08** PROCEDIMIENTO PARA LA GESTIÓN CAMBIOS Y CAPACIDAD TECNOLÓGICA	GESTIÓN DE TECNOLOGÍAS 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			**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			**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	HERRAMIENTAS DE ANTIVIRUS Y FIREWALL		**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		7.4. COPIAS DE RESPALDO Y 8.7. POLÍTICA DE GESTIÓN DE ALMACENAMIENTO (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)	**PGTI-03** PROCEDIMIENTO PARA LA REALIZACIÓN Y CONTROL 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	INFORMES TRIMESTRALES DE SEGURIDAD LÓGICA		**PGTI-08** PROCEDIMIENTO DE GESTIÓN CAMBIOS Y CAPACIDAD	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			**PGTI-07** PROCEDIMIENTO DE CONTROL DE ACCESO USUARIOS	GESTIÓN DE TECNOLOGÍAS 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			**PGTI-06** PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMÁTICA Y LAS COMUNICACIONES	GESTIÓN DE TECNOLOGÍAS 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	CONFIGURACIÓN EN SERVIDOR CENTRAL - SINCRONIZACIÓN HORA LEGAL SERVIDORES			GESTIÓN DE TECNOLOGÍAS 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			**PGTI-04** PROCEDIMIENTO DE REGISTRO Y ATENCIÓN DE REQUERIMIENTOS DE SOPORTE **PGTI-05** PROCEDIMIENTO DE GESTIÓN DE RECURSOS Y SERVICIOS TECNOLÓGICOS	GESTIÓN DE TECNOLOGÍAS 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	INFORME DE VULNERABILIDADES		**PGTI-06** PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMÁTICA Y LAS COMUNICACIONES	GESTIÓN DE TECNOLOGÍAS 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			**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 TECNOLOGÍAS 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			**PGTI-09** PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN PGTI-08 PROCEDIMIENTO DE GESTIÓN CAMBIOS Y CAPACIDAD	GESTIÓN DE TECNOLOGÍAS 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			**PGTI-06** PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMÁTICA Y LAS COMUNICACIONES	GESTIÓN DE TECNOLOGÍAS 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	CATALOGO DE SERVICIOS DE TI		**PGTI-06** PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMÁTICA Y LAS COMUNICACIONES	GESTIÓN DE TECNOLOGÍAS 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			**PGTI-06** PROCEDIMIENTO GESTIÓN DE SEGURIDAD INFORMÁTICA Y LAS COMUNICACIONES	GESTIÓN DE TECNOLOGÍAS 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		7.13. TRANSFERENCIA DE LA INFORMACIÓN (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 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	CLÁUSULAS DE CUMPLIMIENTO INCLUIDAS DENTRO DE LOS CONTRATOS CON PROVEEDORES	7.13. TRANSFERENCIA DE LA INFORMACIÓN (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)		GESTIÓN DE TECNOLOGÍAS 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	AVISO LEGAL (DISCLAIMER) INCLUIDO DESDE EL SERVIDOR CENTRAL EN CORREOS ELECTRONICOS	8.5. USO CORREO ELECTRONICO (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)		GESTIÓN DE TECNOLOGÍAS 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 confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	SI	CLÁUSULAS DE CONFIDENCIALIDAD INCLUIDAS DENTRO DE LOS CONTRATOS	7.9. PRIVACIDAD Y CONFIDENCIALIDAD (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)	**PGTH-04-13** ACUERDO DE CONFIDENCIALIDAD	GESTIÓN DE TALENTO HUMANO GESTIÓN ADMINISTRATIVA Y FINANCIERA

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		8.8. USO DE LOS SISTEMAS O HERRAMIENTAS DE INFORMACIÓN (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)	**PGTI-09** PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGÍAS 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	CERTIFICADO SSL IMPLEMENTADO PARA EL SITIO WEB E INTRANET			GESTIÓN DE TECNOLOGÍAS 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 debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	SI	CERTIFICADO SSL IMPLEMENTADO PARA EL SITIO WEB E INTRANET			GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	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		7.5. DESARROLLO SEGURO (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)	PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGÍAS 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			**PGTI-08** GESTIÓN CAMBIOS Y CAPACIDAD PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGÍAS 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 no haya impacto adverso en las operaciones o seguridad de la organización.	SI			**PGTI-08** GESTIÓN CAMBIOS Y CAPACIDAD **PGTI-09** PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGÍAS DE LA 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			**PGTI-08** GESTIÓN CAMBIOS Y CAPACIDAD PGTI-09 PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGÍAS 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			**PGTI-09** PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGÍAS 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	SI			**PGTI-09** PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

	que comprendan todo el 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			**PGTI-09** PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGÍAS 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			**PGTI-09** PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGÍAS 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			**PGTI-09** PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGÍAS 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			**PGTI-09** PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.	GESTIÓN DE TECNOLOGÍAS DE LA 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		7.6. RELACIONES CON LOS PROVEEDORES (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 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			**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 suministro de productos y servicios de tecnología de información y comunicación.	SI			**PGAF-08** PROCEDIMIENTO PARA LA GESTIÓN CONTRACTUAL	GESTIÓN ADMINISTRATIVA Y FINANCIERA
	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			**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			**PGAF-08** PROCEDIMIENTO PARA LA GESTIÓN CONTRACTUAL **PGTI-08** GESTIÓN CAMBIOS Y CAPACIDAD	GESTIÓN ADMINISTRATIVA Y FINANCIERA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	**A.16.1 Gestión de incidentes y mejoras en la seguridad de la información**						
	A.16.1.1 Responsabilidades y procedimientos	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	R.R.046 DE 2019 R.R.031 DE 2019	7.11. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)	**PDE-02** MANUAL DEL SISTEMA INTEGRADO DE GESTION-SIG	COMITÉ PG-DIGITAL (o quien haga sus veces) DIRECCIONAMIENTO ESTRATÉGICO GESTIÓN TALENTO HUMANO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
	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			**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.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 sistemas o servicios.	SI			**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.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			**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.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			**PGTI-10** PROCEDIMIENTO GESTIÓN INCIDENTES DE SEGURIDAD	GESTIÓN DE TECNOLOGÍAS 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			**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.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			**PGTI-10** PROCEDIMIENTO GESTIÓN INCIDENTES DE SEGURIDAD	GESTIÓN DE TECNOLOGÍAS 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	PGTI-19 ANÁLISIS DE IMPACTO AL NEGOCIO – BIA PGTI -15 PLAN DE CONTINGENCIA DE TIC PLAN DE PREVENCIÓN, PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS	7.14. CONTINUIDAD DE OPERACIÓN INSTITUCIONAL (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)		COMITÉ PG-DIGITAL (o quien haga sus veces) DIRECCIONAMIENTO ESTRATÉGICO
	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	PGTI-19 ANÁLISIS DE IMPACTO AL NEGOCIO – BIA PGTI -15 PLAN DE CONTINGENCIA DE TIC PLAN DE PREVENCIÓN, PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS	8.10. USO DE HERRAMIENTAS OFIMATICAS Y COLABORATIVAS EN ENTORNOS VUCA (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)		COMITÉ PG-DIGITAL (o quien haga sus veces) DIRECCIONAMIENTO ESTRATÉGICO GESTION DE TECNOLOGÍAS DE LA INFORMACIÓN
	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	PGTI-19 ANÁLISIS DE IMPACTO AL NEGOCIO – BIA PGTI -15 PLAN DE CONTINGENCIA DE TIC PLAN DE PREVENCIÓN, PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS		**PDE-07** PROCEDIMIENTO PARA LA ADMINISTRACION INTEGRAL DE LOS RIESGOS INSTITUCIONALES	COMITÉ PG-DIGITAL (o quien haga sus veces) DIRECCIONAMIENTO ESTRATÉGICO GESTION DE TECNOLOGÍAS DE LA INFORMACIÓN
	A.17.2 Redundancias						
	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	SI	PROYECTO PETI 2022 - DISEÑO DE UN CENTRO DE DATOS ALTERNO SEDE SAN CAYETANO			GESTIÓN ADMINISTRATIVA Y FINANCIERA GESTIÓN DE TECNOLOGÍAS 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 información y para la organización.	SI	MARCO LEGAL INCLUIDO EN LA DOCUMENTACION DEL SGSI Y SIG			DIRECCIONAMIENTO ESTRATÉGICO TODOS LOS PROCESOS
	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			**PGTI-05** PROCEDIMIENTO GESTIÓN DE RECURSOS Y SERVICIOS TECNOLÓGICOS **PGTI-09** PROCEDIMIENTO PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	GESTIÓN DE TECNOLOGÍAS 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	TABLAS DE CONTROL DE ACCESO		**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 REALIZACIÓN Y CONTROL DE COPIAS DE RESPALDO	GESTIÓN DOCUMENTAL GESTIÓN DE TECNOLOGÍAS 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	R.R.012 DE 2019	7.9. PRIVACIDAD Y CONFIDENCIALIDAD (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)	**PDE-10** POLÍTICAS INSTITUCIONALES	DIRECCIONAMIENTO ESTRATÉGICO
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		7.3. CONTROLES CRIPTOGRÁFICOS (PGTI-16 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL)		GESTIÓN DE TECNOLOGÍAS 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 cambios significativos.	SI	PROGRAMA ANUAL DE AUDITORÍAS INTERNAS PAAI		**PEM-03** PROCEDIMIENTO PARA AUDITORÍA INTERNA AL SISTEMA INTEGRADO DE GESTIÓN - SIG	EVALUACION Y MEJORA
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,	SI			**PDE-08** REVISIÓN POR LA DIRECCIÓN	DIRECCIONAMIENTO ESTRATÉGICO

		con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.					
	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	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 TECNOLOGÍAS DE LA INFORMACIÓN

CONTROL DE CAMBIOS

Versión	R.R., Acta[1] y Fecha	Descripción de la Modificación
1.0	Acta No.5 Comité SIGEL 19-dic-2018	Versión Inicial
2.0	Acta No.2 Comité PG-DIGITAL 11-jun-2020	Actualización de los responsables de la implementación de los controles y ajuste de estos a los nombres de procesos.
3.0	Acta No.1 Comité PG-DIGITAL 05-may-2022	Actualización de los responsables de la implementación de los controles, ajuste de estos a los nombres de procesos y se clasifica la aplicabilidad del control así: Actividad / Documento; Políticas; Documentación SIG
4.0		

[1]Registrar Acta con el nombre del Comité y su correspondiente N° y fecha, si se adoptó por resolución reglamentaria igual se registra su N° y fecha.