Consejo de Protección de Derechos del Distrito Metropolitano de Quito

POLÍTICAS DE LA GESTIÓN INTERNA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CONSEJO DE PROTECCIÓN DE DERECHOS DEL DISTRITO METROPOLITANO DE QUITO

DIRECCIÓN ADMINISTRATIVA FINANCIERA Y LA GESTIÓN INTERNA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

2026

Control de versiones

VERSIÓN	FECHA	DESCRIPCIÓN	AUTOR
1.0	24/10/2025	Elaboración del documento	DAF-GITIC- ATIC4
1.1	09/02/2026	Emisión de observaciones.	DAJ - GITIC
1.2	23/06/2026	Modificación de políticas	DAF-GITIC- AI4
1.2	29/06/2026	Observaciones subsanadas, realizar ajustes de forma.	DAJ - GITIC
1.3	30/06/2026	Documento final	DAF-GITIC- AI4

FIRMAS DE RESPONSABILIDAD		
APROBADO		**FIRMA**
Valeria Jacqueline Urgiles Valle	**Secretaria Ejecutiva (E)**	Firmado electrónicamente por: VALERIA JACQUELIN URGILES VALLE
REVISADO		**FIRMA**
Johanna del Carmen Delgado Infante	**Directora Administrativa Financiera**	Firmado electrónicamente por: JOHANNA DEL CARMEN DELGADO INFANTE
Verónica Paola Betancourt Berrones	**Directora de Asesoría Jurídica**	Validar únicamente en FirmaEC. Firmado electrónicamente por: VERONICA PAOLA BETANCOURT BERRONES
ELABORADO		**FIRMA**
Henry Gustavo Villarroel Mantilla	**Analista Informático 4**	Firmado electrónicamente por: HENRY GUSTAVO VILLARROEL MANTILLA

Índice de Contenido

1. INTRODUCCIÓN: 7
2. BASE LEGAL: 10
3. GLOSARIO DE TÉRMINOS Y ABREVIATURAS: 11
4. POLÍTICAS DE GOBIERNO DIGITAL Y TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES 19
4.1. OBJETIVO, ÁMBITO DE APLICACIÓN Y GENERALIDADES 19
4.1.1. Objetivo. - 19
4.1.2. Ámbito de aplicación. - 19
4.1.3. Generalidades. - 19
4.1.3.1. De la gestión de proyectos. - 19
4.1.3.2. De las adquisiciones, desarrollos y cambios a los Sistemas de Información. - 19
4.1.3.3. De las adquisiciones de bienes y/o contratación de servicios tecnológicos. - 19
4.1.3.4. Cumplimiento. - 20
4.1.3.5. Excepciones. - 20
4.2. OBLIGACIONES RESPECTO AL USO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES 20
4.2.1. De la GITIC. – 20
4.2.2. De los funcionarios / servidores institucionales / trabajadores institucionales del CPD-DMQ. – 21
4.2.3. Del Funcionario/a Institucional de GITIC 21
4.2.4. De las de unidades / direcciones dueñas de los sistemas de información. – 22
4.3. DE LA MÁXIMA AUTORIDAD DE LA DEPENDENCIA 22
4.3.1. Rol de la Máxima Autoridad de la Dependencia. – 22
4.3.2. Responsabilidades. – 22
4.3.2.1 Gestión Funcional. – 23
4.3.2.2. Gestión no funcional. – 24
4.3.2.3. Gestión de datos. – 24
4.3.2.4. Gestión de contingencia y disponibilidad. – 24
4.4. DEL DUEÑO DE LOS SISTEMAS DE INFORMACIÓN 25
4.4.1. Rol del Dueño de los Sistemas de Información. – 25

4.4.2. Responsabilidades. – 25
4.5. DEL ADMINISTRADOR FUNCIONAL 25
4.5.1. Rol del Administrador Funcional. – 25
4.5.2. Responsabilidades. – 26
4.5.2.1. Gestión Funcional: 26
4.5.2.2. Gestión no Funcional: 27
4.5.2.3. Gestión de Datos: 28
4.5.2.4. Gestión de contingencia y disponibilidad: 28
4.6. DEL CUSTODIO 29
4.6.1. Rol del Custodio. – 29
4.6.2. Responsabilidades. – 29
5. POLÍTICAS PARA LA GESTIÓN DE GOBIERNO DIGITAL 30
5.1. DEL GOBIERNO DIGITAL 30
5.2. POLÍTICAS DE GOBIERNO DIGITAL 30
6. POLÍTICAS DE LA CALIDAD DE LOS DATOS E INFORMACIÓN 30
6.1. DE LA CALIDAD DE LOS DATOS E INFORMACIÓN 30
6.2. INTEGRIDAD DE LOS DATOS E INFORMACIÓN 31
6.3. RESPONSABILIDAD 31
7. POLÍTICAS PARA LA GESTIÓN DE PROYECTOS E INNOVACIÓN DE TIC 31
7.1. DE LOS PROYECTOS E INNOVACIÓN DE TIC 31
7.2 POLÍTICAS PARA LA GESTIÓN DE PROYECTOS E INNOVACIÓN DE TIC 31
8. POLÍTICAS PARA LA GESTIÓN DE SISTEMAS DE INFORMACIÓN Y SERVICIOS TECNOLÓGICOS 32
8.1. DE LOS SISTEMAS DE INFORMACIÓN Y SERVICIOS TECNOLÓGICOS 32
8.2. POLÍTICAS PARA LA GESTIÓN DE SISTEMAS DE INFORMACIÓN 32
8.2.1. GENERALES. – 32
8.2.2. CLASIFICACIÓN DE LOS SISTEMAS DE INFORMACIÓN. – 34
8.2.3. APLICACIONES MÓVILES (APPS) Y AULAS VIRTUALES. – 35
8.2.4. TIPOS DE ATENCIÓN PARA LOS SISTEMAS DE INFORMACIÓN 35
8.2.5. ENTORNO (AMBIENTE) DE TRABAJO. - 35
8.2.6. DERECHOS DE AUTOR. – 36
8.3. POLÍTICAS PARA LA GESTIÓN DE LOS SERVICIOS TECNOLÓGICOS 36

8.3.1. POLÍTICAS DE USO DE SOFTWARE 36
8.3.1.1. Administración 36
8.3.1.2. De la instalación de Sistemas de Información: 37
8.3.2. POLÍTICA GENERAL DE USO DE CORREO ELECTRÓNICO. - 37
8.3.2.1. Del Correo Electrónico: 37
8.3.2.2 Tipos de Cuentas: 37
8.3.2.3. Uso del servicio: 37
8.3.2.4. Responsabilidades: 38
8.3.2.5. Gestión del buzón de correo: 39
8.3.2.6. Uso inaceptable: 39
8.3.3. POLÍTICA DE ENLACE DE DATOS, USO DE INTERNET E INTRANET, DOMINIOS Y SUBDOMINIOS. – 40
8.3.3.1. De los Enlaces de Datos, Uso de Internet e Intranet, Dominios y Subdominios: 40
8.3.3.2. Políticas: 40
8.3.3.3. Dominios y subdominios: 41
8.3.4. POLÍTICA GENERAL PARA LA ADMINISTRACIÓN DE PORTALES WEB Y REDES SOCIALES. - 41
8.3.5. POLÍTICA GENERAL DE HERRAMIENTAS DE SOPORTE PARA LA MODALIDAD DE TELETRABAJO. - 42
9. POLÍTICAS PARA LA GESTIÓN DE SEGURIDAD DE TIC 42
9.1. DE LA SEGURIDAD DE TIC 42
9.2. POLÍTICAS GENERALES 42
9.2.1. GENERALES. - 42
9.2.2. RESPONSABLES DE LA SEGURIDAD DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES (TIC). - 44
9.2.2.1. De la GITIC: 44
9.2.2.2. De los servidores institucionales de TIC: 44
9.2.2.3 De las áreas institucionales: 45
9.2.3 ACUERDO DE CONFIDENCIALIDAD. - 45
9.2.4 CLASIFICACIÓN DE LA INFORMACIÓN. - 45
9.3 CONDUCTA DEL USUARIO INTERNO 47
9.4 ACCESO A RECURSOS Y PRIVILEGIOS 48

9.5 GESTIÓN DE INCIDENTES DE SEGURIDAD DE TIC 48
9.6 EXCEPCIONES DE SEGURIDAD 48
9.7 POLÍTICA GENERAL DE MANEJO DE CONTRASEÑAS 48
9.7.1 ADMINISTRACIÓN. -..... 48
10. POLÍTICAS PARA LA GESTIÓN, ADQUISICIÓN Y SERVICIOS DE INFRAESTRUCTURA..... 49
10.1 GENERALES 49
10.2 HARDWARE..... 51
10.3 DATA CENTER 52
10.4 SEGREGACIÓN FUNCIONAL 52
10.5 RESPALDO DE LA INFORMACIÓN TECNOLÓGICA 52
10.6 RETIRO DE ACCESOS 53
10.7 REGISTRO Y REVISIÓN DE TRANSACCIONES O LOGS..... 54
10.8 PROPIEDAD DE LA INFORMACIÓN..... 54
10.9 CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACIÓN.... 54
11. POLÍTICAS DE USO DE FIRMAS ELECTRÓNICAS 55
11.1 ÁMBITO..... 55
11.2 EFECTOS DE LA FIRMA ELECTRÓNICA..... 55
11.3 INSTRUMENTOS PÚBLICOS ELECTRÓNICOS 55
11.4 DE LAS INFRACCIONES AL USO DE FIRMAS ELECTRÓNICAS 55
12. PROHIBICIONES PARA EL USO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES 55
13. SANCIONES 57
13.1 INCUMPLIMIENTO DE LAS POLÍTICAS..... 57

1. INTRODUCCIÓN:

La reforma al Estatuto Orgánico de gestión Organizacional por Procesos del Consejo de Protección de Derechos del Distrito Metropolitano de Quito, aprobado mediante Resolución No. 225 de 17 de junio de 2015, en El Art. 2 determina: – *"(…) El Consejo de Protección de Derechos del Distrito Metropolitano de Quito es el organismo colegiado, paritario Estado-Sociedad Civil, que garantiza la protección y defensa de los derechos de los grupos de atención prioritaria, en situación de vulnerabilidad y/o riesgo, naturaleza y animales, en el marco del Sistema de Protección Integral del Distrito Metropolitano de Quito."*

El Art. 7 ibidem establece. – "*Representaciones Gráficas de los Procesos Institucionales (…)*"

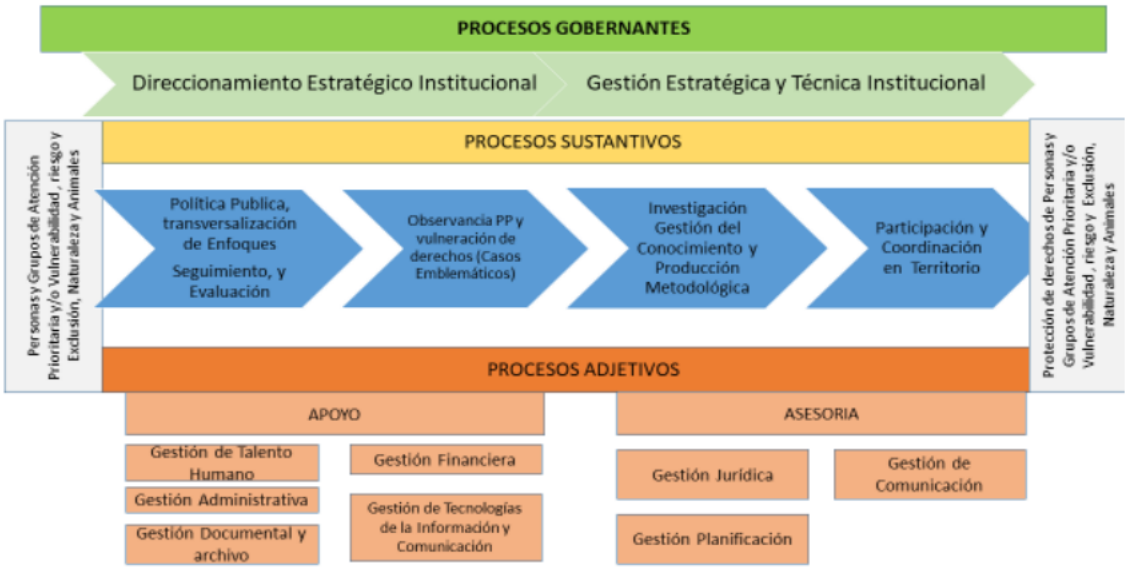

Figura Nro. 1 Cadena de Valor – CPD DMQ

El Art. 9. – *"Representación gráfica de la estructura institucional"*

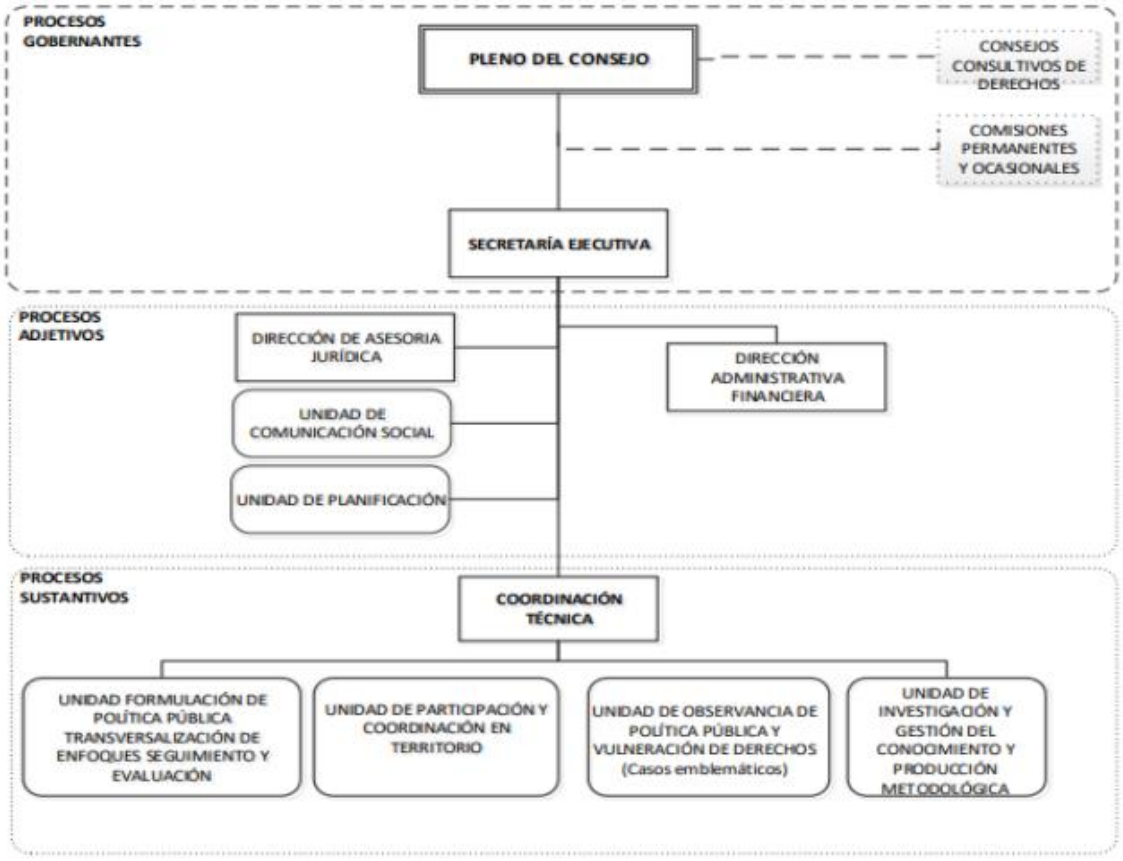

Figura Nro. 2 Estructura institucional – CPD-DMQ

Un nuevo desafío para la Gestión Interna de Tecnologías de la Información y Comunicación (GITIC), adscrita a la Dirección Administrativa Financiera del Consejo de Protección de Derechos del Distrito Metropolitano de Quito (CPD-DMQ), es potenciar el uso estratégico de las Tecnologías de la Información y la Comunicación (TIC). En este contexto, la GITIC asume un rol clave en la transformación institucional hacia un modelo más eficiente, accesible y sostenible. Su función no solo es técnica, sino que también contribuye directamente a fortalecer las capacidades del Consejo para ofrecer productos orientados a la protección integral de derechos, con enfoque inclusivo, equitativo y sin dejar a nadie atrás. Asimismo, las GITIC impulsan la innovación institucional, mejoran la eficacia operativa y permiten generar soluciones tecnológicas alineadas con los principios de participación, corresponsabilidad y justicia social que guían la labor del CPD-DMQ.

La Gestión Interna de Tecnologías de la Información y Comunicación (GITIC) del Consejo de Protección de Derechos del Distrito Metropolitano de Quito (CPD-DMQ) representa un nuevo hito en el fortalecimiento institucional del Consejo. A través de la GITIC, se promueve la adopción de estrategias y buenas prácticas tecnológicas orientadas a impulsar planes, programas y proyectos innovadores en materia de gobernanza digital,

uso de datos, herramientas para la transparencia, participación ciudadana, y conectividad. Todo ello permite avanzar hacia un manejo más inteligente, eficiente y colaborativo de los procesos internos del CPD-DMQ, facilitando la toma de decisiones basadas en evidencia y fortaleciendo los mecanismos de protección de derechos. Asimismo, esta gestión tecnológica estratégica incrementa la capacidad institucional para adoptar soluciones TIC que aporten valor, mejoren el soporte a la ciudadanía y fortalezcan la inclusión, la equidad y la resiliencia institucional.

La GITIC constituye un pilar fundamental para la gestión tecnológica y el fortalecimiento del gobierno digital dentro del Consejo de Protección de Derechos del Distrito Metropolitano de Quito (CPD-DMQ). Su rol estratégico permite articular acciones con las diferentes áreas del Consejo, orientadas a definir e implementar modelos de buenas prácticas tecnológicas, adaptadas al contexto institucional y alineadas con estándares de calidad, seguridad y control. Esto permite avanzar hacia una madurez tecnológica adecuada, garantizando eficiencia, trazabilidad e innovación en los procesos orientados a la protección y garantía de derechos.

El nuevo enfoque de la GITIC, que actualmente brinda soporte tecnológico a las operaciones institucionales del CPD-DMQ, permitirá ejecutar y sostener procesos clave para la transformación digital del Consejo. Esta transformación no solo optimiza la gestión interna, sino que también potencia la capacidad del CPD-DMQ para brindar servicios más ágiles, accesibles y centrados en la ciudadanía, fortaleciendo así su rol como garante de derechos humanos y colectivos.

La incorporación de tecnologías interoperables, seguras y confiables es fundamental para consolidar una gestión institucional moderna y sostenible. El uso estratégico de las TIC permitirá al CPD-DMQ gestionar grandes volúmenes de información de manera eficiente, generar conocimiento útil para la toma de decisiones, mejorar la conectividad interna y reforzar la seguridad digital, contribuyendo a una institución más resiliente, transparente y conectada con las necesidades de la ciudadanía.

Finalmente, la transformación digital impulsa la modernización de los servicios públicos, acercándolos a la comunidad de manera más efectiva. Esto implica integrar sistemas de información interoperables, fortalecer las redes de telecomunicaciones, aprovechar el potencial de los datos masivos para la formulación de políticas basadas en evidencia, y asegurar un entorno tecnológico confiable, con enfoque en la protección de datos y la equidad digital.

Las GITIC en cumplimiento del marco normativo vigente que rige para el buen funcionamiento del gobierno digital y de las tecnologías de información y comunicaciones, lo dispuesto por la Contraloría General del Estado en el Acuerdo No. 004-CG-2023 de 27 de febrero de 2023, “Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que

dispongan de Recursos Públicos"; así como, lo señalado en la Reforma al Estatuto Organizacional por Procesos del Consejo de Protección de Derechos del DMQ en lo que corresponde a las atribuciones y responsabilidades para la Gestión Interna de Tecnologías de la Información y Comunicación, la GITIC ha desarrollado el presente documento.

En virtud de lo expuesto, las Políticas de la Gestión Interna de Tecnologías de la Información y Comunicación del CPD-DMQ constituyen una herramienta que servirá para regular o estandarizar los procesos y/o procedimientos en el ámbito de Gobierno Digital y el uso de las Tecnologías de la Información y Comunicaciones, con el fin de garantizar la calidad en la prestación de servicios al interior de la institución y consecuentemente a la ciudadanía.

2. BASE LEGAL:

- ✓ Constitución de la Republica del Ecuador
- ✓ Ley Orgánica de la Contraloría General del Estado, publicada en el Registro Oficial Suplemento 595 de 12 de junio de 2002 y sus reformas.
- ✓ Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, publicado en el Registro Oficial Suplemento Nro. 899 de 9 de diciembre de 2016, y sus reformas.
- ✓ Ley Orgánica para la Transformación Digital y Audiovisual, publicada en el Registro Oficial Suplemento 245 de 07 de febrero de 2023.
- ✓ Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos, publicada en el Registro Oficial Suplemento 353 de 23 de octubre de 2018 y sus reformas.
- ✓ Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial Suplemento 459 de 26 de mayo de 2021.
- ✓ Ley de Comercio Electrónico, Firmas y Mensajes de Datos, publicada en el Registro Oficial Suplemento Nro. 557 de 17 de abril de 2002 y sus reformas.
- ✓ Acuerdo Nro. 004-GG-2023 de la Contraloría General del Estado, publicado en el Registro Oficial Suplemento 257 de 27 de febrero de 2023, mediante el cual se expidió las "Normas de Control Interno para las Entidades, organismos del sector público y de las personas jurídicas de derecho privado que dispongan de recursos públicos", en especial la norma 410 "Tecnología de la Información".
- ✓ Acuerdo Ministerial No. 012-2016, emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información el 23 de mayo del 2016, publicado en el Registro Oficial Nro. 783 de 24 de junio de 2016, y sus reformas.
- ✓ Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información el 8 de febrero de 2024, publicado en el Registro Oficial Tercer Suplemento Nro. 509 de 01 de marzo de 2024.

3. GLOSARIO DE TÉRMINOS Y ABREVIATURAS:

TÉRMINO	DEFINICIÓN
Acceso físico	Se refiere a la capacidad que tiene una persona para entrar o acercarse físicamente a los equipos, dispositivos o instalaciones tecnológicas de la institución, como servidores, switches, computadoras, centros de datos, racks, etc.
Acceso lógico	Es el proceso mediante el cual un usuario obtiene autorización para ingresar y utilizar recursos digitales o sistemas informáticos mediante credenciales electrónicas, como usuarios, contraseñas, tokens, certificados digitales o biometría.
Activo de información	Cualquier elemento que contenga información y tenga valor para el CPD-DMQ. Puede encontrarse almacenado en diferentes medios como Discos Duros, USB, Data Center, impresiones, entre otros.
Administrador Funcional	Servidor institucional encargado de la administración y operatividad de los sistemas de información y/o aplicativos.
Anonimización	La aplicación de medidas dirigidas a impedir la identificación o re-identificación de una persona natural, sin esfuerzos desproporcionados.
Backup	Respaldo de información.
Base de Datos	Una base de datos es una recopilación organizada de información o datos estructurados que se almacena de forma electrónica en un sistema informático. Su propósito es permitir el acceso, la gestión y la actualización de la información de manera eficiente.
Calidad de los Datos	Se refiere al estado de un conjunto de datos, evaluando qué tan adecuados son para cumplir con su propósito en un contexto específico.
Ciclo de Vida de los sistemas de información	Contempla las fases de análisis, diseño, desarrollo, pruebas, lanzamiento a producción y mantenimiento.
Consejo de Protección de Derechos CPD	El Consejo de Protección de derechos se compone de el Pleno del Consejo, Consejos Consultivos de Derechos, Comisiones Permanentes y Ocasionales, Secretaria Ejecutiva, Dirección Administrativa Financiera, Dirección de Asesoría Jurídica, Unidad de Comunicación Social, Unidad de Planificación, Coordinación Técnica, Unidad de Formulación de Política Pública Transversalización de Enfoques Seguimiento y Evaluación, Unidad de Participación y Coordinación en Territorio, Unidad de Observancia y Política Pública y Vulneración de Derechos,

TÉRMINO	DEFINICIÓN
	Unidad de Investigación y Gestión del Conocimiento y Producción Metodológica.
Consentimiento	Manifestación de voluntad libre, previa, específica, expresa, informada e inequívoca, mediante la cual el titular de los datos personales autoriza al responsable del tratamiento a recopilar, usar, almacenar y tratar dichos datos, conforme a las finalidades previamente informadas.
Cookies	Pequeños archivos de texto que un sitio web envía y almacena en el navegador del usuario durante su visita, cuya finalidad es recopilar y conservar información sobre su actividad, preferencias y configuración. Las cookies permiten reconocer al usuario en visitas posteriores, gestionar sesiones, personalizar contenidos, recordar configuraciones como el idioma, obtener estadísticas de uso y facilitar determinadas funcionalidades del sitio web, conforme a la normativa vigente en materia de protección de datos personales.
Correo Spam	Se denomina spam o correo basura a los mensajes no solicitados, generalmente de tipo publicitario, enviados masivamente a un gran número de destinatarios. Esta práctica no se limita al correo electrónico y afecta a otras plataformas como la mensajería instantánea y las redes sociales.
Cuarto de Procesamiento	Espacio físico destinado al alojamiento de servidores y equipos de procesamiento de información, que cuenta con condiciones técnicas controladas de energía eléctrica, climatización, seguridad física y conectividad, a fin de garantizar la continuidad, integridad y disponibilidad de los sistemas tecnológicos.
Cuarto de telecomunicaciones	Espacio físico específico destinado a albergar el equipamiento de telecomunicaciones, como switches, routers, paneles de parcheo y otros dispositivos de red, que cuenta con condiciones técnicas de seguridad, energía y climatización para garantizar la correcta transmisión de datos y la continuidad de los servicios de conectividad.
Custodio de la información	Unidad o área responsable de ejecutar los procesos de respaldo, almacenamiento, conservación y protección de la información institucional, así como de coordinar y aplicar los mecanismos técnicos y administrativos que garanticen su seguridad, integridad, disponibilidad y confidencialidad.
Data Center	Infraestructura física especializada destinada al alojamiento de servidores, sistemas de almacenamiento, equipos de telecomunicaciones y soluciones de cómputo, que opera bajo condiciones controladas de energía, climatización, seguridad y conectividad, con el objetivo de garantizar la disponibilidad,

TÉRMINO	DEFINICIÓN
	integridad y continuidad de los servicios tecnológicos y de la información.
DMQ	Distrito Metropolitano de Quito.
Dueño de los sistemas de información	Dependencia requirente, administradora de los sistemas de información, de los datos y de su tratamiento, representada por su máxima autoridad y que forma parte de la Estructura Orgánica Funcional del Consejo de Protección de Derechos del Distrito Metropolitano de Quito (CPD-DMQ).
Ecosistema de Innovación Tecnológica	Conjunto de actores, relaciones y dinámicas que interactúan de manera articulada, tales como empresas, instituciones educativas, Entidades gubernamentales, centros de investigación, emprendedores y otros agentes relevantes, con el propósito de promover el desarrollo, adopción y transferencia de tecnologías, así como la generación de soluciones innovadoras que impulsen el progreso económico, social e institucional.
Áreas institucionales del GAD-DMQ	Son las áreas, Entidades, agencias y unidades ejecutoras que forman parte de la estructura orgánica del Gobierno Autónomo Descentralizado del Distrito Metropolitano de Quito.
Hardware	Conjunto de componentes físicos y tangibles que conforman un sistema informático o de comunicación, tales como computadoras, servidores, impresoras, dispositivos de red y otros equipos electrónicos necesarios para el procesamiento, almacenamiento y transmisión de información.
Herramientas informáticas	Conjunto de aplicaciones y programas diseñados para facilitar tareas específicas del usuario final, tales como la gestión de documentos, análisis de datos, comunicación, diseño gráfico, desarrollo de software, entre otros, que permiten mejorar la productividad y eficiencia en diversos procesos.
Información	Conjunto de datos organizados y procesados que adquieren un significado y valor para la institución, permitiendo la toma de decisiones, el cumplimiento de objetivos y la gestión eficiente de los recursos y procesos institucionales.
Infraestructura tecnológica	Conjunto de componentes de hardware, software, redes, plataformas y servicios tecnológicos interconectados que conforman el entorno de tecnologías de la información, y que soportan, habilitan y sustentan las operaciones, procesos y servicios de la institución.
Infraestructura tecnológica de usuario final	Conjunto de equipos y herramientas tecnológicas utilizados de manera directa por los usuarios finales para el desarrollo de sus actividades, que incluye computadores, impresoras, escáneres,

TÉRMINO	DEFINICIÓN
	proyectores, dispositivos periféricos y aplicaciones informáticas, orientados a facilitar la productividad y el cumplimiento de las funciones institucionales.
Firma electrónica	Mecanismo tecnológico que constituye el equivalente digital de la firma manuscrita, utilizado para identificar al firmante y manifestar su aceptación del contenido de un documento o mensaje de datos por medios electrónicos, garantizando la autenticidad, integridad y no repudio del documento, conforme a la normativa vigente.
Gobierno Digital	Uso estratégico y sistemático de las tecnologías digitales y de la gestión de datos en la Administración Pública, como parte de los procesos de modernización del Estado, orientado a la creación de valor público, la mejora de la eficiencia institucional, la transparencia, la participación ciudadana y la calidad de los servicios ofrecidos a la sociedad.
Innovación de TIC	Aplicación de nuevas ideas, enfoques, métodos, procesos o tecnologías en el ámbito de las Tecnologías de la Información y las Comunicaciones (TIC), orientada al desarrollo, mejora o transformación de productos, servicios y procesos. Comprende áreas como el desarrollo de software y hardware, redes, aplicaciones móviles, sistemas de gestión de la información, inteligencia artificial, Internet de las Cosas (IoT), ciberseguridad, entre otras, e implica la creación o adopción de soluciones innovadoras y disruptivas que generen valor, eficiencia y mejora continua en las organizaciones.
Innovación Tecnológica	Proceso mediante el cual se introducen, adoptan o aplican nuevas tecnologías, técnicas, herramientas o métodos que generan mejoras significativas en productos, servicios o procesos existentes. Estas mejoras pueden reflejarse en la eficiencia operativa, la funcionalidad, la calidad, la seguridad, la accesibilidad o la optimización de recursos, contribuyendo al desarrollo, modernización y competitividad de las organizaciones.
Integridad de la información	Principio de seguridad que garantiza que la información, ya sea almacenada, procesada o transmitida, se mantiene completa, exacta y confiable, asegurando que no ha sido alterada, modificada, eliminada o destruida de forma accidental o intencionada, sin la debida autorización.
Internet	Red informática global de comunicación que interconecta millones de redes y dispositivos a nivel mundial, permitiendo el intercambio de información, datos y servicios de diversa naturaleza entre sus usuarios, mediante protocolos

TÉRMINO	DEFINICIÓN
	estandarizados. Su denominación proviene del término en inglés International Network (red internacional).
Malware	Refiere a cualquier tipo de software malicioso diseñado con el propósito de causar daño, interrumpir el funcionamiento, obtener acceso no autorizado o robar información de sistemas informáticos, dispositivos o redes. El malware incluye, entre otros, virus, gusanos, troyanos, spyware, ransomware y otros programas que representan una amenaza para la seguridad de la información y la infraestructura tecnológica.
Máxima Autoridad de la Dependencia	Funcionario Directivo representante de la dependencia institucional, dueña de la información que tiene capacidad de toma de decisiones.
Outsourcing	Término en idioma inglés que se refiere a la subcontratación, externalización o tercerización de servicios, procesos o funciones de una institución a un proveedor externo especializado, con el fin de optimizar recursos, mejorar la eficiencia operativa y enfocarse en las actividades estratégicas.
Password	Término en idioma inglés que se traduce como contraseña y corresponde a una clave de acceso utilizada para autenticar la id institución de un usuario y permitir el ingreso seguro a sistemas, aplicaciones, equipos o servicios digitales.
POA	Plan Operativo Anual.
Proyecto de TIC	Un proyecto de Tecnologías de la Información y Comunicación (TIC) es una iniciativa planificada, estructurada y con objetivos definidos, orientada a implementar, mejorar o desarrollar soluciones tecnológicas que optimicen la gestión, comunicación, procesamiento, seguridad y almacenamiento de la información dentro de una institución o institución. Estos proyectos pueden comprender, entre otros, la implementación de infraestructura de hardware, el desarrollo o adquisición de software, la puesta en marcha de sistemas de información, el fortalecimiento de la ciberseguridad y la adopción de tecnologías emergentes o disruptivas.
Ráfagas de correo	Se refiere al envío masivo de múltiples correos electrónicos desde una misma cuenta o sistema en un corto período de tiempo. En el contexto de la seguridad informática, este comportamiento puede constituir un indicador de actividades maliciosas, tales como spam, phishing, suplantación de id institución o la distribución de malware, y puede afectar la disponibilidad, reputación y seguridad de los servicios de correo electrónico institucionales.

TÉRMINO	DEFINICIÓN
Recuperación de sistemas de información	Es el conjunto de procedimientos y acciones técnicas que se ejecutan para restablecer un sistema de información a un estado operativo previo, utilizando copias de seguridad previamente generadas, con el fin de garantizar la continuidad del servicio, la disponibilidad de la información y la mitigación de impactos ante fallos, incidentes o eventos adversos.
Requerimiento Funcional	Es la especificación de una función o comportamiento que un sistema de información debe cumplir, describiendo de manera clara y detallada las acciones, procesos u operaciones que el software debe ejecutar para satisfacer las necesidades del usuario, del negocio o de la institución.
Requerimiento no funcional	Es la especificación de los criterios y atributos de calidad que determinan cómo debe operar un sistema de información, incluyendo aspectos como rendimiento, seguridad, disponibilidad, usabilidad, confiabilidad, escalabilidad y mantenibilidad, sin describir funcionalidades específicas del sistema.
Respaldo de sistemas de información	Es el procedimiento mediante el cual se realiza la copia de seguridad de los datos y sistemas de información en un medio o dispositivo alterno, con el propósito de garantizar su preservación y permitir la restauración total o parcial del sistema y de la información ante pérdidas, fallos, incidentes o contingencias.
Seguridad lógica	Conjunto de medidas, controles, políticas y procedimientos de carácter tecnológico y administrativo orientados a proteger los sistemas de información y los datos, mediante la restricción, control y monitoreo de accesos, garantizando que únicamente las personas y sistemas debidamente autorizados puedan acceder, modificar o utilizar la información.
Servicio en nube	Modelo de prestación de servicios tecnológicos que proporciona recursos de computación (como procesamiento, almacenamiento, bases de datos, redes, etc.), software, análisis de datos, entre otros, a través de Internet. Este modelo permite el acceso remoto a dichos recursos de manera escalable, flexible y bajo demanda, sin la necesidad de contar con infraestructura local o hardware propio.
Servidores institucionales	Son aquellas personas que, bajo cualquier modalidad, título o vínculo, desempeñan funciones, prestan servicios o ejercen cargos dentro del Gobierno Autónomo Descentralizado (GAD) del Distrito Metropolitano de Quito (DMQ), independientemente de su estatus laboral, ya sea permanente, transitorio o por contrato.

TÉRMINO	DEFINICIÓN
Servidor Municipal TIC	Servidor o servidora municipal que ejecuta, administra o apoya procesos relacionados con las Tecnologías de la Información y Comunicaciones (TIC) en las distintas áreas institucionales, independientemente de su modalidad de vinculación, tipo de nombramiento o relación contractual.
Sistemas de Información	Conjunto de sistemas de información automatizados integrados por componentes de hardware, software, datos, redes y procedimientos interrelacionados, que permiten la recopilación, procesamiento, almacenamiento, transmisión y gestión de la información, mediante la interacción con las personas, para apoyar las operaciones, la toma de decisiones y el cumplimiento de los objetivos institucionales.
Sistemas de información legados	Son aquellos sistemas de información heredados o denominados “legacy”, que han alcanzado el fin de su ciclo de vida tecnológico. Se caracterizan por no contar con mantenimiento oficial, soporte del proveedor ni actualizaciones periódicas, salvo desarrollos o ajustes locales realizados por equipos internos, lo que puede generar limitaciones en términos de seguridad, interoperabilidad, escalabilidad y continuidad operativa.
Software	Conjunto de programas, aplicaciones y sistemas operativos que permiten el funcionamiento, control y operación de los equipos informáticos, posibilitando la ejecución de tareas, el procesamiento de información y la interacción entre el usuario y el hardware.
Software libre	Tipo de software que garantiza a los usuarios las libertades de ejecutar el programa para cualquier propósito, estudiar su funcionamiento, copiarlo, distribuirlo y modificarlo, así como mejorar el código fuente y compartir dichas mejoras, promoviendo la transparencia, la colaboración y la inarea tecnológica.
Soporte 1er. Nivel	Servicio de asistencia técnica inicial orientado a la atención de incidencias y requerimientos básicos, en el cual el personal técnico recopila información sobre el problema reportado, realiza un diagnóstico preliminar y proporciona soluciones de primera instancia o canaliza el caso a niveles superiores de soporte cuando corresponda.
Tecnologías Digitales	Conjunto de Tecnologías de la Información y la Comunicación (TIC) que incluyen Internet, redes y dispositivos móviles, plataformas digitales y herramientas de analítica de datos, utilizadas para la generación, recopilación, intercambio, almacenamiento, procesamiento, análisis, acceso, búsqueda y

TÉRMINO	DEFINICIÓN
	presentación de información en formato digital, así como para el desarrollo e implementación de servicios y aplicaciones orientadas al fortalecimiento del gobierno digital.
TI	Tecnología de Información.
TIC	Tecnologías de la Información y Comunicación.
Titular de datos personales	Persona natural cuyos datos personales son objeto de tratamiento
Transformación Digital	Proceso continuo y estratégico de adopción integral y multimodal de tecnologías digitales que transforma de manera sustantiva la forma en que las instituciones públicas y privadas conciben, planifican, diseñan, implementan y operan sus servicios y procesos, con el objetivo de incrementar la eficiencia, seguridad, confiabilidad, agilidad y calidad de los servicios, optimizar costos y fortalecer la transparencia, trazabilidad y rendición de cuentas del Estado en su relación con la ciudadanía.
Tratamiento	Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea mediante procedimientos automatizados o manuales, que comprenden, entre otras, la recogida, obtención, registro, institución, estructuración, conservación, custodia, adaptación, modificación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, así como la habilitación de acceso, cotejo, interconexión, limitación, supresión, eliminación, destrucción y, en general, cualquier forma de uso de los datos personales.
Usuario	Persona natural que accede a los servicios de la municipalidad o utiliza un sistema informático institucional, lo que implica su adhesión plena e incondicional a las presentes políticas. En consecuencia, es responsabilidad del usuario conocer y revisar previamente dichas políticas, así como las modificaciones que estas pudieran incorporar, aceptando su cumplimiento y sujeción a las mismas.
Veracidad de la información	Principio que garantiza que la información ingresada por el usuario funcional o por el dueño de los sistemas de información sea correcta, fidedigna, completa y corresponda a la realidad, constituyéndose en un elemento esencial para la confiabilidad, legalidad y adecuado uso de los sistemas de información institucionales.

4. POLÍTICAS DE GOBIERNO DIGITAL Y TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

4.1. OBJETIVO, ÁMBITO DE APLICACIÓN Y GENERALIDADES

4.1.1. Objetivo. -

Las Políticas de Gestión Interna de Tecnologías de la Información y Comunicación tienen como propósito regular y unificar los procedimientos tecnológicos dentro del Consejo de Protección de Derechos del Distrito Metropolitano de Quito. El fin es asegurar la calidad en la prestación de productos a la ciudadanía, promoviendo una administración más eficiente y accesible.

4.1.2. Ámbito de aplicación. -

Las Políticas de Gestión Interna de Tecnologías de la Información y Comunicación son de obligatorio cumplimiento para los funcionarios del CPD-DMQ.

4.1.3. Generalidades. -

4.1.3.1. De la gestión de proyectos. -

Las áreas del CPD-DMQ que requieran gestionar proyectos concernientes a gobierno digital y de tecnologías de la información y comunicaciones, previo a ser aprobada la proforma presupuestaria, deberán remitir la documentación técnica de los mismos a la Gestión de Planificación para su revisión, quien contará con el asesoramiento técnico de la GITIC para la inclusión de las propuestas de proyectos en la proforma presupuestaria.

4.1.3.2. De las adquisiciones, desarrollos y cambios a los Sistemas de Información. -

Las áreas del CPD-DMQ requirentes deberán actuar en función de las políticas establecidas en el presente documento, así como, los lineamientos emitidos para el efecto.

4.1.3.3. De las adquisiciones de bienes y/o contratación de servicios tecnológicos. -

Las áreas del CPD-DMQ serán responsables de generar sus procesos para la adquisición de bienes y/o contratación de servicios tecnológicos de acuerdo con sus necesidades.

Las áreas del CPD-DMQ que requieran adquirir infraestructura tecnológica de usuario final, deberán considerar en su presupuesto la inclusión de sus necesidades.

En caso de que se identifique la necesidad de adquisición de bienes y/o contratación de servicios tecnológicos de interés común entre las distintas áreas del CPD-DMQ, se optará por generar compras por parte de la GITIC con el objeto de conseguir mejores condiciones de contratación y aprovechar economías de escala, las cuales se ejecutarán bajo los lineamientos emitidos para el efecto.

En caso de que las GITIC identifique la necesidad de adquisición de bienes y/o contratación de servicios tecnológicos de interés común entre las distintas áreas del CPD-DMQ, optará por generar compras globales.

4.1.3.4. Cumplimiento. -

El CPD-DMQ cuenta con la Gestión Interna de Tecnologías de la Información y Comunicación, la cual deberá dar estricto cumplimiento a la normativa vigente, especialmente a lo dispuesto en la Norma 410 "Tecnología de la Información" de las Normas de Control Interno para las Entidades y Organismos del Sector Público y para las Personas Jurídicas de Derecho Privado que dispongan de Recursos Públicos. El cumplimiento de esta normativa será de su responsabilidad, dentro del ámbito de sus competencias.

4.1.3.5. Excepciones. -

La GITIC tiene la responsabilidad de custodiar los diferentes sistemas de información y la infraestructura tecnológica del CPD-DMQ.

1. Por excepción, en casos debidamente justificados y coordinados con la GITIC, las distintas áreas podrán alojar su infraestructura tecnológica y sus sistemas de información en el cuarto de telecomunicaciones, siempre que cumplan con los requisitos normativos y lineamientos establecidos.

2. En caso de necesidad, si se requiere realizar la contratación de personal tecnológico con competencias en desarrollo de software o afines, para implementar sistemas de información, aplicaciones móviles y/o portales de gestión de información, previo a la mencionada contratación, deberán coordinar los aspectos técnicos con la GITIC, con la finalidad de asegurar el cumplimiento de las políticas de TIC y sus lineamientos.

4.2. OBLIGACIONES RESPECTO AL USO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Con el fin de garantizar el adecuado uso de las tecnologías de la información y comunicación, deberán observarse las siguientes obligaciones:

4.2.1. De la GITIC. –

1. Expedir los lineamientos para la aplicación de las presentes políticas, de obligatoria aplicación para el CPD-DMQ.

2. Emitir los informes de factibilidad técnica para las áreas del CPD-DMQ, conforme los lineamientos emitidos para el efecto.

4.2.2. De los funcionarios / servidores institucionales / trabajadores institucionales del CPD-DMQ. –

1. Cumplir las políticas, normativas, reglamentos, lineamientos, procesos y/o procedimientos definidos por la GITIC.

2. Utilizar las herramientas tecnológicas institucionales únicamente para el cumplimiento de sus labores.

3. Requerir el mantenimiento preventivo y/o correctivo del equipamiento TIC del CPD-DMQ. El mantenimiento con y/o sin vigencia tecnológica, será ejecutado únicamente por el personal técnico autorizado de manera formal.

4. Solicitar la autorización a los funcionarios/as de GITIC para la instalación de un software o aplicación para llevar a cabo sus actividades laborales y éste a su vez procederá conforme los lineamientos emitidos por la GITIC en este ámbito. Se prohíbe instalar cualquier tipo de software con o sin licencia en los dispositivos conectados a la red institucional.

4.2.3. Del Funcionario/a Institucional de GITIC

1. Realizar las actividades de soporte técnico, mantenimiento y cambios de configuración en el equipamiento TIC de propiedad del CPD-DMQ, de conformidad con los lineamientos definidos por la GITIC. Son los únicos autorizados para el efecto.

2. Mantener un inventario actualizado de los recursos informáticos conforme los lineamientos de la GITIC.

3. Realizar la instalación, desinstalación, actualización o modificación de sistemas de información o cualquier otro software que se requiera para el desarrollo de las actividades oficiales de la institución; además proporcionar soporte técnico del mismo en el equipamiento TIC.

4. Autorizar a la arrendataria, previa coordinación con la GITIC, la ejecución de labores de mantenimiento preventivo o correctivo en los equipos TIC que se encuentren bajo la figura de arrendamiento, siendo la instancia competente para otorgar dicha autorización en los casos de equipamiento TIC arrendado.

5. Verificar que los computadores del CPD-DMQ cuenten exclusivamente con la versión del software de antivirus institucional determinada por la GITIC.

6. Proceder conforme los lineamientos establecidos por la GITIC para que los usuarios puedan tener acceso a la red privada o alguna en específica del CPD-DMQ.

7. Atender los incidentes y requerimientos TIC asignados a través de mesa de ayuda de acuerdo con los lineamientos y/o procedimientos definidos por la GITIC.

8. Gestionar y verificar que los recursos informáticos cuenten con los accesos y medidas de control de seguridad física correspondientes.

4.2.4. De las de unidades / direcciones dueñas de los sistemas de información. –

1. Autorizar el acceso a sus bases de datos, sistemas de información y aplicativos. Son las únicas facultadas para el efecto.

2. Entregar o compartir los datos o información de sus sistemas, a los entes o entidades del GAD-DMQ y a personas naturales o jurídicas, previa solicitud, cumpliendo la normativa vigente. Son las únicas facultadas para el efecto. En el caso de datos personales, deberán cumplir con las disposiciones legales vigentes para su tratamiento y protección.

4.3. DE LA MÁXIMA AUTORIDAD DE LA DEPENDENCIA

4.3.1. Rol de la Máxima Autoridad de la Dependencia. –

Es la dueña de los sistemas de información y/o aplicativos, que tiene capacidad de toma de decisiones.

4.3.2. Responsabilidades. –

Son responsabilidades de la máxima autoridad de la Dependencia:

1. Autorizar y velar por la implementación de acciones para mitigar los riesgos que puedan afectar a la calidad de datos, así como también al funcionamiento normal de los sistemas de información, y las medidas preventivas y correctivas necesarias para mejorar la calidad de la información.

2. Proponer proyectos de gobierno digital y tecnologías de la información y comunicaciones, de los sistemas de información, a ser implementados en la institución, que estarán bajo la coordinación, gestión y control del administrador funcional correspondiente. Estos proyectos deberán ser coordinados con la GITIC, en calidad de asesor en el ámbito de sus competencias.

3. Solicitar el asesoramiento a la Gestión de Planificación para el levantamiento de procesos que sustentan el desarrollo de sistema de información y que deberán presentarse en el anteproyecto.

4. Designar al Administrador Funcional de cada uno de sus sistemas de información por primera vez, en caso de cese de funciones o reemplazo, y en ausencia temporal, designar al “suplente”; a fin de garantizar la continuidad en la gestión.

5. Comunicar a la GITIC, de manera formal (oficio/memorando) de la designación de un administrador funcional quien asumirá las responsabilidades descritas en estas políticas y en los lineamientos emitidos por la misma.

6. Solicitar formalmente (oficio/memorando) la creación, activación y/o desactivación del usuario Administrador Funcional y adjuntar el Acuerdo de Confidencialidad respectivo a la GITIC.

7. Solicitar y aprobar el correspondiente informe de fin de gestión del Administrador Funcional, en caso de cese de funciones o cambio; este informe deberá realizarse sobre todo el período de su actuación y estar debidamente sustentado con medios de verificación digitales y físicos.

8. Disponer de manera oficial al Administrador Funcional saliente que, en caso de ausencia temporal, cese de funciones o cambio de designación o roles, efectúe la transferencia de conocimiento al nuevo Administrador Funcional.

9. Implementar un canal/proceso especifico a través del cual los titulares de los datos personales puedan hacer efectivos sus derechos al acceso, eliminación, rectificación, actualización, cancelación, oposición, anulación y demás establecidos en la Ley Orgánica de Protección de Datos Personales y otras leyes o normativa conexa, en coordinación con el Administrador Funcional.

10. Coordinar con la GITIC, con base a las necesidades de la área o dirección, el dimensionamiento y disponibilidad de recursos financieros, humanos, infraestructura tecnológica y servicios; en caso de existir variaciones de la demanda del servicio, o la necesidad de implementar nuevos proyectos institucionales.

4.3.2.1 Gestión Funcional. –

1. Remitir a la GITIC, en los formatos dispuestos y requeridos, definiciones y/o requerimientos funcionales de los sistemas de información y/o aplicativos propuestos por el Administrador Funcional debidamente suscritos.

2. Emitir y socializar lineamientos, directrices y procedimientos necesarios y sustentados en la norma, a fin de que los sistemas de información y/o aplicativos generen la información de manera correcta, confiable y actualizada.

3. Promover la capacitación en el uso de los sistemas de información y/o aplicativos, conforme al ámbito de su gestión.

4. Promover la aplicación de acciones preventivas y correctivas para la gestión de riesgos que puedan afectar a la calidad de datos y/o el funcionamiento normal de los sistemas de información y/o el aplicativo y su disponibilidad.

4.3.2.2. Gestión no funcional. –

Remitir a la GITIC en los formatos requeridos, definiciones y/o requerimientos no funcionales de los sistemas de información y/o aplicativos propuestos por el Administrador Funcional.

4.3.2.3. Gestión de datos. –

1. Establecer instrumentos normativos como: estrategias, procedimientos, lineamientos o cualquier otro, para asegurar que el usuario final del sistema de información y/o aplicativo, acceda, registre y use la información de manera correcta, procurando que la misma sea completa, confiable y actualizada, con el fin de mejorar la calidad de datos.

2. Coordinar, proporcionar y autorizar la entrega de información de los sistemas de información y/o aplicativos de su propiedad, en atención a las solicitudes de las instituciones de control, áreas internas y externas, además de personas naturales o jurídicas; cumpliendo el marco normativo.

3. Autorizar el acceso del uso interno y externo de la información de los sistemas y/o aplicativos, bajo su competencia.

4.3.2.4. Gestión de contingencia y disponibilidad. –

1. Disponer la planificación, ejecución, pruebas y evaluación de los procedimientos de operación bajo modalidades de contingencia, con el objeto de precautelar la continuidad de los servicios a los usuarios finales y ciudadanía. Una vez superadas las condiciones de contingencia que impedían el normal funcionamiento del sistema de información y/o aplicativo, coordinará con la GITIC la recuperación de servicios y disponibilidad de la información.

2. Coordinar las estrategias de socialización de los procedimientos de utilización de los sistemas de información y/o aplicativos, en condiciones normales y bajo modalidad de contingencia, a usuarios internos y externos, en el CPD-DMQ de acuerdo con su competencia.

3. Solicitar y/o autorizar la suspensión temporal de los sistemas de información, aplicativos o servicios en producción, requeridos para la ejecución de procesos de mantenimiento

preventivo y correctivo planificados, en coordinación con la GITIC cuya socialización se realizará a través de los canales de comunicación establecidos para el efecto.

4.4. DEL DUEÑO DE LOS SISTEMAS DE INFORMACIÓN

4.4.1. Rol del Dueño de los Sistemas de Información. –

Es la dependencia requirente, administradora de los sistemas de información y/o aplicativos representada por su máxima autoridad y que forma parte de la Estructura Orgánica Funcional del Consejo de Protección de Derechos del Distrito Metropolitano de Quito.

Es responsable de los activos de información, definir su clasificación y derechos de acceso de los usuarios; así como de velar por el correcto funcionamiento del sistema de información / aplicativo / módulo, en el ámbito de sus competencias.

Las áreas de la institución que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo y responderán por la veracidad, autenticidad; y, su custodia y debida conservación de los registros en coordinación con la GITIC.

La responsabilidad sobre la veracidad y autenticidad de los datos suministrados al CPD-DMQ u otra institución con las que se interopera, es exclusiva de la o el declarante cuando provee toda la información; y su registro es responsabilidad del usuario que ingresa la información al sistema y/o aplicativo.

4.4.2. Responsabilidades. –

Son responsabilidades del Dueño de los Sistemas de Información:

1. Comunicar formalmente a la GITIC el desuso de los sistemas, además debe considerar el impacto a los sistemas relacionados o que se integran con el mismo.

2. Atender las comunicaciones de la GITIC respecto a los riesgos tecnológicos y generar las acciones respectivas dentro de sus competencias, para contrarrestarlos o minimizarlos.

4.5. DEL ADMINISTRADOR FUNCIONAL

4.5.1. Rol del Administrador Funcional. –

Cada uno de los sistemas de información y/o aplicativos de la institución, contarán con un Administrador Funcional del área dueña de los sistemas de información quien reportará a su máxima autoridad de la Dependencia, inconsistencias, novedades y otros aspectos relevantes respecto de su funcionamiento, gestión, operatividad, proyecciones de crecimiento de la demanda, entre otros.

El Administrador Funcional debe ser un funcionario, con conocimiento de los procesos relacionados, la normativa legal vigente y que garantice la adecuada administración y operatividad de los sistemas de información y/o aplicativos, implementados en la infraestructura tecnológica de la institución, en concordancia con los criterios emitidos en estas políticas.

4.5.2. Responsabilidades. –

Son responsabilidades del Administrador Funcional:

1. Proponer, de ser pertinente, proyectos tecnológicos, de sistemas de información y/o aplicativos (desarrollo interno o adquisición) a la máxima autoridad de la Dependencia. Deberá coordinar su elaboración conforme a las políticas y lineamientos de la GITIC; así como, demás normativa vigente para el efecto.

4.5.2.1. Gestión Funcional:

1. Administrar, capacitar, monitorear, controlar, depurar y dar seguimiento a la gestión funcional del sistema de información y/o aplicativo.

2. Administrar los usuarios y perfiles en el sistema de información y/o aplicativo, actividad que incluye la creación, actualización, depuración e inactivación; así como su control y registro periódico. Este proceso lo realizará en coordinación con la GITIC

3. Elaborar los requerimientos funcionales debidamente documentados, con detalle de especificidad, prioridad y criterios de aceptación; del sistema de información y/o aplicativo que administra, que deberán ser propuestos a la máxima autoridad de la Dependencia; procurando su mantenimiento evolutivo y correctivo, en cumplimiento de disposiciones expedidas y la normativa vigente. En caso de que el requerimiento funcional responda a la necesidad de otra área o área para la elaboración de los requerimientos funcionales, el Administrador funcional trabajará de manera coordinada con el solicitante.

   Una vez planteado el requerimiento deberá:

   a) Revisar y aceptar formalmente la propuesta técnica elaborada y remitida por la GITIC. En caso de que el requerimiento funcional responda a la necesidad de otra área, la revisión debe ser conjunta entre el solicitante y el Administrador funcional.

   b) Coordinar con la GITIC, el proceso de pruebas, validación y aprobación de la funcionalidad del sistema de información y/o aplicativo actualizado, con el fin de garantizar que se cumpla con los requerimientos del área requirente, en los tiempos establecidos.

c) Aprobar el paso a producción, sobre los cambios desarrollados y validados detallados en los requerimientos funcionales, conforme el régimen jurídico vigente para el efecto.

4. Proponer acciones preventivas y correctivas para la gestión de riesgos que puedan afectar a la calidad de datos y/o el funcionamiento normal del sistema de información y/o aplicativo y su disponibilidad.

5. Proponer a la máxima autoridad de la Dependencia, en lo que aplique, directrices, lineamientos y/o procedimientos motivados en la norma vigente, que permitan la operación normal del sistema de información y/o aplicativo; y, que promuevan la generación de información de manera correcta, confiable y actualizada.

6. Presentar a la máxima autoridad de la Dependencia, su informe de fin de gestión como Administrador Funcional, en caso de cese de funciones o cambio; este informe deberá realizarse sobre todo el período de su actuación y estar debidamente sustentado con medios de verificación digitales y físicos.

7. Validar la operación y funcionalidad del sistema de información y/o aplicativo, motivado de ser el caso, por disposiciones institucionales y/o cambios en la normativa legal vigente.

8. Reportar a la GITIC, mediante el canal y formatos establecidos, los incidentes del sistema de información y/o aplicativo, y hacer el seguimiento hasta que se realicen los correctivos necesarios solicitados.

9. Capacitar a los servidores de la institución en el uso de los sistemas y/o aplicativos que administra, para cumplir con la normativa legal, políticas, lineamientos y/o procedimientos vigentes, para la correcta operación funcional, tanto en condiciones normales como de contingencia.

10. Comunicar, difundir y coordinar las actualizaciones de los sistemas de información y aplicativos a los usuarios.

4.5.2.2. Gestión no Funcional:

1. Proponer a la máxima autoridad de la Dependencia, de acuerdo con las necesidades, las definiciones y/o requerimientos no funcionales del sistema y/o aplicativos en los formatos requeridos.

2. Realizar, en coordinación con la GITIC el levantamiento del respectivo requerimiento, con base a las necesidades de su área, su dimensionamiento y disponibilidad de recursos financieros, humanos, infraestructura tecnológica y servicios; en caso de existir variaciones de la demanda del servicio o la necesidad de implementar nuevos proyectos institucionales.

4.5.2.3. Gestión de Datos:

1. Coordinar y supervisar la ejecución de políticas, estrategias, procedimientos, lineamientos u otros instrumentos que promuevan la mejora de la calidad de la información de los sistemas y/o aplicativos, velando por su correcta funcionalidad y procurando la disponibilidad de información íntegra, actualizada y confiable, incluyendo procesos de depuración de base de datos.

2. Ejecutar periódicamente actividades de supervisión que promuevan la calidad de la información de los sistemas y/o aplicativos bajo su administración, velando por su correcta funcionalidad, procurando la disponibilidad de información íntegra, actualizada y confiable.

3. Diseñar estrategias para depurar la información, considerando lo establecido en las leyes, reglamentos y demás disposiciones expedidas que se deben observar conforme el régimen jurídico aplicable a su competencia.

4. Monitorear periódicamente la información mediante análisis de los registros que constan en el sistema y/o aplicativo con el objetivo de determinar inconsistencias en los datos registrados. Las novedades encontradas serán notificadas a la máxima autoridad de la Dependencia y se solicitará formalmente la remediación a la GITIC en el ámbito de sus competencias.

5. Preparar y poner a disposición la información, que previamente haya sido autorizada por la máxima autoridad de la Dependencia, en atención a las solicitudes realizadas por parte de las instituciones de control, internas y externas, y personas naturales o jurídicas respetando el marco normativo para el efecto.

6. Gestionar ante la máxima autoridad de la Dependencia, conforme el requerimiento correspondiente del solicitante, el acceso y uso interno y externo de la información de los sistemas y/o aplicativos, bajo su competencia de acuerdo con las necesidades y conforme al marco normativo vigente.

7. Proponer, de acuerdo con la necesidad de la institución, instrumentos normativos como: estrategias, procedimientos, lineamientos o cualquier otro; para asegurar que el usuario final del sistema de información y/o aplicativo, acceda, registre y use la información de manera correcta, procurando que la misma sea completa, confiable y actualizada, con el fin de mejorar la calidad de datos.

4.5.2.4. Gestión de contingencia y disponibilidad:

1. Poner a consideración de la máxima autoridad de la Dependencia, la propuesta del Plan de Contingencia sobre el normal funcionamiento del sistema de información y/o aplicativo, acorde a sus competencias y la normativa vigente. Una vez superadas las condiciones de

contingencia coordinará con la GITIC la recuperación de servicios y disponibilidad de la información.

2. Realizar la socialización de las políticas, lineamientos o procedimientos de utilización de los sistemas de información y/o aplicativos, en condiciones normales y bajo modalidad de contingencia, a usuarios internos y externos, en el CPD-DMQ de acuerdo con su competencia.

3. Coordinar con la GITIC, el tratamiento de incidentes de seguridad que se presenten en el sistema de información y/o aplicativo que administra.

4. Comunicar a la máxima autoridad de la Dependencia sobre la necesidad de la suspensión temporal de los sistemas de información, aplicativos o servicios en producción, para la ejecución de procesos de mantenimiento preventivo y correctivo planificados, en coordinación entre el Administrador Funcional y la GITIC y; viceversa, que propondrán la información a socializarse a través de los canales de comunicación establecidos para el efecto.

4.6. DEL CUSTODIO

4.6.1. Rol del Custodio. –

El Custodio de la información es aquel que, por la naturaleza de sus competencias y atribuciones, tiene la facultad de administrar, gestionar y resguardar o asegurar la integridad de las bases de datos. En el CPD-DMQ, estas competencias están asignadas a la GITIC, salvo los casos de excepción que por conveniencia de gestión autónoma como: empresas públicas, agencias metropolitanas y otras entidades; ejecuta los respaldos, gestiona el almacenamiento y coordina sus mecanismos de aseguramiento, conforme a los requerimientos del Administrador Funcional aprobados por la máxima autoridad de la Dependencia, dueña de los sistemas de información.

4.6.2. Responsabilidades. –

Son responsabilidades del Custodio:

1. Establecer el lineamiento o mecanismo para otorgamiento/revocación de accesos a la información.
2. Mantener la disponibilidad, integridad y confidencialidad de acceso a la información.

3. Gestionar, almacenar y respaldar la información con base al requerimiento del dueño de los sistemas de información y/o aplicativos, además generar los mecanismos de aseguramiento de la información custodiada.

4. Precautelar los accesos gestionados por el Administrador Funcional, hacia la información y funcionalidades del sistema de información y/o aplicativo.

5. POLÍTICAS PARA LA GESTIÓN DE GOBIERNO DIGITAL

5.1. DEL GOBIERNO DIGITAL

El gobierno digital comprende el uso estratégico de tecnologías digitales y datos dentro del Distrito Metropolitano de Quito, como parte de la estrategia de modernización del gobierno local para crear valor público.

5.2. POLÍTICAS DE GOBIERNO DIGITAL

Para la gestión del gobierno digital y ciudad inteligente se definen las siguientes políticas:

1. Las áreas del CPD-DMQ que ejecuten iniciativas relacionadas con Gobierno Digital, deberán identificar y determinar los indicadores y metas que aporten a la medición de los niveles de madurez y al cumplimiento de indicadores macros determinados en los diferentes instrumentos de planificación del CPD-DMQ.

2. Con la finalidad de asegurar un proceso continuo de adopción de tecnologías digitales, las áreas del CPD-DMQ que ejecuten iniciativas en temas relacionados con Gobierno Digital y Ciudades Inteligentes y Sostenibles remitirán a la GITIC la evidencia documental del cumplimiento de los indicadores de implementación, ejecución y gestión, al cierre de cada fase o hito del proyecto; así como de manera obligatoria al finalizar la iniciativa, a fin de garantizar el seguimiento y control oportuno de la información.

3. La GITIC, desarrollará evaluaciones del nivel de madurez de Ciudades Inteligentes y Sostenibles, para establecer estrategias de uso efectivo de las tecnologías digitales en el CPD-DMQ y mejorar la percepción de los servicios; esta evaluación se la realizará con la participación de todas las áreas involucradas.

4. La GITIC, fomentará y promoverá programas de competencias digitales para el talento humano del DMQ y que generen una base de conocimiento para la transformación digital.

6. POLÍTICAS DE LA CALIDAD DE LOS DATOS E INFORMACIÓN

6.1. DE LA CALIDAD DE LOS DATOS E INFORMACIÓN

La calidad de los datos permite medir el cumplimiento de los criterios de precisión, integridad, presentación, consistencia, exactitud, veracidad, completitud, validez y disponibilidad. El cumplimiento de estándares de calidad en los datos permite que la toma de decisiones basadas en estos, permitan cumplir con los objetivos trazados por el CPD-DMQ.

La veracidad de los datos y de la información ingresada en las bases de datos y/o de la información almacenada en aplicativos, será responsabilidad directa del titular de la información y la calidad de la información ingresada será responsabilidad del dueño de los sistemas de información.

6.2. INTEGRIDAD DE LOS DATOS E INFORMACIÓN

La GITIC velará que las bases de datos e información almacenada en equipos informáticos del Cuarto de Telecomunicaciones no sufran corrupción o alteración cuando se realice cualquier tipo de operación con los datos que afecten su integridad y/o disponibilidad. Entre las acciones previstas mantendrá respaldos de los datos y de la información para recuperarlos en caso de daños físicos u otros factores, cifrado de datos, controles de acceso, donde incluya la asignación de los privilegios de lectura/escritura.

6.3. RESPONSABILIDAD

Los dueños de los sistemas de información que actualmente o en el futuro administren y controlen bases o registros de datos públicos, son responsables de la integridad, protección, calidad, consistencia, exactitud, completitud, conservación, autenticidad y veracidad de los datos e información provista por los titulares de la información e ingresada en la base de datos y/o de la información almacenada en aplicativos, la misma que no debe estar errónea, desactualizada, equivocada o incompleta, en coordinación con la GITIC.

La responsabilidad sobre la veracidad y autenticidad de los datos suministrados al CPD-DMQ u otra institución con las que se interopera, es exclusiva de la o el declarante cuando provee toda la información; y su registro es responsabilidad del usuario que ingresa la información al sistema de información y/o aplicativo.

7. POLÍTICAS PARA LA GESTIÓN DE PROYECTOS E INNOVACIÓN DE TIC

7.1. DE LOS PROYECTOS E INNOVACIÓN DE TIC

La gestión de proyectos tecnológicos en el CPD-DMQ tiene el propósito de garantizar una ejecución desde una perspectiva sistémica que asegure que todos los proyectos relacionados con el uso de tecnología se alineen con las estrategias institucionales. Además, se impulsará la ejecución de proyectos de TIC innovadores que coordinen la participación de los diversos actores del ecosistema.

7.2 POLÍTICAS PARA LA GESTIÓN DE PROYECTOS E INNOVACIÓN DE TIC

Para la gestión de proyectos tecnológicos e iniciativas de innovación de gobierno digital y de tecnologías de la información y comunicaciones se definen las siguientes políticas:

1. Las áreas del CPD-DMQ que tengan necesidades de adquisición concernientes a gobierno digital y de tecnologías de la información y comunicaciones, deberán remitir la documentación a la GITIC para la emisión de la respectiva factibilidad técnica, conforme a los lineamientos emitidos por la misma. La validez de la favorabilidad del informe de factibilidad técnica se determinará en el lineamiento emitido por la GITIC.

2. Las áreas del CPD-DMQ que requieran realizar cambios y/o mantenimiento evolutivo de los sistemas de información existentes, deberán remitir de manera formal los requerimientos

funcionales a la GITIC y la misma proporcionará la respectiva propuesta técnica que deberá ser aceptada previo al inicio de la implementación.

3. Las áreas del CPD-DMQ, que requieran ejecutar proyectos relacionados a gobierno digital y tecnologías de la información y comunicaciones, deberán adoptar y aplicar la metodología para la gestión de proyectos de TIC, definida por la GITIC.

4. La GITIC, liderará propuestas de Innovación TIC, fomentando una cultura de innovación entre los diversos actores del ecosistema y generando nuevos conocimientos digitales para las diferentes áreas del CPD-DMQ.

5. La GITIC, coordinará de manera conjunta con las áreas del CPD-DMQ y demás participantes del ecosistema de innovación, las iniciativas de innovación en el ámbito de gobierno digital y tecnologías de la información y comunicaciones.

8. POLÍTICAS PARA LA GESTIÓN DE SISTEMAS DE INFORMACIÓN Y SERVICIOS TECNOLÓGICOS

8.1. DE LOS SISTEMAS DE INFORMACIÓN Y SERVICIOS TECNOLÓGICOS

Tiene como propósito gestionar los Sistemas de Información cumpliendo el ciclo de vida de software, así como brindar servicios tecnológicos para satisfacer las necesidades de los usuarios internos del CPD-DMQ.

8.2. POLÍTICAS PARA LA GESTIÓN DE SISTEMAS DE INFORMACIÓN

8.2.1. GENERALES. –

Para la gestión del ciclo de vida de los sistemas de información se definen las siguientes políticas:

1. Las áreas del CPD-DMQ, que requieran servicios referentes a sistemas de información, adoptarán y aplicarán la metodología del ciclo de vida de sistemas de información, mejores prácticas y estándares tecnológicos definidos en los lineamientos emitidos por la GITIC para el efecto.

2. Las GITIC, serán responsables de coordinar y gestionar el cumplimiento del ciclo de vida de los sistemas de información centralizados, descentralizados, adquiridos, donados y de servicios en la nube conforme los lineamientos establecidos, presentando un informe anual a la Dirección Administrativa Financiera.

3. Para la adquisición, desarrollo, donaciones y/o traspasos de sistemas de información, las áreas del CPD-DMQ deberán acogerse a los lineamientos de la GITIC correspondiente a la gestión de proyectos tecnológicos.

4. Las áreas del CPD-DMQ que posean sistemas de información propios y/o adquiridos, que se consideren legados y requieran sustituirlos, se considerarán nuevos proyectos y deben ejecutarse conforme a los lineamientos establecidos por la gestión de proyectos tecnológicos.

5. Los sistemas de información producto de adquisiciones, donaciones y/o desarrollos descentralizados de las diferentes áreas del CPD-DMQ, deberán ser entregados a la GITIC acorde a los lineamientos, para que sean considerados como parte del inventario institucional, y los mismos estén a disposición de las distintas áreas del CPD-DMQ. Todos los sistemas de información deberán cumplir con el ciclo de vida de desarrollo de software y con los lineamientos emitidos por la GITIC.

6. En el caso que exista donación de aplicaciones y/o sistemas de información, los cuales se entreguen por convenios, acuerdos, entre otros instrumentos; las áreas del CPD-DMQ deberán cumplir con la presente política y los lineamientos emitidos por la GITIC, especialmente en lo relacionado a desarrollo de software y/u otros instrumentos.

7. Las distintas áreas del CPD-DMQ que, requieran el desarrollo evolutivo de sus sistemas de información o nuevos desarrollos, deberán gestionar dichos desarrollos dentro de su propia estructura orgánica. Además, deberán cumplir con los lineamientos emitidos por la GITIC.

8. Las áreas del CPD-DMQ que posean desarrollos de software propios y/o adquiridos y que se estén ejecutando a la fecha, deberán informar a la GITIC sobre el proyecto de desarrollo de software que están realizando y deberán regularizar el proceso de conformidad a los lineamientos emitidos por la GITIC.

9. Las áreas del CPD-DMQ que posean desarrollos de software propios y/o adquiridos deberán presentar anualmente una hoja de ruta que permita evidenciar la evaluación de riesgo de sus aplicativos informáticos, los cuales serán considerados como sistemas informáticos legados de la institución. En caso de identificarse riesgos, se deberá elaborar un plan de migración a tecnologías de vanguardia, el cual será desarrollado de manera conjunta entre el área requirente y la GITIC, considerando los aspectos funcionales y técnicos, incluidos los procedimientos de migración de información y los riesgos asociados. Dicho plan deberá ser aprobado por la GITIC y ejecutado por las áreas involucradas en un plazo determinado y acordado conjuntamente.

10. Los códigos fuentes de los aplicativos y/o desarrollos de software que han sido entregados a las áreas institucionales, deberán ser alojados en el Cuarto de Comunicaciones de la institución en un repositorio general, con los respectivos ejecutables y documentación técnica pertinente, con la finalidad de compartir software entre las áreas institucionales y no generar duplicidad de intervenciones tecnológicas entre las mismas áreas del CPD-DMQ.

11. El código fuente generado de los sistemas de información desarrollados al interior del CPD-DMQ y/o adquiridos, pasará a ser propiedad intelectual de la institución, no deberá ser

divulgado, con el fin de resguardar la confidencialidad e integridad de la información y deberá cumplir con lo establecido en los lineamientos definidos por la GITIC para el efecto.

12. Las áreas del CPD-DMQ que requieran la contratación de servicios externos de desarrollo de sistemas deberán justificar y obtener autorización de la GITIC, en función de los lineamientos emitidos por la misma.

13. Los servidores y/o equipos institucionales TIC de las áreas del CPD-DMQ que desarrollen o sean parte de un equipo de desarrollo de sistemas de información, deberán suscribir un acuerdo de confidencialidad técnico (NDA), el mismo que asegurará que el servidor y/o equipo a futuro o posterior a su desvinculación de cualquier área institucional, no comercialice la información de los sistemas institucionales, propiedad del CPD-DMQ.

14. Las áreas del CPD-DMQ en el caso que requieran sistemas de información en la nube, deberán cumplir la normativa nacional vigente, la presente política y lineamientos establecidos por la GITIC.

15. Para el seguimiento y control de la calidad de los Sistemas de Información se implementará la Metodología de Aseguramiento de la Calidad de los Sistemas de información, la misma que, establecerá procesos y procedimientos que regulen el paso a producción de los sistemas de información, así como, las actualizaciones de estos.

8.2.2. CLASIFICACIÓN DE LOS SISTEMAS DE INFORMACIÓN. –

La clasificación de los sistemas de información permitirá una correcta aplicación de las presentes políticas y determinará los lineamientos a seguirse.

La clasificación es la detallada a continuación:

1. **Sistemas de información centralizados:** Son sistemas de información que por sus requerimientos especializados son desarrollados con los recursos propios de la GITIC.

2. **Sistemas de información descentralizados:** Son sistemas de información que están alojados o no en la GITIC, y que la institución posee personal informático que entre sus actividades tienen el desarrollo de sistemas de información.

3. **Sistemas de información adquiridos:** Son sistemas de información que son adquiridos o contratados a proveedores.

4. **Sistemas de información donados:** Son sistemas y/o aplicativos que, por convenios, acuerdos institucionales, entre otros instrumentos; son donados al CPD-DMQ.

8.2.3. APLICACIONES MÓVILES (APPS) Y AULAS VIRTUALES. –

Para garantizar la gestión segura y eficiente en la creación, uso y actualización de Apps, se definen las siguientes políticas:

1. Las áreas del CPD-DMQ deberán mantener las aplicaciones móviles y aulas virtuales con información actualizada y acorde a la normativa vigente, además deberán coordinar con la Gestión de Comunicación Social la disponibilidad, estructura jerárquica y ordenamiento y vigencia del contenido.

2. Las áreas del CPD-DMQ dueñas de los sistemas de información, aplicaciones móviles y aulas virtuales notificarán a la GITIC las que no se encuentren en uso, y éstas a su vez tomarán las acciones pertinentes y de ser necesario procederán a la baja del aplicativo.

3. Las áreas del CPD-DMQ que requieran el desarrollo, adquisición o servicio de aplicaciones móviles, deberán solicitar la aprobación técnica a la GITIC.

8.2.4. TIPOS DE ATENCIÓN PARA LOS SISTEMAS DE INFORMACIÓN

Se define los siguientes tipos de atención para los sistemas de información:

1. **Nuevos sistemas de información:** Solicitudes para nuevos sistemas de información por parte de las diferentes áreas del CPD-DMQ que requieren la implementación a través de un proyecto como se establece en estas políticas y en los lineamientos emitidas por la GITIC.

2. **Requerimientos para cambio:** Solicitudes de ampliación de funcionalidades, modificación, actualización, migración o cambios en los sistemas de información que se encuentran en producción.

3. **Mantenimiento:** Solicitudes de atención para atender incidentes relacionados a inconsistencias y fallas sobre los sistemas puestos en producción.

Según los tipos de servicios para los sistemas de información que se determine, se deberán acoger a los lineamientos específicos correspondientes y establecidas por la GITIC.

8.2.5. ENTORNO (AMBIENTE) DE TRABAJO. -

La GITIC ha definido los siguientes entornos (ambientes) para los procesos de desarrollo:

1. **Desarrollo:** Ambiente utilizado para la construcción de los sistemas de información y/o aplicaciones en donde los desarrolladores crean el código fuente y prueban las funcionalidades.

2. **Preproducción (pruebas):** Establecido como un ambiente similar al de producción, utilizado para el aseguramiento de la calidad y pruebas del sistema en el cual se pueden identificar y corregir errores en un ambiente controlado sin afectaciones a los usuarios.

3. **Producción:** Ambiente utilizado para la operación de los sistemas, donde los usuarios finales usan la aplicación.

Además, de estos ambientes utilizados para el desarrollo de sistemas de información, se establecen ambientes de apoyo (consultas, capacitaciones, entre otros) para las solicitudes y necesidades institucionales bajo análisis y justificación en cumplimiento con las políticas y lineamientos vigentes.

8.2.6. DERECHOS DE AUTOR. –

En los contratos realizados con terceros para desarrollo de software deberá constar que los derechos de autor serán de la institución y el contratista entregará el código fuente para actualización y mantenimiento. En la definición de los derechos de autor se aplicarán las disposiciones de la normativa que regula los derechos de propiedad intelectual.

Los derechos de autor del software desarrollado a la medida pertenecerán a la institución y serán registrados, conforme la normativa que regula los derechos de propiedad intelectual. Para el caso de software adquirido se obtendrá las respectivas licencias de uso. Dicho registro deberá ser remitido a la GITIC

8.3. POLÍTICAS PARA LA GESTIÓN DE LOS SERVICIOS TECNOLÓGICOS

8.3.1. POLÍTICAS DE USO DE SOFTWARE

8.3.1.1. Administración

En lo relacionado a la gestión del uso de software en equipamiento TIC del usuario final, se definen las siguientes políticas:

1. El Servidor institucional de TIC del CPD-DMQ será el responsable de la gestión del inventario, registro y control de las licencias de uso de sistemas de información y de cualquier otro software, conforme los lineamientos emitidos por la GITIC.

2. Para el uso de software o herramientas informáticas, se deberá contar con la respectiva licencia, suscripción o derecho de uso a nombre del CPD-DMQ.

No se deberá instalar sistemas de información y/o herramientas informáticas, adquiridos para uso personal del usuario (sin fines institucionales), a excepción de los autorizados por la GITIC.

8.3.1.2. De la instalación de Sistemas de Información:

Todo usuario que requiere la instalación de un determinado sistema de información en un computador institucional para sus actividades deberá solicitar la instalación a la GITIC o a los servidores institucionales de TIC, conforme al lineamiento establecido por la GITIC.

8.3.2. POLÍTICA GENERAL DE USO DE CORREO ELECTRÓNICO. -

8.3.2.1. Del Correo Electrónico:

El correo electrónico institucional es un recurso o servicio tecnológico proporcionado por el CPD-DMQ a sus funcionarios. Es una herramienta de comunicación, colaboración e intercambio de información oficial.

8.3.2.2 Tipos de Cuentas:

Se definen los siguientes tipos de cuentas de correo electrónico:

1. **Cuentas personales:** Lo funcionarios institucionales del CPD-DMQ, contarán con una cuenta de correo, en el servidor de la institución con capacidad de bandeja asignada, la dirección electrónica se conformará de acuerdo con lo señalado en los lineamientos para el efecto.

2. **Cuentas temporales:** Estas cuentas se crearán bajo propósitos específicos, que serán detallados en el campo de texto “notas” al momento de crearlas. Además, se especificará el tiempo de validez, para que sea borrada una vez que ya no se la necesite. El formato de este tipo de cuenta será: proposito@derechosquito.gob.ec

3. **Cuentas departamentales:** Estas cuentas serán creadas con el objetivo de comunicar a todos los miembros de una determinada dirección o lista de usuarios específicos. El formato de este tipo de cuenta será: nombredelarea@derechosquito.gob.ec

4. **Cuentas de servicios:** Estas cuentas están asociadas a los servicios que tiene implementado el CPD-DMQ para que se envíen comunicados hacia los usuarios de estos, el formato de este tipo de cuenta será: notificaciones.nombredelservicio@derechosquito.gob.ec.

8.3.2.3. Uso del servicio:

El uso del servicio de correo electrónico está sujeto a lo siguiente:

1. El acceso a este servicio, se lo realiza por medio del cliente de correo electrónico, intranet o de la página web institucional que la GITIC defina para el efecto.

2. Las comunicaciones institucionales efectuadas por correo electrónico solo podrán ser realizadas por las cuentas de correo institucionales.

3. Las cuentas de correo asignadas a los funcionarios institucionales deben utilizarse exclusivamente para actividades laborales relacionadas con los propósitos y funciones institucionales.

4. Los buzones de correo electrónico creados para los funcionarios institucionales, así como toda la información contenida en ellos, son propiedad exclusiva del CPD-DMQ.

5. La GITIC se reserva el derecho de modificar las condiciones de uso según sea necesario. También puede modificar o bloquear servicios relacionados con el correo electrónico por razones administrativas, de mantenimiento, de seguridad de TIC, fuerza mayor o necesidades institucionales.

6. La GITIC puede cancelar o desactivar la cuenta de cualquier usuario en cualquier momento sin previo aviso, incluso eliminarla por falta de uso o si se considera que el usuario ha infringido las reglas establecidas en los lineamientos definidos por la GITIC. Con la finalidad de resguardar la información de estas cuentas, los servidores institucionales TIC o la GITIC, coordinaran lo pertinente para generar los respaldos correspondientes. En tales casos, la GITIC no se hace responsable de la información ni de las posibles consecuencias de dicha cancelación o desactivación.

8.3.2.4. Responsabilidades:

Son responsabilidades para el uso de correos electrónicos:

1. Los servicios de correo electrónico serán administrados por la GITIC, que será responsable de garantizar el correcto funcionamiento y operación del servicio.

2. La Gestión Interna de Administración de Talento Humano comunicará de manera formal y en el término máximo de dos días a la GITIC sobre las entradas, vacaciones superiores a quince días laborales, movimientos y salidas de personal en la institución para la activación, modificación o desactivación correspondiente.

3. Los usuarios son los únicos responsables de todas las actividades realizadas desde su cuenta de correo.

4. La información transmitida a través del correo electrónico es responsabilidad exclusiva de cada usuario. El CPD-DMQ no es responsable de los contenidos y mensajes enviados a través de este servicio.

5. Las cuentas de correo son intransferibles y, por lo tanto, la información será responsabilidad exclusiva de cada usuario y no debe ser proporcionada a terceros.

6. La información recibida de manera personal y confidencial por correo electrónico no debe reenviarse a otras personas sin la autorización del remitente o propietario de la

información; además, se debe actuar conforme a los lineamientos emitidos por la GITIC para el efecto.

8.3.2.5. Gestión del buzón de correo:

Se establece lo siguiente:

1. Los usuarios son responsables de trasladar regularmente correos electrónicos a su archivo de almacenamiento local si está disponible, con el objetivo de evitar llenar el buzón de correo institucional.

2. La gestión de la información en las cuentas de correo electrónico debe ser adecuada. Se recomienda revisar periódicamente la bandeja de entrada y la capacidad disponible. Se deben eliminar los mensajes que no se deban conservar y archivar el resto en la carpeta o subcarpeta apropiada del archivo de almacenamiento local.

3. Se debe proteger la seguridad del buzón de correo evitando recibir o abrir correos de remitentes desconocidos, ya que en ocasiones pueden disponer de contenido potencialmente peligroso, como malware.

4. La GITIC determinará el espacio del buzón de correo electrónico de acuerdo con las necesidades laborales e institucionales y sus lineamientos.

5. El funcionario institucional será el responsable de generar un respaldo del buzón de correos, de acuerdo con los lineamientos emitidos por la GITIC.

8.3.2.6. Uso inaceptable:

Se considera mal uso o uso inaceptable del correo electrónico las siguientes actividades:

1. Utilizar el correo electrónico para actividades que no estén relacionadas con la institución.

2. Participar en la propagación de cadenas, esquemas piramidales y otros envíos similares con el correo institucional.

3. Enviar o reenviar mensajes con contenido difamatorio, ofensivo, racista, discriminatorio u obsceno.

4. Enviar mensajes anónimos o que afirmen títulos, cargos o funciones no oficiales.

5. Utilizar mecanismos y sistemas, que intenten ocultar o suplantar la identidad institucional del emisor del correo electrónico.

6. Distribuir mensajes con contenido inapropiado o perjudicial que atente contra la moral o las buenas costumbres, como apología al terrorismo, uso de programas piratas,

pornografía, amenazas, estafas, esquemas de enriquecimiento ilícito, lenguaje obsceno, malware u otro código malicioso.

7. Apropiarse de cuentas de correo electrónico diferentes a las asignadas.

8. Enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado “spam”.

9. Dirigir mensajes a un usuario o al sistema de correo electrónico con el propósito de paralizar el servicio al saturar la capacidad del servidor de correo o el espacio en disco del usuario.

8.3.3. POLÍTICA DE ENLACE DE DATOS, USO DE INTERNET E INTRANET, DOMINIOS Y SUBDOMINIOS. –

8.3.3.1. De los Enlaces de Datos, Uso de Internet e Intranet, Dominios y Subdominios:

Los servicios de Internet e Intranet que se brindan a través de los enlaces son recursos que la institución pone a disposición de los funcionarios institucionales, como herramientas de consulta de información, investigación y acceso a los sistemas institucionales, facilitando la realización de las labores institucionales. En cuanto a los dominios y subdominios institucionales, se definirá estructuras para un proceso ordenado y que los nombres se asocien a los institucionales.

8.3.3.2. Políticas:

Los enlaces, así como, el acceso y uso de los servicios de Internet e Intranet están condicionados a las siguientes políticas:

1. La administración y operatividad de los enlaces de datos, internet e intranet será responsabilidad de la GITIC.

2. El acceso a los enlaces de datos, internet e intranet deberán estar centralizados para asegurar la implementación de mecanismos de seguridad de acceso que permitan dar confiabilidad a los servicios de intercambio de información a través de ellos.

3. La implementación de nuevos enlaces o modificación de los existentes será responsabilidad de la GITIC, siendo esta quien debe establecer los convenios o contratos de servicios con los proveedores de servicios de telecomunicaciones.

4. En cuanto a la gestión y administración de los anchos de banda de los enlaces se procederá conforme los lineamientos emitidos por al GITIC.

5. El uso de servicio de Internet e Intranet está limitado a la realización de actividades laborales que estén relacionadas con los propósitos y funciones institucionales.

6. El acceso a internet será otorgado a los funcionarios institucionales y bajo la aprobación formal de la máxima autoridad de la Dependencia para tal efecto, se deberá proceder conforme lo señalado en los lineamientos emitidos por al GITIC.

7. Para los usuarios externos, ajenos a la institución, que requieran el acceso al servicio de internet, acceso a la red privada o una red específica se procederá conforme lo establecido en los lineamientos emitidos por la GITIC.

8. La información y mensajes que se envíen a través de internet, serán de completa responsabilidad del usuario emisor. En ningún momento dichos mensajes o el uso del internet podrán atentar contra la imagen y reputación del CPD-DMQ, de sus autoridades, funcionarios o servidores.

9. El usuario será el único responsable por los sitios web visitados desde su perfil de acceso a internet, por lo tanto, será también responsable de mantener en privado las credenciales de su cuenta.

10. Queda prohibido utilizar el internet como medio para realizar cualquier actividad comercial o lucrativa, acceso a sitios de juegos y actividades recreativas o de promoción de interés personal, tales como: chats, concursos entre otros.

11. Está prohibido acceder a sitios web que puedan ser percibidos como obscenos, que distribuyan, emitan o promocionen material pornográfico, material ofensivo o con humor inapropiado; que atente a la moral y buenas costumbres, entre otros.

12. También está prohibido transmitir amenazas, material indecente o de hostigamiento, así como, intimidar, insultar difamar, ofender, acosar a otras personas o interferir en el trabajo de otros usuarios.

13. Además, con el fin de precautelar el buen uso del internet e intranet se definen restricciones y/o prohibiciones operativas en los lineamientos emitidos por al GITIC.

8.3.3.3. Dominios y subdominios:

Con el fin de asegurar una gestión eficiente de los dominios y subdominios asociados con la infraestructura de TIC y con la finalidad de realizar un proceso de ordenamiento, asociado a los nombres de dominios y subdominios institucionales, las áreas del CPD-DMQ deberán cumplir con una estructura definida por la GITIC, de conformidad a los lineamientos respectivos.

8.3.4. POLÍTICA GENERAL PARA LA ADMINISTRACIÓN DE PORTALES WEB Y REDES SOCIALES. -

Para garantizar la gestión segura y eficiente en la construcción, uso y actualización de portales web se define las siguientes políticas:

1. Las áreas del CPD-DMQ que requieran construir y/o actualizar portales web, deberán solicitar a la Gestión de Comunicación Social el mapa del sitio para estructurar la información, y ésta a su vez, coordinará con la GITIC el desarrollo de las plantillas de diseño, el mismo que será estructurado en el siguiente orden de prioridad de construcción: CPD-DMQ, Secretaria Ejecutiva, Coordinación Técnica, Dirección Administrativa Financiera, Dirección de Asesoría Jurídica, Gestión de Comunicación Social, Gestión de Planificación.

2. La GITIC mediante informe técnico, notificará a las áreas del CPD-DMQ acerca de los portales web, que no se encuentren en uso, para que estas áreas tomen las acciones pertinentes y de ser necesario se proceda a la baja del aplicativo.

3. En lo que respecta a la administración de redes sociales, conforme el estatuto orgánico por procesos esta competencia le corresponde a la Gestión de Comunicación Social.

4. La Gestión de Comunicación Social, como ente rector de la comunicación institucional será la encargada de coordinar la documentación e información que se publique en el portal web institucional.

8.3.5. POLÍTICA GENERAL DE HERRAMIENTAS DE SOPORTE PARA LA MODALIDAD DE TELETRABAJO. -

Cuando las áreas del CPD-DMQ ejecuten proyectos relacionados a la modalidad de teletrabajo, las mismas deberán acogerse a los lineamientos emitidos por la GITIC en lo que respecta a las herramientas que se deben implementar para garantizar el acceso seguro y solo a las aplicaciones y recursos necesarios para llevar a cabo su trabajo, dependiendo del perfil de cada usuario.

9. POLÍTICAS PARA LA GESTIÓN DE SEGURIDAD DE TIC

9.1. DE LA SEGURIDAD DE TIC

Comprende la gestión de la seguridad de los sistemas de información, aplicaciones y usuarios; administrando los recursos tecnológicos de seguridad para precautelar la operación de los sistemas de información y aplicaciones de las áreas del CPD-DMQ.

9.2. POLÍTICAS GENERALES

9.2.1. GENERALES. -

Para la gestión de seguridad de TIC se definen las siguientes políticas:

1. La Seguridad de la Información estará liderada por la máxima autoridad de la Dependencia del CPD-DMQ, quien desempeña un papel fundamental para la adopción de los lineamientos a nivel de toda la institución, definirá la estructura, los roles y responsabilidades con respecto a la seguridad de la información, protección de datos personales y normativa relacionada.

2. Los usuarios internos de las áreas del CPD-DMQ deberán bloquear sus computadores si se alejan de su estación de trabajo por cualquier motivo.

3. La GITIC aplicará un protector de pantalla estándar en los computadores, de manera que se active después de un período de inactividad.

4. Los usuarios internos de las áreas del CPD-DMQ no deberán modificar las configuraciones de red, protectores de pantalla, configuración de software y/o configuraciones de hardware, en el caso que se requiera modificación de configuración, el único personal a cargo de dicha acción será el personal técnico autorizado por la GITIC.

5. Los usuarios internos de las áreas del CPD-DMQ son responsables de precautelar la seguridad de los computadores portátiles y/o todo en uno asignados, la Gestión Interna de Tecnologías de la Información y Comunicación (GITIC), evaluará la factibilidad de implementar mecanismos de seguridad física, como el uso de candados. De determinarse viable esta medida, la Dirección Administrativa Financiera gestionará la adquisición de dichos dispositivos.

6. Los usuarios internos de las áreas del CPD-DMQ para evitar pérdida de información, deberán respaldar su información periódicamente en los recursos que la GITIC le asigne para el efecto; conforme los lineamientos emitidos por la GITIC.

7. Los usuarios internos de las áreas del CPD-DMQ no deberán reubicar los equipos tecnológicos, sin autorización de la máxima autoridad de la Dependencia y bajo la supervisión del servidor institucional de TIC.

8. Los usuarios internos de las áreas del CPD-DMQ deberán utilizar únicamente versiones de software proporcionados por la institución conforme a los lineamientos emitidos por la GITIC.

9. Se prohíbe la explotación y/o escaneo de vulnerabilidades en los recursos tecnológicos a todos los servidores y trabajadores del CPD-DMQ, con excepción del personal autorizado por la GITIC; y en caso de que exista alguna sospecha o vulnerabilidad detectada, la misma debe ser comunicada de manera inmediata a la GITIC.

10. Los servidores institucionales de TIC de las áreas institucionales del CPD-DMQ serán responsables de la Seguridad de TIC de cada área asignada y deberán controlar la existencia de la documentación, la misma que debe contemplar su actualización y deberá estar relacionada con los procesos de comunicaciones, operaciones y sistemas.

11. Los servidores institucionales de TIC de las áreas institucionales del CPD-DMQ serán responsables de monitorear las necesidades de capacidad de los sistemas en operación y se deberá proyectar las futuras demandas de capacidad para mitigar y gestionar incidencias de seguridad de TIC.

12. Los servidores institucionales de TIC de las áreas institucionales del CPD-DMQ deberán cumplir los lineamientos emitidos por la GITIC para mitigar y gestionar incidentes de seguridad de TIC.

13. Los servidores institucionales TIC de las áreas institucionales del CPD-DMQ deberán mantener actualizados los sistemas operativos de acuerdo con los lineamientos emitidos por al GITIC.

14. Los usuarios de las áreas institucionales del CPD-DMQ serán los únicos responsables de la información y transmisión de esta en los computadores de la institución, para lo cual deberán cumplir con los lineamientos emitidos por la GITIC.

15. Los usuarios de las áreas institucionales del CPD-DMQ cumplirán con todas las regulaciones, políticas, lineamientos y procedimientos de uso de internet de la institución; no deberá conectarse a enlaces que no sean los oficiales de la institución y se prohíbe el acceso a cualquier fuente de información cuyo contenido no se encuentre relacionado con las actividades laborales dentro de los ámbitos de competencia del CPD-DMQ.

9.2.2. RESPONSABLES DE LA SEGURIDAD DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES (TIC). -

Se definen a los siguientes grupos como responsables de la Seguridad de TIC: el ente rector del Gobierno Digital y de las Tecnologías de la Información y Comunicaciones; los servidores institucionales de TIC que conforman el CPD-DMQ.

9.2.2.1. De la GITIC:

Actuará como responsable de la seguridad de TIC acorde a las funciones y competencias emitidas en el Estatuto Orgánico por Procesos; así como, al marco normativo vigente para el efecto.

9.2.2.2. De los servidores institucionales de TIC:

1. Responsables de la seguridad de TIC en la Dirección Administrativa Financiera en las cuales se encuentren prestando sus servicios profesionales.

2. Participar en la evaluación del impacto operativo de cambios previstos en el sistema y equipamiento.

3. Participar en la administración de medios técnicos para la segregación de ambientes de procesamiento.

4. Colaborar en el monitoreo de amenazas a sistemas informáticos, o cualquier otro software e infraestructura tecnológica.

5. Participar en la gestión de incidentes de seguridad de informática.

9.2.2.3 De las áreas institucionales:

1. Responsables de la seguridad y calidad de la información que se genera en sus áreas.

2. Participar en el monitoreo de amenazas a sistemas informáticos e infraestructura tecnológica.

3. Controlar la obtención de copias de respaldo de información y realizar pruebas periódicas de su restauración.

4. Utilizar los formatos definidos por la GITIC para el cumplimiento de procedimientos para mitigar incidentes de seguridad.
5. Elaborar el procedimiento para comunicar fallas en el procesamiento de los datos, información o sistema de comunicaciones, tomando medidas correctivas; y verificar su cumplimiento.

6. Implementar controles de seguridad definidos en las directrices de seguridad de TIC constantes en los lineamientos emitidos por la GITIC.

7. Implementar procedimientos para la administración de medios informáticos de almacenamiento y la eliminación segura de los mismos definidos en los lineamientos emitidos por la GITIC.

9.2.3 ACUERDO DE CONFIDENCIALIDAD. -

Los funcionarios, servidores y trabajadores institucionales deberán firmar los acuerdos de confidencialidad, de no divulgación de información de conformidad, entre otros, con lo dispuesto en la normativa vigente y las necesidades de protección de información de la institución.

La Gestión Interna de Administración de Talento Humano será la encargada de controlar que los acuerdos de confidencialidad de la información, documento físico o electrónico, sean firmados por el personal de la institución; gestionar la custodia de los acuerdos firmados, en los expedientes físico o electrónicos, de cada funcionario o servidor, y controlar que la firma de los acuerdos sean parte de los procedimientos de incorporación del nuevo personal a la institución, sin excepción.

El personal de otras instituciones públicas o privadas, que requieran ingresar a los equipos y/o los sistemas de información del CPD-DMQ, deberán suscribir un acuerdo de confidencialidad previo a la autorización para acceder a la información, el cual será gestionado por el área dueña de los sistemas de información o equipamiento.

9.2.4 CLASIFICACIÓN DE LA INFORMACIÓN. -

Para la clasificación de la información se establece lo siguiente:

1. Los activos de la información de la institución deberán ser clasificados en uno de los niveles definidos en el presente artículo, de conformidad con la normativa vigente y los lineamientos emitidos por la Gestión Interna de Tecnologías de la Información y Comunicación (GITIC) del CPD DMQ, en su calidad de órgano rector en materia de gestión y seguridad de la información. En este sentido, se establecen los siguientes niveles:

   Pública: Es la información que por su naturaleza puede ser visible o divulgada por todo el personal de la institución, usuarios o ciudadanía en general, sin riesgo de que su contenido pueda afectar en ningún sentido la integridad o financieramente a la institución.
   Esta información puede ser entre otras publicaciones, anuncios de prensa, páginas web de la institución.

   Sensible: La información sensible es la de uso solo interno destinada a uso exclusivo por parte de los funcionarios, servidores y trabajadores institucionales en el desarrollo rutinario de sus funciones, atribuciones, responsabilidades y roles. La divulgación y visibilidad de esta será dentro de la institución, la divulgación fuera de la misma puede tener un impacto leve o moderado a la privacidad e imagen del personal o a la institución. Esta información puede ser: oficios, memorandos, contratos, acuerdos entre otros.

   Confidencial: Es la información cuyo acceso se encuentra restringido de conformidad con la normativa vigente, incluyendo la Ley Orgánica de Transparencia y Acceso a la Información Pública y la Ley Orgánica de Protección de Datos Personales, cuya divulgación, acceso o tratamiento no autorizado podría ocasionar la vulneración de derechos de las personas o un daño grave a la institución.

   Esta información solo podrá ser conocida y gestionada por personal expresamente autorizado, conforme a los lineamientos definidos por la instancia competente en materia de seguridad de la información.

   Entre otros, se considera información confidencial: datos personales, especialmente datos sensibles; expedientes administrativos reservados; información financiera interna; credenciales de acceso a sistemas; y aquella que haya sido clasificada formalmente como tal conforme a la normativa aplicable.

2. Los dueños o responsables de la información deberán clasificar adecuadamente la información que manejan y deben asegurarse de que se respete el acceso a la misma por parte del personal a su cargo o un tercero.

3. Toda la información deberá ser etiquetada de forma clara, visible y uniforme, conforme a su nivel de clasificación: Pública, Sensible o Confidencial. Para garantizar la estandarización en su rotulación y etiquetado, se establecen los siguientes parámetros:

   - La etiqueta deberá ubicarse en un lugar visible del documento, preferentemente en el encabezado o pie de página; en el caso de archivos digitales, también deberá constar en el nombre del archivo.

- Se utilizarán de manera obligatoria las denominaciones estandarizadas: Pública, Sensible y Confidencial, sin variaciones.

- El formato de la etiqueta deberá incluir como mínimo: nivel de clasificación, fecha de emisión o actualización y área o responsable de la información.

- Se podrán emplear códigos de colores institucionales para cada nivel de clasificación, con el fin de facilitar su identificación (verde para Pública, amarillo para Sensible y rojo para Confidencial).

- La rotulación deberá mantenerse visible y sin alteraciones durante todo el ciclo de vida de la información.

- En el caso de información impresa, la etiqueta deberá constar en la portada o primera página; para información digital, deberá incluirse adicionalmente en los metadatos cuando sea aplicable.

4. Toda la información generada en la institución que no cuente con una clasificación específica será considerada de nivel PRIVADA, correspondiente a información de uso institucional no pública, cuya divulgación no está autorizada y que requiere manejo restringido dentro de la entidad.

9.3 CONDUCTA DEL USUARIO INTERNO

El usuario interno deberá cumplir con los siguientes lineamientos y responsabilidades en el uso de los recursos tecnológicos institucionales:

1. El usuario es el único responsable del contenido de las transmisiones realizadas a través de cualquier servicio institucional, debiendo garantizar que estas se efectúen bajo parámetros de confidencialidad, integridad y uso adecuado de la información, conforme a las políticas de seguridad de la institución.

2. El usuario deberá cumplir con la normativa legal vigente relacionada con la transmisión de datos, tanto en el país de origen como en el destino de la información, especialmente en el uso del correo electrónico institucional.

3. El usuario no deberá utilizar los servicios institucionales para fines ilegales o no autorizados.

4. El usuario deberá cumplir con todas las normativas, políticas y procedimientos institucionales relacionados con el uso de internet y de los recursos tecnológicos.

5. El usuario deberá mantener una comunicación respetuosa y profesional, evitando conductas abusivas y el uso de lenguaje inapropiado.

6. Se prohíbe el acceso a fuentes de información cuyo contenido no esté relacionado con las actividades laborales y los ámbitos de competencia del CPD-DMQ.

9.4 ACCESO A RECURSOS Y PRIVILEGIOS

Los usuarios deberán tener sólo los privilegios que son esenciales para acceder a los sistemas de información y aplicaciones para realizar las actividades diarias a su cargo; por defecto se cumplirá el principio de privilegio mínimo al configurar los perfiles de acceso a recursos y sistemas institucionales.

9.5 GESTIÓN DE INCIDENTES DE SEGURIDAD DE TIC

La gestión de incidentes de seguridad de TIC debe realizarse considerando los siguientes objetivos:

1. Responder rápida y efectivamente,
2. Contener y reparar el daño causado por los incidentes,
3. Prevenir daños futuros.

9.6 EXCEPCIONES DE SEGURIDAD

Para propósitos de mantenimiento y pruebas de seguridad de la red del CPD-DMQ, por excepción el personal debidamente autorizado, podrá estar exento de cumplir algunas de las restricciones anteriores, debido a las responsabilidades bajo su cargo o a eventos programados. Estos privilegios o autorizaciones de acceso deberán ser solicitados a la máxima autoridad de la Dependencia mediante oficio o memorando con la justificación respectiva.

9.7 POLÍTICA GENERAL DE MANEJO DE CONTRASEÑAS

9.7.1 ADMINISTRACIÓN. -

Para la administración de contraseñas se debe cumplir con las siguientes consideraciones:

1. Los funcionarios, servidores y trabajadores del CPD-DMQ contarán con un usuario y una contraseña que les permita identificarse de manera única para el acceso a los sistemas de información y servicios de red como correo electrónico, impresión, archivos compartidos, intranet e internet.

2. En aplicaciones o sistemas de información que admitan la autenticación multifactor, se debe implementar esta configuración para fortalecer la autenticación de los usuarios y control de acceso.

3. Al momento de crear contraseñas, estás deben cumplir requisitos mínimos de seguridad establecidos en los lineamientos emitidos por la GITIC. En estos mismos lineamientos se detallará la temporalidad de cambios de contraseñas y el procedimiento a seguir en caso de cambio, olvido, bloqueo y almacenamiento de contraseñas.

4. Las contraseñas son personales e intransferibles. Los usuarios son responsables de no compartir su contraseña con terceros. Toda actividad generada con el usuario/contraseña es de responsabilidad exclusiva del mismo.

5. En el caso de sistemas o aplicaciones no vinculados al Directorio Activo, se utilizarán contraseñas independientes. La autorización para crear usuarios en estos sistemas y gestionar contraseñas corresponde al administrador funcional cumpliendo con los parámetros de seguridad definidos en los lineamientos emitidos por la GITIC.

6. Cuando un usuario deje de pertenecer a la Institución, la Gestión Interna de Administración de Talento Humano notificará de inmediato la desactivación del usuario a la GITIC.

7. Si un usuario cambia de funciones dentro de la institución, la Gestión Interna de Administración de Talento Humano debe solicitar la modificación de permisos en la red y en los sistemas relacionados con su nuevo rol al área correspondiente.

8. La Gestión Interna de Administración de Talento Humano deberá solicitar a todos los funcionarios, servidores y trabajadores del CPD-DMQ la firma del compromiso de responsabilidad de seguridad y uso de usuario y contraseñas al iniciar su relación laboral con la institución.

9. Queda prohibido: compartir su contraseña de cualquier forma; escribir la contraseña o almacenarla en archivos sin cifrado, comunicarla en el texto de mensajes u otros medios electrónicos; comunicar las contraseñas en conversaciones electrónicas.

10. POLÍTICAS PARA LA GESTIÓN, ADQUISICIÓN Y SERVICIOS DE INFRAESTRUCTURA

10.1 GENERALES

Para la gestión de resguardo y contención de la información obtenida de los sistemas y/o aplicativos para la GITIC se definen las siguientes políticas:

1. La GITIC a través de la Dirección Administrativa Financiera será la encargada de brindar asesoría especializada para los proyectos de adquisición de infraestructura tecnológica, contratación de servicios en nube y servicios tecnológicos, acorde a los lineamientos emitidos por la GITIC.

2. Las áreas institucionales del CPD-DMQ que requieran adquirir sus sistemas de información con adopción de servicio en nube deberán regirse a los lineamientos emitidos por la GITIC.
3. Las áreas institucionales del CPD-DMQ que requieran gestionar procesos de reestructuración de obra civil que implique remodelación o cambio de sus instalaciones deberán contemplar dentro del presupuesto referencial la instalación de cableado estructurado y el equipamiento activo de red.

4. Las áreas institucionales del CPD-DMQ deben garantizar que el equipamiento activo de red, cableado estructurado y computadores se encuentren en buen estado, operativos y con vigencia tecnológica; con el fin de que la GITIC pueda proveer los servicios de acceso a internet, enlace de datos, correo electrónico, entre otros; de manera eficiente y eficaz. En el caso de que los equipos no reúnan las características antes descritas las áreas a la brevedad posible, deben realizar los respectivos procesos para la renovación del equipamiento antes mencionado.

5. Los servidores institucionales de TIC de CPD-DMQ, deberán elaborar informes anuales sobre las necesidades de incremento de capacidades, en los cuales se realice la evaluación de riesgos tecnológicos, costos y vida útil de los equipos para futuras actualizaciones; así como, deberán presentar un Plan a 4 años; para la adquisición de infraestructura y contratación de servicios tecnológicos; lo cual, deberá ser presentado al inicio de gestión de cada nueva administración.

6. Las áreas institucionales del CPD-DMQ no podrán contratar canales de comunicación de Datos e Internet de forma independiente y los mismos se canalizarán a través de la GITIC.

7. La GITIC será la encargada de asignar los recursos necesarios de almacenamiento para resguardar la información considerada como crítica de cada área institucional, de acuerdo con los lineamientos emitidos por la GITIC.

8. Los servidores institucionales de TIC serán los únicos responsables de custodiar la información que se encuentra respaldada y almacenada en los servidores de archivos, además los sitios en donde se almacenan las copias de respaldo deben ser físicamente seguros, con controles físicos y ambientales y de conformidad a los lineamientos emitidos por la GITIC.

9. Los funcionarios directivos y/o responsables de las áreas institucionales del CPD-DMQ, serán los encargados de llevar un control de los respaldos de los activos necesarios para mantener operativos los procesos correspondientes a su función, anticipándose a posibles eventos de pérdida de información.

10. Los servidores institucionales de TIC del CPD-DMQ deberán respaldar con mecanismos de encriptación la información que está catalogada como sensible, crítica y/o confidencial; de conformidad con lineamientos emitidos por la GITIC, además planificará los eventos regulares de verificación y restauración de los medios de respaldo para garantizar que sean confiables para uso en caso de emergencia o siniestro.

11. Los servidores institucionales de TIC del CPD-DMQ deberán supervisar a las áreas custodias de la información conforme a sus competencias, el cumplimiento con los periodos de permanencia de la información en función de su naturaleza con el fin de garantizar la

consulta histórica de la misma considerando lo establecido en la normativa de archivo vigente.

12. Los funcionarios, servidores y trabajadores institucionales de las áreas institucionales del CPD-DMQ, serán los responsables de la obtención de respaldo de la información contenida en el computador asignado (computadores de escritorios o portátiles) conforme lo establecido en los lineamientos emitidos por la GITIC.

13. Los funcionarios, servidores y trabajadores de las áreas institucionales del CPD-DMQ al finalizar su relación laboral con la institución, deberán entregar los respaldos de información de su equipo de cómputo a cargo y deberán entregar a su jefe inmediato superior, previo a la respectiva acta entrega recepción del puesto.

14. Los funcionarios, servidores y trabajadores de las áreas institucionales del CPD-DMQ serán los responsables de verificar que los respaldos generados se encuentren íntegros y disponibles en el caso de ser requeridos.

10.2 HARDWARE

El hardware de propiedad del CPD-DMQ se utilizará exclusivamente para actividades relacionadas con los objetivos y metas institucionales. En los casos en que se contemple el uso de equipos bajo la modalidad de arrendamiento, este deberá aplicarse de manera excepcional y debidamente justificada para ciertos tipos de hardware, para lo cual se observará lo siguiente:

1. La máxima autoridad o quienes tengan la competencia de cada área aprobará el cronograma de mantenimiento de sus equipos informáticos y los servidores institucionales de TIC serán los responsables de ejecutar el mismo, de acuerdo con los lineamientos emitidos por la GITIC.

2. En caso de mantenimientos preventivos, cada dependencia deberá contar con el presupuesto respectivo aprobado.

3. Cuando el hardware institucional sea afectado por algún siniestro (robo, extravío y/o daño físico), el responsable del bien debe comunicar formalmente a la Dirección Administrativa Financiera; además dar a conocer a la GITIC.

4. En caso que se requiera examinar los equipos informáticos y que no cuenten con garantía técnica vigente, el personal de la GITIC son los únicos autorizados para realizar estas actividades.

5. Cuando los equipos informáticos dispongan de garantía técnica vigente, los únicos autorizados para dar mantenimiento es el personal técnico calificado de la contratista, previa autorización del Administrador del Contrato.

10.3 DATA CENTER

En el Data Center principal del CPD-DMQ se alojarán los servidores, equipos de comunicaciones, soluciones de respaldo, sistemas y equipos de apoyo energético y ambiental necesarios para la operación de las actividades del CPD-DMQ; de manera general se debe cumplir con lo siguiente:

1. Los sistemas informáticos, base de datos y/o aplicativos desarrollados internamente o de propiedad del CPD-DMQ estarán bajo custodia de la GITIC y centralizados en el Data Center principal y/o en soluciones tecnológicas definidas por esta. En el caso de sistemas o aplicativos provistos por terceros, bajo modalidad de licenciamiento, suscripción o servicio, estos serán gestionados y administrados por la GITIC, conforme a las condiciones contractuales y técnicas establecidas.

Por excepción, previa justificación y autorización de la GITIC, las áreas institucionales podrán coordinar su alojamiento o implementación en sus dependencias, siempre que cumplan con los lineamientos emitidos para el efecto.

2. En el caso de sistemas de información y/o base de datos aisladas que no sean compatibles con la infraestructura tecnológica de la GITIC o de las soluciones alternas, las áreas a cargo de estos deben promover proyectos de integración y/o migración en coordinación con los lineamientos establecidos por la GITIC.

3. Se permitirá la construcción y/o repotenciación de centros de datos, adicionales a los existentes y/o soluciones alternas para alojamiento de información, concernientes a los recursos de cómputo.

4. Queda restringido el acceso físico y/o lógico a los centros de datos y equipamiento tecnológico de propiedad del CPD-DMQ, salvo aquel personal autorizado por la GITIC.

10.4 SEGREGACIÓN FUNCIONAL

Ningún proceso crítico debe ser conocido y ejecutado por una sola persona o que una misma persona tenga privilegios o accesos en diferentes fases de un proceso. Los distintos procesos del negocio deben ser claramente descritos.

10.5 RESPALDO DE LA INFORMACIÓN TECNOLÓGICA

La GITIC, así como las áreas institucionales del CPD-DMQ responsables de la información, según correspondan, determinarán el procedimiento de resguardo y contención de la información obtenida de los sistemas y/o aplicativos informáticos, considerando al menos los siguientes puntos:

1. Etiquetado de las copias de respaldo, contenido, periodicidad y retención.

2. Extensión (completo/diferencial) y la frecuencia de respaldos, de acuerdo con los requisitos de la institución.

3. Los medios de almacenamiento se utilizarán conforme a la vida útil recomendada por el proveedor. Una vez finalizado su ciclo de uso, se procederá a su baja y destrucción segura, previa autorización de la GITIC y en coordinación con la máxima autoridad de la Dependencia. Este proceso deberá realizarse bajo supervisión del responsable de activos tecnológicos y contemplará, según corresponda, el borrado seguro de la información mediante técnicas de sobrescritura certificada y/o la destrucción física del medio (trituración, desmagnetización u otro método técnico aprobado). Como evidencia del proceso, se deberá generar el acta correspondiente, debidamente suscrita por los responsables.

4. El resguardo de los respaldos de la información deberá realizarse en un sitio seguro que prevenga daños por intervención humana o desastres naturales. Para el efecto, los respaldos se almacenarán en un equipo NAS ubicado en el Data center ó cuarto de comunicaciones del CPD-DMQ, el cual deberá contar con controles de acceso restringido, condiciones ambientales adecuadas y medidas de seguridad física y lógica.

5. Adicionalmente, se recomienda implementar un esquema de respaldo complementario en servidores en la nube, que cuenten con mecanismos de seguridad como cifrado de la información, autenticación robusta y disponibilidad controlada, con el fin de garantizar la continuidad y recuperación de la información ante incidentes.

6. Grado apropiado de protección física y ambiental.

7. Eventos regulares de verificación y restauración de los medios de respaldo para garantizar sean confiables para uso de emergencia.

8. Protección de la información confidencial por medio de encriptación.

9. Generación de respaldos a discos duros y en el mismo sitio si se tiene suficientes recursos, ya que, en caso de mantenimientos de los sistemas de información, es más rápida su recuperación.

10.6 RETIRO DE ACCESOS

La GITIC retirará los accesos a los activos de información y a los servicios de procesamiento de información (tales como: sistema de directorio, correo electrónico, accesos físicos, aplicaciones de software, entre otros) inmediatamente luego de que se comunique formalmente a la GITIC la terminación de la relación laboral del funcionario, servidor o trabajador institucional por parte de la Gestión Interna de Administración de Talento Humano del CPD-DMQ.

Cuando el colaborador haga uso de vacaciones por un periodo de igual o superior a quince días laborables consecutivos, se deberá desactivar temporalmente sus accesos a los sistemas institucionales, como medida de seguridad de la información. La reactivación de dichos accesos

se realizará previa solicitud, mediante correo electrónico del jefe inmediato superior dirigido a la mesa de ayuda de la GITIC.

10.7 REGISTRO Y REVISIÓN DE TRANSACCIONES O LOGS

La máxima autoridad de la Dependencia y los servidores institucionales de TIC son los responsables del registro, revisión y conservación de las transacciones o logs de los sistemas de información y de las plataformas tecnológicas que administran directamente, de acuerdo con las leyes y normativa vigente. Para tal efecto, la GITIC, emitirá los lineamientos respectivos.

10.8 PROPIEDAD DE LA INFORMACIÓN

Los datos e información que se genere en los sistemas, aplicaciones y cualquier medio de procesamiento electrónico son de propiedad y responsabilidad del CPD-DMQ, por lo cual se debe considerar los siguientes parámetros.

1. Los derechos patrimoniales de un programa de computación o los generados a través de estos creados por uno o varios servidores y trabajadores institucionales en el desempeño de sus cargos corresponderán al CPD-DMQ.

2. La información que genere el servidor y trabajador institucional en su equipo tecnológico, en el ejercicio de sus funciones y competencias, es propiedad del CPD-DMQ y forma parte de su patrimonio documental.

3. Los respaldos que contengan información del CPD-DMQ, realizados o solicitados por el usuario del equipo tecnológico, se tendrán exclusivamente bajo resguardo; no se permitirá su distribución o publicación a terceros sin la debida autorización de su jefe inmediato superior.

4. Los servidores y trabajadores institucionales almacenarán en los computadores asignados la información de trabajo, o en su defecto en las carpetas compartidas institucionales.

5. Al finalizar su relación laboral con el área, los respaldos de la información del equipo de cómputo a cargo del usuario, incluyendo el respaldo de su correo electrónico, deberán ser entregados a su jefe inmediato superior, previo a la respectiva acta entrega recepción del puesto.

10.9 CONTINUIDAD, CONTINGENCIA, RECUPERACIÓN Y RETORNO A LA NORMALIDAD CON CONSIDERACIONES DE SEGURIDAD DE LA INFORMACIÓN

El CPD-DMQ se compromete a proveer los recursos necesarios para garantizar una respuesta efectiva de los funcionarios, servidores, trabajadores y los procesos ante situaciones de emergencia o desastres que puedan afectar la continuidad de sus operaciones. Se buscará restablecer las operaciones con el menor costo y pérdidas posibles, manteniendo una

comunicación adecuada con funcionarios, servidores, trabajadores, proveedores y otras partes interesadas, y asegurando la seguridad de la información de la institución.
En cuanto a la redundancia, se asegurará de contar con una plataforma tecnológica redundante que cumpla con los requerimientos de disponibilidad establecidos por la institución.

11. POLÍTICAS DE USO DE FIRMAS ELECTRÓNICAS

11.1 ÁMBITO

El uso de firmas electrónicas dentro del CPD-DMQ estará amparado en la normativa vigente relacionada para su aplicación.

11.2 EFECTOS DE LA FIRMA ELECTRÓNICA

La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio.

11.3 INSTRUMENTOS PÚBLICOS ELECTRÓNICOS

Se reconocerá la validez jurídica de los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmados electrónicamente. Dichos instrumentos públicos electrónicos deberán observar los requisitos, formalidades y solemnidades exigidos por la ley y demás normas aplicables.

11.4 DE LAS INFRACCIONES AL USO DE FIRMAS ELECTRÓNICAS

Los delitos o infracciones informáticas relacionada al uso de firmas electrónicas serán sancionadas acorde a lo establecido en las disposiciones legales vigentes para el efecto.

12. PROHIBICIONES PARA EL USO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Para el correcto uso de las Tecnologías de la Información y Comunicaciones, será prohibido:

1. Violar los derechos de cualquier persona o institución por derechos de autor, patentes, confidencialidad o cualquier otra forma de propiedad intelectual. Entre otras actividades, se incluye la distribución o instalación de software sin la licencia de uso adecuada adquirida por el CPD-DMQ.

2. Difundir información identificada como confidencial a través de cualquier medio que involucren el uso de la Tecnología de Información.

3. Introducir software malicioso (virus, gusanos, troyanos, spyware, ráfagas de correo electrónico, entre otros) en la red, computadores o servidores del CPD-DMQ o cualquiera de sus áreas adscritas.

4. Utilizar la infraestructura tecnológica para conseguir o transmitir material con ánimo de lucro.

5. Utilizar el sistema de comunicaciones del CPD-DMQ con el fin de realizar algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil.

6. Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios propios del CPD-DMQ.

7. Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios.

8. Monitorear puertos o realizar análisis de tráfico de la red con el propósito de evaluar vulnerabilidades de seguridad.

9. Burlar mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.
10. Interferir o negar el servicio a usuarios autorizados con el propósito de afectar la prestación o, deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (internet, intranet).

11. Usar comandos o programas de envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (intranet e internet).

12. Instalar cualquier tipo de software en los equipos de cómputo del CPD-DMQ sin la previa autorización de la GITIC y los servidores institucionales TIC de cada área.

13. Modificar la configuración del software antivirus, firewall o cualquier otro sistema de seguridad implementados en los equipos de cómputo del CPD-DMQ sin autorización previa de la GITIC y los servidores institucionales de TIC.

14. Compartir un repositorio de información sin restricciones de usuario. La GITIC puede cambiar permisos de recursos compartidos por los usuarios si detecta que éstos no cumplen con las mejores prácticas definidas.

15. Reproducir música de cualquier formato que no esté ubicada en el disco duro del computador del usuario o en algún otro medio de almacenamiento. No se permite la reproducción de archivos de música si éstos están ubicados en recursos compartidos de la red privada del CPD-DMQ o en cualquier URL de Internet (aplicable para los usuarios que hacen uso del servicio de internet).

16. Usar indebidamente la data e información institucional, por parte de las y los usuarios de los sistemas informáticos del CPD-DMQ.

13. SANCIONES

13.1 INCUMPLIMIENTO DE LAS POLÍTICAS

Ante el incumplimiento de las obligaciones contempladas en este instrumento y dependiendo de la gravedad de la infracción cometida, se iniciarán las respectivas acciones y procedimientos administrativos y judiciales, de conformidad a las normas que las regulan, a fin de que se determine la responsabilidad civil, administrativa y penal, a que haya lugar, en contra de los servidores responsables.

El CPD-DMQ podrá iniciar las acciones de oficio o a petición del jerárquico superior que solicite el inicio de las acciones, a través de los órganos judiciales o administrativos correspondientes.