

MEMORANDO Nro. EPMGDT-JS-2019-0168

Quito, 8 de Noviembre de 2019

PARA : Luis Ruales
GERENTE FINANCIERO ADMINISTRATIVO

DE : Karla Arellano
JEFE DE SISTEMAS

ASUNTO : Contestación Memorando No. EPMGDT-SRA-2019-014

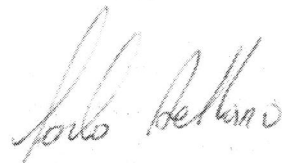
Dando contestación al memorando No. EPMGDT-SRA-2019-014, se remita las acciones ejecutadas en relación al cumplimiento de recomendaciones del Informe DNA5-0044-2019 que indica lo siguiente:

Dispondrá al Gerente Financiero Administrativo verifique que la Jefa de Sistemas elabore un plan informático estratégico y de contingencias el cual incluirá un análisis de la situación actual y las propuestas de mejora, para la recuperación de los sistemas oportunamente en caso de suspensión del servicio de los sistemas, diseñe e implemente políticas y procedimientos para realizar el mantenimiento y/o gestión de cambios de las aplicaciones, respaldar y recuperar redes, documentos que pondrá en conocimiento de la máxima autoridad para su aprobación y difusión a fin de que las acciones de esta área estén alineadas a los objetivos de la Empresa y la información que se genere sea confiable para la toma de decisiones y conocimiento del usuario externo.

Pongo en su conocimiento que se encuentra cumplida de acuerdo a la Resolución Administrativa N. EPMGDT-GG-LE-2019-490 emitida el 14 de junio de 2019, donde se encuentra aprobada los siguientes documentos:

- Plan Estratégico de Tecnología de Información 2019-2020
- Plan de Contingencia
- Políticas de Redes, Comunicaciones, Infraestructura y Seguridad Informática

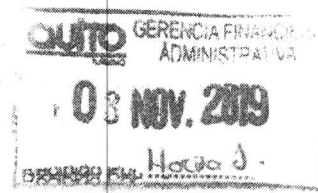
Particular que informo para los fines pertinentes.



Karla Arellano
JEFE DE SISTEMAS

Adjunto Resolución

ACCIÓN	NOMBRE	SUMILLA A	FECHA	SUMILLA
Elaborado por:	Karla Arellano	JS	08-11-2019	



RESOLUCIÓN ADMINISTRATIVA N° EPMGDT-GG -LE-2019-490

Leonidas Espinosa G.
GERENTE GENERAL, SUBROGANTE
EMPRESA PÚBLICA METROPOLITANA
DE GESTIÓN DE DESTINO TURÍSTICO -QUITO TURISMO-

Considerando:

- Que, el artículo 225 de la Constitución de la República prescribe que el sector público comprende, entre otros, a las personas jurídicas creadas por acto normativo de los gobiernos autónomos descentralizados para la prestación de servicios públicos;
- Que, el artículo 226 Ibídem prescribe: *"Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución."*
- Que, el artículo 227 de la Constitución de la República prescribe: *"La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación";*
- Que, el artículo 315 ibídem señala que el Estado constituirá empresas públicas para la gestión de sectores estratégicos, la prestación de servicios públicos, el aprovechamiento sustentable de recursos naturales o de bienes públicos y el desarrollo de otras actividades económicas;
- Que, el artículo 4 inciso primero de la Ley Orgánica de Empresas Públicas LOEP establece: *"...Las empresas públicas son entidades que pertenecen al Estado en los términos que establece la Constitución de la República, personas jurídicas de derecho público, con patrimonio propio, dotadas de autonomía presupuestaria, financiera, económica, administrativa y de gestión. Estarán destinadas a la gestión de sectores estratégicos, la prestación de servicios públicos, el aprovechamiento sustentable de recursos naturales o de bienes públicos y en general al desarrollo de actividades económicas que corresponden al Estado..."*;
- Que, el artículo 10 de la Ley Orgánica de Empresas Públicas determina que el Gerente General de la empresa ejercerá la representación legal, judicial y extrajudicial de la empresa y será en consecuencia el responsable de la gestión empresarial, administrativa, económica, financiera, comercial, técnica y operativa;
- Que, mediante la Ordenanza Metropolitana No. ORD- MET-2019-001 que expide el Código Municipal para el Distrito Metropolitano de Quito, de fecha 29 de marzo de 2019 en su Libro I.2, Título V de las Empresas Metropolitanas, Capítulo I del Régimen Común de las Empresas Públicas Metropolitanas, Sección III de la Administración de Empresas Públicas Metropolitanas, señala en su artículo I.2.84.- que: *"(...) El (la) Gerente(a) General ejerce la*

representación legal, judicial y extrajudicial, de su respectiva empresa y es responsable ante el Directorio por su gestión administrativa, técnica y financiera. El (la) Gerente(a) General está facultado para realizar todos los actos y contratos necesarios para el cumplimiento de los fines de la empresa a su cargo”;

- Que, el precitado Código a través del Capítulo VI de la Empresa Pública Metropolitana de Gestión de Destino Turístico artículo 1.2.131, dispone que la Empresa Pública Metropolitana de Gestión de Destino Turístico, es una persona jurídica de derecho público, sujeta a las disposiciones de la Ley Orgánica de Empresas Públicas;
- Que, en Sesión Ordinaria de Directorio de 08 de mayo de 2019, a través de la Resolución No. 003-05-2019, el Directorio de la Empresa Pública Metropolitana de Gestión de Destino Turístico resuelve: *“Designar por parte del Directorio, al Ingeniero Leonidas Espinosa Gallardo, actual Gerente Administrativo Financiero, como Gerente General Subrogante, a partir del 14 de mayo de 2019, hasta tanto el nuevo Directorio designe al nuevo Gerente General.”;*
- Que, mediante Acción de Personal No. 043-ISE-2019 de 13 de mayo de 2019, vigente a partir del 14 de los mismos mes y año, se designa como Gerente General de la Empresa Pública Metropolitana de Gestión de Destino Turístico Quito – Turismo, al señor Leonidas Espinosa G.;
- Que, el artículo 11 numerales 8 y 15 de la Ley Orgánica de Empresas Públicas establecen que la Gerente General podrá aprobar y modificar los reglamentos internos que requiera la empresa, excepto el señalado en el numeral 8 del artículo 9 de la Ley;
- Que, el artículo 77 literal e) de la Ley Orgánica de la Contraloría General del Estado, otorga atribuciones y obligaciones a las máximas autoridades de las instituciones del Estado, una de ellas la de: *“...e) Dictar los correspondientes reglamentos y demás normas secundarias necesarias para el eficiente, efectivo y económico funcionamiento de sus instituciones...”;*
- Que, las Normas de Control Interno para las entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que Dispongan de Recursos Públicos, en el Número se refiere a Tecnologías de Información en las entidades estatales, señalan la necesidad de contar con Planes Estratégicos de Tecnología de la Información, así como políticas y procedimientos respecto de la seguridad, infraestructura y mantenimiento informáticos;
- Que, es necesario establecer políticas internas que permitan establecer procesos claros de control, mantenimiento, soporte y seguridad informáticos, así como contar con un Plan Estratégico institucional que fortalezca la gestión de productos y servicios de TI;

En ejercicio de las competencias y funciones conferidas, y de conformidad con las disposiciones Constitucionales y normativa vigente,

RESUELVE:

Art. 1.- Aprobar los siguientes documentos que fueron debidamente elaborados por la Jefatura de Sistemas y Revisados por la Gerencia Administrativa Financiera, los mismos que forman parte integrante de la presente Resolución:

1. Plan Estratégico de Tecnología de Información 2019-2020;
2. Plan de Contingencia; y,
3. Políticas de Redes, Comunicaciones, Infraestructura y Seguridad Informática (contienen el procedimiento de Soporte y Mantenimiento Informático y la Bitácora de Infraestructura).

Art.2.- Disponer al personal de la Empresa Pública Metropolitana de Gestión de Destino Turístico – Quito Turismo, la aplicación inmediata de los documentos aprobados en el artículo primero de esta Resolución.

Art.3.- Encargar la aplicación, cumplimiento y difusión de la presente Resolución y de las disposiciones contenidas en los documentos enumerados en el artículo primero a la Gerencia Financiera Administrativa a través de la Jefatura de Sistemas.

Art.4.- La presente resolución entrará en vigencia a partir de su suscripción, y será publicada en la página web institucional.

DISPOSICIÓN TRANSITORIA ÚNICA.- Deróguense todas las normas de igual o menor jerarquía emitidas en Quito Turismo, que se opongan o no guarden conformidad con las disposiciones de las aprobadas en esta Resolución.

COMUNÍQUESE Y PUBLÍQUESE.- Quito, Distrito Metropolitano, 14 de junio de 2019.


Leonidas Espinosa G.
GERENTE GENERAL, SUBROGANTE
EMPRESA PÚBLICA METROPOLITANA
DE GESTIÓN DE DESTINO TURÍSTICO
-QUITO TURISMO-

Anexos: Plan Estratégico de Tecnología de Información 2019-2020; Plan de Contingencia; y, Políticas de Redes, Comunicaciones, Infraestructura y Seguridad Informática (contienen el procedimiento de Soporte y Mantenimiento Informático y la Bitácora de Infraestructura).

ACCIÓN	RESPONSABLE	SIGLA	FECHA	SUMILLA
Elaborado por:	A. Sierra	GJ	14-06-2019	
Aprobado por	J. Díaz	GJ	14-06-2019	
Aprobado por:	A. Lozano	GFA	14-06-2019	

Anexo No. 1

Plan Estratégico de Tecnología de Información 2019-2020; Plan de Contingencia; y, Políticas de Redes, Comunicaciones, Infraestructura y Seguridad Informática (contienen el procedimiento de Soporte y Mantenimiento Informático y la Bitácora de Infraestructura)

PLAN ESTRATÉGICO DE TECNOLOGÍA DE INFORMACIÓN 2019-2020

Mayo 2019

Elaborado por: Sistemas	Revisado por: Gerencia Financiera Administrativa	Aprobado por: Gerente General
Firma: Arellano K. Medina F.	Firma: Lozano A.	Firma:

	PLAN ESTRATÉGICO TECNOLOGÍA DE INFORMACIÓN 2019-2020	FECHA: 13-Mayo-2019
		Versión: 1.0

Indice

1	Considerando	3
2	Introducción	4
3	Objetivo	5
4	Ámbito de Aplicación	5
5	Responsables (o Participantes):	5
6	Desarrollo del Plan Estratégico de Tecnología de Información - PETI	5
6.1	Resumen de la metodología utilizada	¡Error! Marcador no definido.
6.2	Diagnóstico para el desarrollo del Plan Estratégico de TI	5
6.2.1	Gestión de Tecnologías de la Información y Comunicación	7
7	Desarrollo y Elaboración del Plan Estratégico de Tecnología de Información	10
7.1	Misión del área de Tecnología de Información	11
7.2	Visión del área de Tecnología de Información	11
7.3	Análisis FODA	12
7.4	Áreas de iniciativa estratégica	12
7.5	Objetivos estratégicos de Tecnología de Información	12
7.6	Estrategias por objetivo estratégico de TI	13
7.6.1	Objetivo 1: Mantener la estabilidad operativa de todos los recursos que provee TIC	13
7.6.2	Objetivo 2: Alcanzar el nivel requerido de satisfacción de usuarios de los productos y servicios de TIC	14
7.6.3	Objetivo 3: Realizar el desarrollo, mantenimiento y mejoras de los sistemas de información críticos	15
7.6.4	Objetivo 4: Implementar proyectos de innovación tecnológica en las unidades de Infraestructura, Desarrollo de Sistemas y Comunicaciones	15

	PLAN ESTRATÉGICO TECNOLOGÍA DE INFORMACIÓN 2019-2020	FECHA: 13-Mayo-2019 Versión: 1.0
---	---	--

PLAN ESTRATÉGICO DE TECNOLOGÍA DE INFORMACIÓN 2019-2020

1 Considerando

La elaboración del presente Plan estratégico de Tecnología de Información se sustenta en los siguientes considerandos:

Que, de acuerdo a las normas de control interno de la Contraloría General del Estado 410-03 Plan Informático Estratégico de Tecnología indica que; "la Unidad de Tecnología de la Información elaborará e implementará un Plan Informático Estratégico para administrar y dirigir todos los recursos tecnológicos, el mismo que estará alineado con el Plan Estratégico Institucional y éste con el Plan Nacional Desarrollo y las Políticas Públicas de Gobierno".

El Control Interno constituye un proceso integral aplicado a la máxima autoridad, la dirección y el personal de cada entidad. Constituyen componentes del control interno el ambiente de control, la evaluación de riesgos, las actividades de control, los sistemas de información y comunicación y el seguimiento.

El Control Interno está orientado a cumplir con el ordenamiento jurídico, técnico y administrativo, promover eficiencia y eficacia de las operaciones de la entidad y garantizar la confiabilidad y oportunidad de la información, así como la adopción de medidas oportunas para corregir las deficiencias de control.

Los objetivos y estrategias detalladas en el presente plan se encuentran orientados a cumplir con las directrices suscritas en las Normas de Control Interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, abarcando proyectos que toman en cuenta los tres ejes o áreas de trabajo (Infraestructura Tecnológica, Desarrollo de Software de Quito Turismo, teniendo en cuenta siempre como base la innovación tecnológica y la satisfacción del usuario final tanto interno como externo.

Las Normas de Control Interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos en las que se enfatiza en el presente plan son:

- Desarrollo y adquisición de software aplicativo (código ingenios aplicando software libre)
- Adquisición de Infraestructura Tecnológica
- Mantenimiento y control de la infraestructura tecnológica

	PLAN ESTRATÉGICO TECNOLOGÍA DE INFORMACIÓN 2019-2020	FECHA: 13-Mayo-2019
		Versión: 1.0

- Monitoreo y evaluación de los procesos y servicios

Se ha creído necesario efectuar una revisión de las definiciones estratégicas planteadas en este plan y realizar el desarrollo pertinente que le permitan a Quito Turismo proseguir con el desarrollo sostenido y contar con un Plan Estratégico de Tecnología de Información. Con este fin, durante el mes de abril se inició un proceso de creación del Plan Estratégico de Tecnología de Información, para proyectarlo al período que inicia en el 2019 y finaliza en el 2020.

En base a estas definiciones estratégicas, durante el mes de marzo de 2019 y con la participación de los funcionarios directamente involucrados en las estrategias definidas en el Plan Estratégico de Tecnología de Información, se desarrolló el Plan Operativo detallado que serviría de guía para el periodo 2019-2020.

2 Introducción

La Gerencia General de Quito Turismo, ha priorizado el componente tecnológico como un aspecto clave para el logro de los objetivos estratégicos de la Institución, los mismos que se orientan hacia una excelencia de la promoción de ciudad tanto nacional como internacional, asegurando transparencia, y fortaleciendo la imagen institucional, y su relación con la sociedad a través de la servicios eficientes y oportunos. La incorporación de tecnología en la ejecución de los procesos de la institución debe realizarse con base en los objetivos institucionales y con un enfoque de soporte efectivo a sus procesos.

El área de Sistemas ha realizado el proceso de formulación de su Plan Estratégico (PETI), el cual define el enfoque tecnológico para la Institución y la forma como este enfoque apoya a la consecución de los objetivos del Plan Estratégico de Quito Turismo. Para la elaboración de este plan, ha sido necesario realizar la revisión y análisis de la situación actual de Tecnología y de la Institución, tomando como referencia aspectos internos y externos desde el punto de vista operativo y tecnológico, su entorno específico y su entorno general; definir los componentes estratégicos de TI aplicables a la Institución.

Es importante resaltar que para el desarrollo del PETI, se recopiló información acerca del estado actual de la Institución y del área de Sistemas, información que sirvió como base para elaborar un diagnóstico de la situación actual; identificar fortalezas, debilidades, oportunidades, amenazas y requerimientos de información actuales y futuros, además de proporcionar la base de insumos necesaria para el desarrollo de las etapas de la formulación del PETI.

3 Objetivo

Fortalecer la gestión y generación de productos y servicios de TI.

4 Ámbito de Aplicación

El presente Plan Estratégico de Tecnología de Información (PETI) para el periodo 2019-2020, al encontrarse en concordancia a los objetivos estratégicos de Quito Turismo, marca la línea guía en la cual los diferentes funcionarios que forman parte del área de Sistemas deben orientar sus esfuerzos, acciones e iniciativas.

5 Responsables:

Para la ejecución del plan a través de:

- Todas los funcionarios de Sistema
 - Jefe de Sistemas
 - Especialista de Sistemas
 - Técnico de Sistemas

Para el seguimiento y monitoreo a través de:

- Gerente Financiero Administrativo
- Gerente General

6 Desarrollo del Plan Estratégico de Tecnología de Información - PET

En la siguiente sección se detalla la metodología y se hace referencia a los distintos componentes que forman parte de la misma.

6.1 Desarrollo del PETI

Para la elaboración del Plan Estratégico de Tecnología de Información conlleva la realización de etapas generales, que son:

1. Diagnóstico para el desarrollo del Plan Estratégico de TI
2. Desarrollo y elaboración del Plan Estratégico de Tecnología de Información

A continuación, se describe el detalle de cada una de estas etapas:

6.2 Diagnóstico para el desarrollo del Plan Estratégico de TI

En esta etapa también se estudió toda la documentación relacionada con el área de sistemas. Entre los documentos analizados se encuentra la estructura orgánica del área, funciones por cargo, estado de la infraestructura tecnológica, informes de Auditoría Informática, planes de acción, etc.

```

graph TD
    DIRECTORIO[DIRECTORIO] --> GERENCIA_GENERAL[GERENCIA GENERAL]
    GERENCIA_GENERAL --> GERENCIA_TECNICA[GERENCIA TÉCNICA]
    GERENCIA_GENERAL --> GERENCIA_FINANCIERA_ADMINISTRATIVA[GERENCIA FINANCIERA ADMINISTRATIVA]
    GERENCIA_GENERAL --> GERENCIA_COMUNICACION[DIRECCIÓN DE COMUNICACIÓN]
    GERENCIA_GENERAL --> DIRECCION_AGENCIA_ATRACCION_INVERSIONES[DIRECCIÓN DE AGENCIA DE ATRACCIÓN DE INVERSIONES]
    
    GERENCIA_TECNICA --> SECCION_INVESTIGACION_DESARROLLO[SECCIÓN DE INVESTIGACIÓN Y DESARROLLO]
    GERENCIA_TECNICA --> SECCION_ASORIA_1[SECCIÓN DE ASesorIA]
    GERENCIA_TECNICA --> SECCION_ASORIA_2[SECCIÓN DE ASesorIA]
    GERENCIA_TECNICA --> SECCION_ASORIA_3[SECCIÓN DE ASesorIA]
    GERENCIA_TECNICA --> SECCION_ASORIA_4[SECCIÓN DE ASesorIA]
    
    GERENCIA_FINANCIERA_ADMINISTRATIVA --> SECCION_ASORIA_5[SECCIÓN DE ASesorIA]
    GERENCIA_FINANCIERA_ADMINISTRATIVA --> SECCION_ASORIA_6[SECCIÓN DE ASesorIA]
    GERENCIA_FINANCIERA_ADMINISTRATIVA --> SECCION_ASORIA_7[SECCIÓN DE ASesorIA]
    GERENCIA_FINANCIERA_ADMINISTRATIVA --> SECCION_ASORIA_8[SECCIÓN DE ASesorIA]
    GERENCIA_FINANCIERA_ADMINISTRATIVA --> SECCION_ASORIA_9[SECCIÓN DE ASesorIA]
    
    GERENCIA_COMUNICACION --> SECCION_ASORIA_10[SECCIÓN DE ASesorIA]
  
```

6.2.1 Gestión de Tecnologías de la Información y Comunicación

6.2.1.1 Misión:

Asesorar y coordinar la gestión de los servicios de tecnologías de la información de la entidad, alineados al plan estratégico institucional y al cumplimiento del Plan Nacional de Gobierno Electrónico y las políticas y objetivos gubernamentales; de manera que garantice la disponibilidad, integridad y confiabilidad de la información institucional.

Atribuciones y Responsabilidades:

- a) Elaborar y gestionar la implementación del Plan Estratégico de Tecnologías de Información (PETI), plan operativo anual de TIC (POATIC), plan anual de compras de TIC (PACTIC) alineados al plan estratégico institucional.
- b) Administrar las metodologías y disponer estudios de factibilidad para la formulación, aprobación, ejecución y control del portafolio de proyectos de TIC propios o adquiridos, así como los recursos humanos, físicos, de infraestructura tecnológica y financiera; de modo que sean correctamente implementados y difundidos en la institución;
- c) Gestionar la aprobación para la ejecución de los proyectos de TIC y de Gobierno Electrónico
- d) Aprobar los términos de referencia y especificaciones técnicas requeridos, informes de administración y fiscalización de contratos de bienes y servicios relacionados con el área de TIC;
- e) Gestionar el esquema gubernamental de seguridad de la información en la institución, así como el ciclo de vida de las aplicaciones y sistemas informáticos para automatizar y mejorar los procesos internos y los servicios al ciudadano;
- f) Administrar el soporte técnico, promover el cambio y la renovación continua capacidad, disponibilidad y continuidad de los aplicativos, sistemas y servicios informáticos, de acuerdo a las políticas, análisis de requerimientos de implementación e implantación y prioridades emitidas por el PETI;
- g) Elaborar informes de gestión, rendición de cuentas, auditorías informáticas, acuerdos e indicadores de niveles de servicio y calidad a nivel interno y externo de los aplicativos, proyectos, sistemas y servicios informáticos de la institución;
- h) Elaborar manuales e informes técnicos relacionados a los procedimientos, instructivos, indicadores de medición que permitan la implementación, uso, aplicación, optimización, control, evaluación y requerimientos de cambio de los aplicativos, sistemas y servicios informáticos de la institución;
- i) Elaborar los diagramas de servicios de mantenimiento, mesa de ayuda, respaldos, infraestructura, seguridad informática; de igual manera los diagramas de red local y nacional e informe de cumplimiento de normativa y del Plan de Gobierno Electrónico;

- j) Observar y ejercer las atribuciones que competan a la unidad de conformidad a las disposiciones establecidas en la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento General de aplicación; y,
- k) Gestionar las demás atribuciones y responsabilidades que le sean asignadas por la autoridad competente.

Gestiones Internas:

- Gestión Interna de Proyectos TIC
- Gestión Interna de Infraestructura de TI
- Gestión Interna de Soporte a Usuarios
- Gestión Interna de Seguridad Informática, Interoperabilidad y Riesgos

Productos y Servicios:**Gestión Interna de Proyectos TIC**

1. Arquitectura tecnológica de TI con características de escalabilidad y flexibilidad que permitan la reducción de tiempos de atención en las soluciones, procesos, y proyectos de TI.
2. Portafolio de desarrollo de soluciones tecnológicas propias, adquiridas y adaptadas, proceso y proyectos informáticos gestionados y administrados por TIC, así como los estándares de programación relacionados con el ciclo de vida de desarrollo o gestión de cambio de nuevas aplicaciones y sistemas informáticos.
3. Repositorios e inventarios de códigos fuente versionados, scripts de base de datos versionados, instaladores, archivos de configuración y parametrización, reportes de control de cambio y versiones del desarrollo de los aplicativos y sistemas informáticos desarrollados, adquiridos o adaptados.
4. Términos de referencia, especificaciones funcionales y técnicas para la contratación del desarrollo de sistemas informáticos, servicios, servicios web, consultorías y demás contrataciones requeridas por la coordinación en base a la normativa legal vigente para este fin.
5. Servicios Web y documentación relacionada para compartir e intercambiar datos e información electrónicos.
6. Informes de gestión de paso a producción de los sistemas informáticos desarrollados, proyectos informáticos y seguimiento y control de incidentes de las aplicaciones, sistemas informáticos desarrollados, adquiridos o adoptados.
7. Informes de administración, transferencia de conocimiento y fiscalización de sistemas informáticos, servicios web, consultorías y contratos requeridos por la institución.

Gestión Interna de Infraestructura de TI

1. Planes de aseguramiento y disponibilidad de infraestructura tecnológica que incluye la instalación, configuración y administración de hardware, middleware, recursos tecnológicos requeridos para el

	PLAN ESTRATÉGICO TECNOLOGÍA DE INFORMACIÓN 2019-2020	FECHA: 13-Mayo-2019 Versión: 1.0
---	---	--

2. Manuales, procedimientos y estándares de operación y monitoreo de equipos redes, bases de datos, servidores de aplicaciones web, balanceadores de carga.
3. Diagramas de aplicaciones y arquitecturas de servidores, redes LAN/WAN/WIRELESS, interconexión, almacenamiento, respaldo y recuperación centralización y virtualización.
4. Planes de acción y mejoras en la infraestructura, aplicaciones y soporte de los servicios tecnológicos, catálogos de problemas y soluciones para las diferentes aplicaciones.
5. Inventario de producción, mantenimiento de redes y telecomunicaciones, incidentes, planes de entrenamiento en aplicativos, respaldos y restauraciones.
6. Planes aprobados e informes de mantenimiento preventivo y correctivo de hardware y software de usuarios finales.
7. Informes de incidentes atribuidos a la arquitectura, gestión y mantenimiento de aplicaciones de sistemas y servicios tecnológicos.

Gestión Interna de Soporte a Usuarios

1. Plan de acción y mejoras de los servicios tecnológicos.
2. Inventario de soporte tecnológico, respaldos y restauraciones.
3. Registro de requerimientos, aprobaciones, asignaciones, renovaciones de cuenta y perfiles, priorizadas, escaladas y efectivamente atendidas.
4. Actas entrega recepción de hardware y software a los usuarios finales.
5. Informes de incidentes atribuidos al soporte de servicios de TI.
6. Informes periódicos del número de activos, y planes de reposición de software y hardware.
7. Reportes de análisis estadísticos de los datos obtenidos en las encuestas sobre los servicios de TI.
8. Reportes de requerimientos emitidos por los usuarios para proponer mejoras e calidad del servicio de soporte.

Gestión Interna de Seguridad Informática, Interoperabilidad y Riesgos

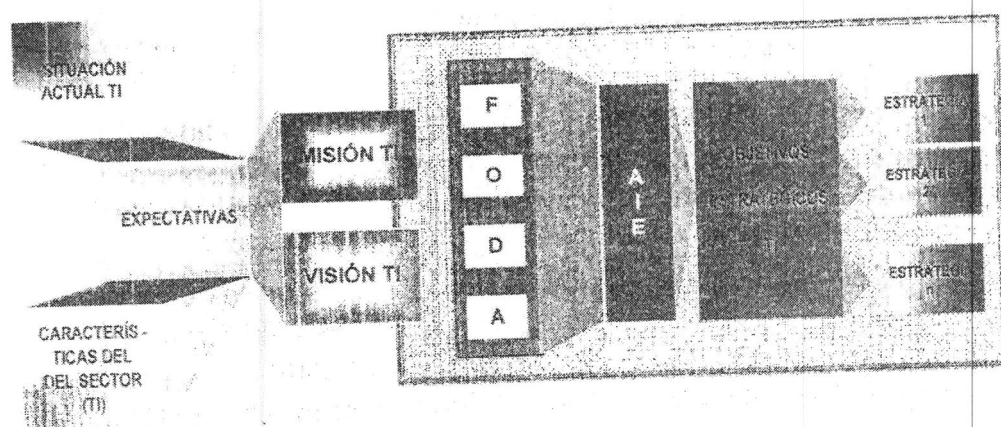
1. Políticas de seguridad de la información y procedimientos para su aplicación.
2. Planes de contingencia y prevención de impacto operativo a nivel de seguridad, por cambios, equipamiento y servicios tecnológicos
3. Acuerdos de servicio y estándares de calidad para el uso de aplicaciones y controles de acceso a los sistemas y servicios informáticos.
4. Acuerdos de confidencialidad de la información suscritos por TIC y por contratistas-contratantes, administradores y usuarios de los diferentes sistemas, servicios y soluciones de tecnologías de la información y comunicación.
5. Pruebas periódicas de copias de resguardo y restauración de la información en base a los perfiles de usuario.
6. Informes de seguimiento y control, así como también de las medidas de prevención de amenazas informáticas.

	PLAN ESTRATÉGICO TECNOLOGÍA DE INFORMACIÓN 2019-2020	FECHA: 13-Mayo-2019
		Versión: 1.0

7. Informes de análisis de riesgo y vulnerabilidades de Seguridad de la Información, así como de las estrategias de prevención y contingencia de estos riesgos.
8. Catálogo de clasificación en diferentes niveles de seguridad según sean: contratistas-contratantes, administradores y usuarios de los diferentes sistemas, servicios y soluciones tecnológicas.
9. Catálogo de procedimientos para asignación, actualización y revocación de cuentas y perfiles de usuarios en las aplicaciones, sistemas y servicios informáticos.

7 Desarrollo y Elaboración del Plan Estratégico de Tecnología de Información

Esta etapa se desarrolló con los funcionarios de Sistemas como "estrategas" y que tienen la responsabilidad de cumplir una metodología específica, que se presenta a continuación:



Del presente diagnóstico realizado, como primer punto se pudo identificar que actualmente Sistemas genera valor agregado a las operaciones de la institución, teniendo como funciones relevantes asesorar y desarrollar proyectos de tecnología, convirtiéndose en un pilar fundamental en las actividades administrativas y operativas de Quito Turismo.

Sin embargo, al diagnóstico realizado se suman resultados que se deben tomar en cuenta para el mejoramiento del modelo de gestión de la Jefatura, los cuales se mencionan a continuación:

- Desarrollo del Plan Estratégico de TI

Los planes han sido actualizados

- No se evidencia los registros de los procesos de soporte, desarrollo e infraestructura
- No se evidencia que los indicadores arrojen resultados reales respecto a la medición del desempeño de sus procesos

Los resultados mencionados serán los puntos en los cuales el presente plan se enfoca con el objetivo de solventar o mejorar mediante el planteamiento de objetivos y estrategias que encaminen a brindar un mejor servicio y satisfagan los requerimientos de las diferentes áreas operativas y administrativas de Quito Turismo.

Siendo una premisa fundamental que las definiciones estratégicas y operativas de tecnología de información deben estar totalmente alineadas con el Plan Estratégico de la Institución, es decir su Visión, Misión y Objetivos institucionales.

La segunda etapa se cumplió a través del desarrollo de los siguientes pasos metodológicos:

- Desarrollo del Plan Estratégico Institucional de TI
- Determinación de los grupos internos y externos que tienen relación con Sistemas, e identificación de sus intereses o requerimientos generales.
- Realización del FODA
- Áreas de Iniciativa Estratégica y de los Objetivos Estratégicos de TI
- Aspectos legales MINTEL Código Ingenios, para la contratación de software.
- Definición de las Estrategias para cada Objetivo Estratégico de TI, análisis, priorización y asignación de responsabilidades

7.1 Misión del área de Tecnología de Información

Conceptualmente la misión es la expresión escrita de una empresa o unidad administrativa, que informa hacia el interior y exterior de la misma, lo que hace, a quien intenta servir y en qué forma piensa hacerlo. En resumen, la misión es la descripción de su razón de ser.

Asesorar y coordinar la gestión de los servicios de tecnologías de la información de la entidad, alineados al plan estratégico institucional y al cumplimiento del Plan Nacional de Gobierno Electrónico y las políticas y objetivos gubernamentales; de manera que garantice la disponibilidad, integridad y confiabilidad de la información institucional.

7.2 Visión del área de Tecnología de Información

La visión es la expresión escrita de la imagen de lo que una organización, empresa o unidad administrativa quiere llegar a ser en un tiempo determinado. La visión para el área de Sistemas es:

	PLAN ESTRATÉGICO TECNOLOGÍA DE INFORMACIÓN 2019-2020	FECHA: 13-Mayo-2019
		Versión: 1.0

“Ser un departamento que brinda oportunamente herramientas y servicios de tecnología de información y comunicaciones de alta calidad, que utiliza un modelo de gestión eficiente, proactivo, estandarizado y alineado con la visión de Quito Turismo, para satisfacer a usuarios”.

7.3 Análisis FODA

AMENAZAS	FORTALEZAS
Cambio de políticas públicas, en cuanto a la adquisición de nueva tecnología, ya sea hardware o software.	Recursos económicos para mantenimiento de la infraestructura tecnológica y comunicaciones.
Falta de Recursos	Infraestructura (hardware, software, seguridades, comunicaciones) nueva y robusta.
	El personal de TI tiene alto empoderamiento de las operaciones de Quito Turismo
	Crecimiento continuo de la cultura tecnológica a nivel institucional.
	Ejecución de procesos y entrega de servicios basados en estándares de calidad
DEBILIDADES	OPORTUNIDADES
Reducido grupo de trabajo para atender los requerimientos de los usuarios de Quito Turismo.	Aplicación de nuevas tecnologías.
Sistemas informáticos críticos de Quito Turismo, con dependencia de proveedores	Leyes, Reglamentos y Normas que favorecen al Quito Turismo para su sostenibilidad y operaciones lo que implica la aplicación de TI como herramienta de gestión
No aplicación de metodologías orientadas a servicios de TI	
Capacitación al Personal de Tecnología	

7.4 Áreas de iniciativa estratégica

Las áreas de iniciativa estratégica se definieron al buscar las relaciones más fuertes entre los aspectos internos de la organización (Fortalezas y Debilidades) y los aspectos externos a la misma (Oportunidades y Amenazas). Las áreas identificadas son las siguientes áreas:

1. Sustentabilidad operativa
2. Satisfacción de los usuarios de los servicios de las TIC
3. Desarrollo, mantenimiento y mejora de los sistemas
4. Mejora e innovación de los recursos TIC

7.5 Objetivos estratégicos de Tecnología de Información

Dentro de las áreas de iniciativa estratégica mencionadas, se definieron los siguientes objetivos estratégicos de tecnología de información, junto con las metas establecidas para su implementación:

No. OBJ	OBJETIVO ESTRATÉGICO	No. IND.	NOMBRE DEL INDICADOR ÍNDICE	DESCRIPCIÓN DEL INDICADOR	LÍNEA BASE ACTUAL	META	UNIDAD DE MEDIDA	MÉTODO DE CÁLCULO (FÓRMULA)	COORD. RESP.
1	Mantener la estabilidad operativa de todos los recursos que provee TIC	1	Porcentaje de contratos gestionados dentro del tiempo de vigencia.	Mide el índice de contratos que han sido ejecutado dentro de su periodo de vigencia sin afectar la calidad de servicio.		80%	%	Número de contratos ejecutados a tiempo/ Número total de contratos	TIC
2	Alcanzar el nivel de satisfacción de usuarios de los productos y servicios de TIC	2	Porcentaje de satisfacción de usuarios sobre los servicios del departamento de TIC	Mide el índice de satisfacción integral de colaboradores de Quito Turismo con los servicios de TI utilizando encuestas semestrales anónimas		70%	%	Número de encuestas calificadas como muy bueno + Número de encuestas calificadas como excelente	TIC
3	Realizar el desarrollo, mantenimiento y mejoras de los sistemas de información críticos	2	Número de sistemas empoderados	Mide el número de sistemas de información que la unidad de desarrollo puede realizar cambios en el código fuente sin necesidad del proveedor.	1	14	Contador	Reporte mensual de avance acerca del nivel de empoderamiento de los sistemas de información	TIC
4	Implementar proyectos de innovación tecnológica en las unidades de Infraestructura, Desarrollo de Sistemas y Comunicaciones	4	Porcentaje de proyectos de innovación ejecutados	Mide el porcentaje de proyectos TIC ejecutados según lo planificado		70%	%	Número de proyectos ejecutados / Número de proyectos planteados.	TIC

7.6 Estrategias por objetivo estratégico de TI

Dentro de este punto, se buscó contar con definiciones más detalladas, sobre los pasos a seguir para que los objetivos propuestos puedan ser conseguidos en la práctica. Las maniobras estratégicas para este período son:

7.6.1 Objetivo 1: Mantener la estabilidad operativa de todos los recursos que provee TIC

El objetivo de gestionar y mantener controlada la vigencia de los contratos de los diferentes servicios de la TIC, es el poder conservar la calidad de entrega de servicios de TI al usuario interno, tomando en cuenta que muchos de los servicios que se entregan son de uso diario y necesarios para el trabajo habitual de los funcionarios de la institución.

	PLAN ESTRATÉGICO TECNOLOGÍA DE INFORMACIÓN 2019-2020	FECHA: 13-Mayo-2019
		Versión: 1.0

Implementar lineamientos para el inicio de procesos de contratación previo a la terminación de estos, permitiendo llevar el control de la vigencia de los contratos.

La gestión como tal, se la realizará mediante el uso de un sistema informático, que contendrá funcionalidades como: gestión del tiempo de inicio del proceso de renovación de contrato, registro de fechas de inicio y terminación, alertas de terminación de vigencia de contrato y todo esto basado en los lineamientos y directrices dictadas para el inicio de procesos de contratación donde se especifica: "con tres meses de anticipación se deben ingresar los contratos y el inicio de ejecución debe constar en los Términos de referencia".

Para tener una idea clara de las subactividades que se deben tener en cuenta para poder trabajarlas como parte de la estabilidad operativa a continuación se detallan:

SUBACTIVIDADES SUSTENTABILIDAD OPERATIVA	
ADQUISICIÓN DE REPUESTOS PARA EQUIPOS DE CÓMPUTO Y COMUNICACIONES	SERVICIO DE MANTENIMIENTO DEL SISTEMA DE ALERTA TEMPRANA
SERVICIO DE INTERNET BACK UP	SERVICIO DE MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE LOS EQUIPOS
SERVICIO DE TELECOMUNICACIONES	ADQUISICIÓN DE PARTES Y PIEZAS INFORMÁTICAS
MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE UPS	RENOVACIÓN DE MEMBRÉSIA EN TIENDA PARA APLICACIÓN MÓVIL ANDROID Y IOS
RENOVACIÓN Y ACTUALIZACIÓN DE PLATAFORMA WEB	ADQUISICIÓN DE REPUESTOS PARA EQUIPOS DE CÓMPUTO Y COMUNICACIONES
RENOVACIÓN Y ACTUALIZACIÓN PARA LA PROTECCIÓN DE VIRUS INFORMÁTICOS	ADQUISICIÓN DE EQUIPOS DE IMPRESIÓN
SERVICIO DE ADQUISICIÓN DE INSUMOS DE IMPRESIÓN	SERVICIO DE INTERNET BACK UP
ACTUALIZACIÓN SISTEMA DE CATASTROS	SERVICIO DE TELECOMUNICACIONES
SERVICIO DE SOPORTE PARA HERRAMIENTAS DE CORREO ELECTRÓNICO LICENCIADO	SERVICIO REPLICACIÓN DE INFORMACIÓN INSTITUCIONAL EN CENTRO ALTERNO DE PROCESAMIENTO DE DATOS
SERVICIO DE SOPORTE Y MANTENIMIENTO DE LA HERRAMIENTA DE VIRTUALIZACIÓN PARA SERVIDORES CORPORATIVOS	RENOVACIÓN Y ACTUALIZACIÓN DE HERRAMIENTAS DE OFIMÁTICA
SERVICIO DE SOPORTE Y MANTENIMIENTO DE HERRAMIENTAS DE INFRAESTRUCTURA INFORMÁTICA	SERVICIO DE SOPORTE Y MANTENIMIENTO PARA EL FIREWALL
SERVICIO DE SOPORTE Y MANTENIMIENTO PARA EL FIREWALL DEL CB-DMQ	RENOVACIÓN DE EQUIPOS INFORMÁTICOS
SERVICIO DE SOPORTE PARA HERRAMIENTA DE RESPADO Y RECUPERACIÓN	ADQUISICIÓN DE PARTES Y PIEZAS INFORMÁTICAS

7.6.2 Objetivo 2: Alcanzar el nivel requerido de satisfacción de usuarios de los productos y servicios de TIC

1. Definir e implementar un modelo de gestión de atención y satisfacción del cliente interno de TIC
2. Definir e implementar un modelo de gestión de TIC basado en buenas prácticas

La implementación de la metodología ITIL basada en buenas prácticas será una de las estrategias para alcanzar la satisfacción de los usuarios a través de productos y servicios de TI de calidad.

El modelo de gestión basado en buenas prácticas será el inicio para el ordenamiento de procedimientos de gestión y atención a usuarios a nivel interno de TIC, ya que a través de este se podrá utilizar de mejor manera los recursos y distribuir mejor las

La aplicación de buenas prácticas permitirá que la gestión de servicios de TI no solamente considere las tecnologías de información como el fin sino como medio para apoyar a negocio y por ende al usuario final, ocasionando así la mejora continua de los servicios entregados.

Los resultados de aplicar buenas prácticas es llegar a contar con un servicio confiable, seguro y consistente dentro los costes esperados, además que proporciona una cultura organizacional que aporta a mayores beneficios en la calidad de servicios.

La gestión de servicios de TI, tendrá como base el uso de una herramienta de OTRS que se encuentra implementada dentro de Quito Turismo, que permitirá el registro de cada uno de los requerimientos o soportes que forman parte de servicios de TIC. La herramienta utilizada permitirá llevar un seguimiento del trabajo generado por TIC, generando indicadores de gestión y de productividad que serán los parámetros que evidencien si se requiere realizar mejoras en cada uno de los procedimientos establecidos.

7.6.3 Objetivo 3: Realizar el desarrollo, mantenimiento y mejoras de los sistemas de información críticos

Se realizara una evaluación de los sistemas y a los usuarios que utilizan cada uno de los sistemas que cuenta Quito Turismo, con el fin de evaluar y tener una mejora continua de dichos sistemas.

En el Desarrollo se considerara las etas de inicio, planeación, ejecución, control, monitoreo y cierre de proyectos, así como los entregables, aprobaciones y compromisos formales mediante actas.

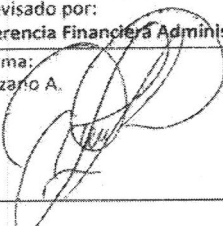
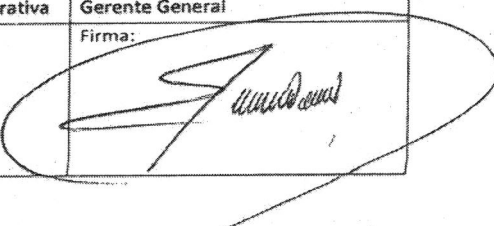
7.6.4 Objetivo 4: Implementar proyectos de innovación tecnológica en las unidades de Infraestructura, Desarrollo de Sistemas y Comunicaciones

Implementar proyectos de innovación que van atados al plan estratégico de ciudad, con el fin de brindar mejor accesibilidad e información de Quito a nivel nacional como internacional.

Mejorar proyectos a nivel de Direcciones con el fin de automatizar procesos y mejorar la eficiencia y eficacia de la empresa.

PLAN DE CONTINGENCIA

Mayo 2019

Elaborado por: Sistemas	Revisado por: Gerencia Financiera Administrativa	Aprobado por: Gerente General
Firma: Arellano K. Medina F.	Firma: Lozano A. 	Firma: 

	PLAN DE CONTINGENCIA	FECHA: 13-Mayo-2019
		Versión: 1.0

Índice

1	INTRODUCCION.....	3
2	GENERALIDADES.....	3
2.1	DEFINICIONES.....	3
A.	PLAN DE CONTINGENCIA:	3
B.	SISTEMA DE INFORMACIÓN.....	4
C.	EMERGENCIA	4
D.	FALLA:.....	4
E.	RECURSOS INFORMÁTICOS:.....	4
F.	TIEMPO DE INACTIVIDAD O DOWNTIME:.....	4
3	PRINCIPIOS, METAS Y OBJETIVOS	4
3.1	OBJETIVO GENERAL.....	5
3.2	OBJETIVOS ESPECÍFICOS	5
4	ALCANCE Y RESPONSABILIDADES	5
5	DETERMINACIÓN Y DETALLE DE LAS MEDIDAS PREVENTIVAS	6
6	PLAN DE CONTINGENCIAS INFORMATICAS	6
7	ESTRATEGIAS INFORMÁTICAS	7
8	ACCESO FÍSICO	7
9	ROLES Y RESPONSABILIDADES.....	7
9.1	Gerente de Administración o Responsable del Plan de Contingencias (PC)	8
9.2	Equipo de Administración de Contingencia	8
9.2.1	Líder del Equipo de Administración de Contingencia.....	9
9.2.2	Miembros del Equipo de Administración de Contingencia:.....	10
9.3	Equipo de Evaluación de Daños	10
9.4	Equipo de Hardware y Redes.....	11
9.5	Equipo de Software.....	12
9.6	Equipo de Comunicación.....	12
9.7	Equipo de Seguridad Personal y Física.....	12
9.8	Equipo de Soporte de Administración y Adquisición.....	12

	PLAN DE CONTINGENCIA	FECHA: 13-Mayo-2019
		Versión: 1.0

PLAN DE CONTINGENCIA

1 INTRODUCCION

El plan de contingencia de tecnologías de información de Quito Turismo, es un documento que establece los lineamientos de respuesta para atender en forma oportuna, eficiente y eficaz, daños en equipos de cómputo o desastres producto de eventos naturales u otros a causa de algún incidente tanto interno como externo a las tecnologías de información.

Durante el desarrollo del presente Plan, se presentan las actividades propias de gestión de contingencia que debe considerar Quito Turismo, cubriendo así los incidentes que afecten el sistema de información de tecnología. Así mismo aspectos conceptuales que permitan un mayor panorama acerca del entendimiento de las contingencias y que servirán como marco de referencia.

Las causas para aplicar el Plan de Contingencias pueden ser variadas, como por ejemplo: daño en los equipos de cómputo de los usuarios finales, daño de impresoras, daño de equipos activos de la red de datos, daño de los servidores de la institución, la elaboración del plan de contingencia implica un importante avance a la hora de superar situaciones de interrupción de las actividades y servicios prestados por Quito Turismo.

Es indispensable para el éxito del plan de contingencia, contar con personal capacitado y comprometido con la institución.

2 GENERALIDADES

2.1 DEFINICIONES

- A. **PLAN DE CONTINGENCIA:** Es una estrategia planificada, con una serie de procedimientos que nos facilitan o nos orientan, a tener una solución alternativa que nos permita restituir rápidamente los servicios de la organización, ante eventos que puedan presentarse en los servicios ya sea de forma parcial o total.
- B. **SISTEMA DE INFORMACIÓN:** Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo. Dichos elementos formarán parte de alguna de las siguientes categorías:

- Actividades o técnicas de trabajo;
- Datos;

	PLAN DE CONTINGENCIA	FECHA: 13-Mayo-2019
		Versión: 1.0

- Recursos materiales en general ((Papel, lápices, libros, carpetas, etc. Estas actividades de recolección y procesamiento de información, eran actividades manuales y solo con la llegada de la tecnología (computadoras, Internet, etc.) se han convertido en sistemas con recursos informáticos y de comunicación).
- C. **EMERGENCIA:** Una emergencia es una atención de forma urgente y totalmente imprevista, ya sea por causa de accidente o suceso inesperado. Depende el ámbito en el que se use, esta palabra podrá tener distintos significados. El termino emergencia suele ser utilizado por la mayoría de las personas para conjeturar una situación que se salió de control y como consecuencia, provocó un desastre.
- D. **FALLA:** es un estado o situación en la que se encuentra un sistema formado por dispositivos, equipos, aparatos y/o personas en el momento que deja de cumplir la función para el cual había sido diseñado."
- E. **RECURSOS INFORMÁTICOS:** Un recurso informático es cualquier aplicación, herramienta, componente o dispositivo que se puede agregar a una computadora o sistema; por lo tanto puede ser tanto un recurso de hardware (dispositivos) como de software (programas).
- F. **TIEMPO DE INACTIVIDAD O DOWNTIME:** El término tiempo de inactividad (downtime) es usado para definir cuando el sistema no está disponible (solo para servidores). Los casos DOWNTIME pueden ser planeados o no planeados. Los casos de tiempos de inactividad planeadas pueden ser por cambio del sistema, cambios de datos, reconfiguración del sistemas o reinicio de servicios. Los casos de tiempos de inactividad no planeadas pueden ser provocados por fallas del sistema, daño en los servidores, fallas de la red de datos, fallas en el fluido eléctrico.

3 PRINCIPIOS, METAS Y OBJETIVOS

Este plan de contingencia aplicable a Quito Turismo establece procedimientos para recuperar la red y los servicios de tecnologías de la información que utilizada para la prestación de servicios luego de una afectación producida en casos de desastres naturales o conmoción interna. Se han establecido los siguientes objetivos para el plan.

3.1 OBJETIVO GENERAL

Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información, para Quito Turismo, en caso de emergencia, fallas o suspensión en el procesamiento de la información por problemas en los equipos informáticos o programas.

	PLAN DE CONTINGENCIA	FECHA: 13-Mayo-2019 Versión: 1.0
---	-----------------------------	--

3.2 OBJETIVOS ESPECÍFICOS

- 5.1. Prevenir o minimizar la pérdida o la corrupción de archivos de datos críticos para la continuidad de las operaciones.
- 5.2. Proteger la propiedad de información de Quito Turismo.
- 5.3. Indicar los lineamientos para la recuperación de los servicios informáticos ante un desastre o falla.
- 5.4. Continuar con las funciones de las diferentes áreas de Quito Turismo, que se haya visto afectadas por una situación adversa.
- 5.5. Prevenir o minimizar el daño permanente a los recursos informáticos.

4 ALCANCE Y RESPONSABILIDADES

El plan de contingencia que se desarrolla en el presente documento es de aplicación a todas las áreas funcionales en la estructura orgánica y mapa de procesos de Quito Turismo que hacen uso de los recursos informáticos de la Institución.

El Jefe de sistemas o quien haga sus veces es el responsable de la ejecución del plan de contingencia con el apoyo del equipo de trabajo de la oficina de sistemas.

La copia de los datos almacenados en las estaciones de trabajo, son responsabilidad de cada uno de los usuarios.

Se debe designar un comité de seguridad con roles específicos.

5 DETERMINACIÓN Y DETALLE DE LAS MEDIDAS PREVENTIVAS

RECURSO	PROBLEMA RELACIONADO (RIESGO ASUMIDO)	
	POSIBILIDAD DE OCURRENCIA DEL PROBLEMA	PERIODO DE PARA ACEPTABLE
PC	MEDIA/ALTA	5 HORAS
SISTEMA DE INFORMACIÓN	BAJA	4 HORAS
SERVIDORES	BAJA	4 HORAS
IMPRESORA	MEDIA/ALTA	4 HORAS

	PLAN DE CONTINGENCIA	FECHA: 13-Mayo-2019
		Versión: 1.0

TELÉFONO IP	BAJA	1 DÍA
RED INALAMBRICA	BAJA	5 DÍAS

6 PLAN DE CONTINGENCIAS INFORMATICAS

La Administración de Sistemas de Quito Turismo creará para los departamentos un plan de contingencias informáticas que incluya al menos los siguientes puntos:

- Continuar con la operación del área con procedimientos informáticos alternos.
- Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.
- Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.
- Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
- Contar con un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía.
- Ejecutar pruebas de la funcionalidad del plan.
- Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.

7 ESTRATEGIAS INFORMÁTICAS

La estrategia informática de Quito Turismo se consolida en el Plan Estratégico de Informática y está orientada hacia los siguientes puntos:

- Plataforma de Sistemas Abiertos.
- Esquemas de operación bajo el concepto multicapas.
- Estandarización de hardware, software base, utilitarios y estructuras de datos
- Intercambio de experiencias entre Departamentos.
- Manejo de proyectos conjuntos con las diferentes áreas.
- Programa de capacitación permanente para los colaboradores de la empresa.

Para la elaboración de los proyectos informáticos y para la asignación de presupuesto de los mismos, se tomarán en cuenta tanto las necesidades de hardware y software del área solicitante, como la disponibilidad de recursos con los que cuente Quito Turismo.

	PLAN DE CONTINGENCIA	FECHA: 13-Mayo-2019 Versión: 1.0
---	-----------------------------	--

8 ACCESO FÍSICO

- Sólo al personal autorizado le está permitido el acceso a las instalaciones donde se almacena la información confidencial de Quito Turismo.
- Sólo bajo la vigilancia de personal autorizado, puede el personal externo entrar en las instalaciones donde se almacena la información confidencial, y durante un período de tiempo justificado.

9 ROLES Y RESPONSABILIDADES

El personal involucrado en las tareas del plan de contingencias para participar en la recuperación de las operaciones, infraestructura, todas las aplicaciones, y de los servicios de Quito Turismo.

9.1 *Gerente de Administración o Responsable del Plan de Contingencias (PC)*

Es el Gerente Financiero Administrativo y es responsable de la administración ejecutiva de todas las facetas del plan de contingencia y ejercicios de prueba del mismo, así como de las operaciones de recuperación, viene a ser el Responsable de Nivel 1 a contactar en caso de desastre natural o conmoción interna. Sus actividades son las siguientes:

- Previo al evento
 - Aprobar el Plan
 - Designar al Comité de acuerdo a las Responsabilidades
 - Asegurar que el plan sea mantenido y actualizado
 - Asegurar que se ejecute el plan de entrenamiento y capacitación
 - Autorizar los ejercicios periódicos de prueba del plan
 - Brindar soporte al líder del Equipo de Administración de Contingencia y a todos los demás participantes, previo y durante los ejercicios de prueba del plan.
- Posterior al Evento
 - Es el encargado de realizar la declaración de ocurrencia de eventos de desastres naturales o conmoción interna
 - Autorizar el desplazamiento y estadía para los miembros de los equipos
 - Autorizar los gastos a través del equipo de Administración.
 - Administrar y monitorear todo el proceso de recuperación.
 - Periódicamente informar a los mandos superiores, clientes, y personal de medios de comunicación acerca del estado del plan.

	PLAN DE CONTINGENCIA	FECHA: 13-Mayo-2019
		Versión: 1.0

- Soporte al líder del equipo de Administración de Contingencia y los demás participantes durante condiciones/situaciones que lo requieran

9.2 Equipo de Administración de Contingencia

El Equipo de Administración de Contingencia es el responsable de administrar los esfuerzos o tareas de recuperación; para asegurar que otros equipos y personal ejecuten todas las actividades del plan; proveer un "Centro de Comando" para coordinación y todas las comunicaciones; para asegurar que las actividades son ejecutadas entre todos los equipos dentro de los tiempos planificados y para proveer asistencia en la resolución de problemas que puedan presentarse. Este equipo es activado por el Gerente de Administración del PC o el propietario del sistema. Todos los demás equipos reportan directamente al equipo de Contingencia/Administración, cuyos deberes específicos son:

9.2.1 Líder del Equipo de Administración de Contingencia

- Previo al Evento
 - Mantener y actualizar el plan de acuerdo a lo requerido o programado, lo cual no debe ser mayor a un año
 - Distribuir copias del plan a los miembros de los equipos
 - Coordinar pruebas requeridas o programadas en un tiempo no mayor a un año
 - Entrenar a los miembros del equipo
- Posterior al Evento
 - Cumplir con la notificación inicial a los miembros del equipo
 - Establecer un centro de comando para las operaciones de recuperación
 - Asistir en la evaluación de daños
 - Coordinará actividades de los equipos de recuperación
 - Notificar de un sitio alternativo para reactivación del sistema en caso de requerirse
 - Notificar a los líderes de los equipos acerca de la activación del Plan de Contingencia
 - Autorizar al Equipo de Administración para realizar los arreglos necesarios para el viaje y hospedaje de los miembros del equipo de recuperación.
 - Reportar periódicamente al Gerente de Administración del PC acerca del estado de las actividades de recuperación y otros detalles de acuerdo a lo requerido

9.2.2 Miembros del Equipo de Administración de Contingencia:

- Previo al Evento
 - Asistir al Líder del Equipo de acuerdo a lo dispuesto

	PLAN DE CONTINGENCIA	FECHA: 13-Mayo-2019 Versión: 1.0
---	-----------------------------	--

- Entender todos los roles y responsabilidades del Plan de Contingencia
- Posterior al Evento
 - Ejecutar funciones del centro de comando
 - Mantener un historial de todas las comunicaciones utilizando las formas provistas

9.3 Equipo de Evaluación de Daños

El Equipo de Evaluación de Daños es responsable de evaluar los daños en la infraestructura, equipos y redes, tan pronto como sea posible luego de la activación del Plan de Contingencia, y reportar el nivel de daños al equipo de Administración de Contingencia/Emergencia. El equipo además, provee asistencia cuando sea posible en los trabajos de limpieza y reparación requeridas. Específicamente las responsabilidades del equipo son:

- Previo al evento
 - Entender su rol y responsabilidades bajo el Plan de Contingencia
 - Trabajar para reducir la probabilidad de eventos que requieran la activación del Plan de Contingencia.
 - Entrenar a los empleados en la preparación para emergencias
 - Participar en los ejercicios y pruebas del Plan de Contingencia.
 - Tener un conocimiento profundo de los procedimientos de evaluación de daños
- Posterior al Desastre
 - Determinar la accesibilidad a la infraestructura, oficinas, y a las áreas/estaciones de trabajo
 - Evaluar la extensión del daño al sistema de telecomunicaciones
 - Evaluar las necesidades y/o adecuaciones físicas de seguridad/protección
 - Estimar el tiempo para recuperar las facilidades primarias y del Sistema
 - Identificar el hardware rescatable
 - Informar al Equipo de Administración de Contingencia acerca del grado de los daños, tiempo estimado de recuperación, la necesidad de seguridad física, y detalle de los equipos recuperables.
 - Mantener un registro de equipo recuperable
 - Coordinar con los proveedores la restauración, reparación o reemplazo del equipamiento que no está bajo la responsabilidad de otros equipos.
 - Colaborar con la limpieza de las facilidades luego del incidente

	PLAN DE CONTINGENCIA	FECHA: 13-Mayo-2019
		Versión: 1.0

9.4 Equipo de Hardware y Redes

El equipo de Hardware y Redes es responsable por la preparación del sitio, planificación física, e instalación del equipamiento y redes para soportar los servicios requeridos cuando se activa el Plan de Contingencia. Las responsabilidades del equipo incluyen la provisión e instalación de hardware, software y redes necesarios en los sitios originales y/o alternos permanentes.

- Previo al Evento
 - Entender los roles y responsabilidades establecidos bajo el PC (Plan de Contingencia).
 - Trabajar conjuntamente con el equipo de Administración de Contingencia para reducir la probabilidad de eventos que requieren la activación del Plan de Contingencia
 - Entrenar a los empleados en la preparación para emergencias
 - Participar en los ejercicios y pruebas del plan de contingencia
 - Comprender a detalle los procedimientos de PC
 - Mantener información actualizada de la configuración del Sistema en un sitio alternativo y en los apéndices del presente plan
- Posterior al Evento
 - Verificar los requerimientos de instalación pendientes en el sitio original o sitio alternativo de requerirse
 - Inspeccionar el espacio físico en el sitio alternativo (de requerirse)
 - Coordinar con los miembros de los equipos de Software, Comunicaciones y Operaciones acerca de la configuración del espacio para el sitio alternativo
 - Coordinar el transporte de equipo rescatable al sitio alternativo
 - Notificar al equipo de administración acerca de los requerimientos de equipos y redes
 - Asegurar la instalación de terminales y estaciones de trabajo temporales requeridos para conexión con el hardware del sitio alternativo
 - Planificar la instalación de hardware y redes en el sitio original o en el alternativo
 - Planificar y coordinar el transporte e instalación de hardware en el sitio original o sitio alternativo permanente, cuando esté disponible

9.5 Equipo de Software

El Equipo de Software es responsable por la instalación y configuración de todos los sistemas y aplicaciones de software no instaladas por otros administradores.

	PLAN DE CONTINGENCIA	FECHA: 13-Mayo-2019 Versión: 1.0
--	-----------------------------	--

- Previo al Evento
 - Comprender los roles y responsabilidades establecidos bajo el PC.
 - Trabajar conjuntamente con el Equipo de Administración de Contingencia para reducir la probabilidad de eventos que pueden requerir la activación del PC.
 - Capacitar a los empleados en la preparación para emergencias
 - Participar en los ejercicios y pruebas de PC
 - Comprender a detalle los procedimientos de PC
 - Mantener actualizada la información de configuración del software en un sitio diferente al de operación normal y de ser posible como anexo al presente plan
- Posterior al Evento
 - Coordinación para la entrega de los contenedores, ubicados en sitio alternativo, que mantienen la información de respaldo
 - Recibir, mantener inventario y controlar el acceso al sitio alternativo de almacenamiento de la información de respaldo
 - Restaurar los archivos de datos del software de los sistemas/aplicaciones no instalados en conjunto con otros planes de recuperación
 - Probar y verificar las funciones del sistema operativo y software de aplicaciones de acuerdo a lo requerido
 - Retornar los contenedores de almacenamiento de la información de respaldo al sitio alternativo de almacenamiento

9.6 Equipo de Comunicación

El equipo de Sistemas es responsable por el establecimiento de enlaces de voz y datos hacia/desde el sitio alternativo. Esto incluye la conexión local y remota de usuarios/clientes al sitio alternativo.

- Previo al Evento
 - Comprender los roles y responsabilidades establecidos bajo el PC
 - Trabajar conjuntamente con el equipo de administración de Contingencia para reducir la probabilidad de eventos que puedan requerir la activación del PC
 - Entrenar a los empleados en la preparación para emergencias
 - Participar en los ejercicios y pruebas de PC
 - Mantener actualizada la información de configuración del sistema de comunicaciones en un sitio alternativo al de operación normal y de ser posible como anexo a este PC
- Posterior al Evento

	PLAN DE CONTINGENCIA	FECHA: 13-Mayo-2019
		Versión: 1.0

- Asistir al equipo de Evaluación de Daños en la evaluación del equipo de comunicaciones
- Planificar, coordinar e instalar el equipo de comunicación requerido en el sitio alternativo
- Planificar, coordinar, e instalar el cableado necesario en el sitio alternativo y que no está incluido en otro procedimiento de recuperación

9.7 Equipo de Seguridad Personal y Física

El equipo de Seguridad Personal y Física es responsable de proveer identificaciones personales y limitaciones de acceso a las diferentes instalaciones y actúa como enlace con el personal de seguridad. Esto es crucial durante el período de un incidente debido al gran número de vendedores, contratistas y otro tipo de visitantes requiriendo acceso a las facilidades.

- Previo al evento
 - Comprender los roles y responsabilidades establecidos bajo el PC
 - Trabajar conjuntamente con el Equipo de Administración de Contingencia para garantizar la seguridad física de la facilidades y sistemas existentes
 - Capacitar a los empleados en la preparación para incidentes
 - Participar en los ejercicios y pruebas PC
 - Comprender a profundidad los procedimiento del PC
- Posterior al Evento
 - Acordonar las facilidades incluyendo oficinas para restringir el acceso a personal no autorizado
 - Coordinar con el administración de la infraestructura para el acceso del personal autorizado
 - Proveer seguridad/resguardo físico adicional
 - Actuar como enlace con el personal de emergencia, tal como departamentos de bomberos y policía
 - Programar y proveer seguridad para la transportación para archivos, reportes y equipamiento
 - Proveer asistencia a oficiales que se hallan investigando los daños del sitio y facilidades

9.8 Equipo de Soporte de Administración y Adquisición

El Equipo de Soporte de Administración y Adquisiciones es responsable de proveer el soporte administrativo, almacenamiento en sitio alterno, y otros

	PLAN DE CONTINGENCIA	FECHA: 13-Mayo-2019
		Versión: 1.0

limitada para financiar gastos emergentes diferentes a los de bienes de capital y salarios. Este equipo es también responsable para transmitir información pertinente al Gerente Financiero Administrativo.

- Previo al Evento
 - Comprender los roles y responsabilidades establecidos en el PC
 - Trabajar conjuntamente con el Equipo de Administración de Contingencia para asegurar que todas las funciones administrativas sean completadas.
 - Trabajar conjuntamente con el Equipo de Administración de Contingencia para reducir la probabilidad de eventos que puedan requerir activación del PC
 - Trabajar conjuntamente con el Equipo de Administrador de Contingencia para asegurar que todos los medios de transportación requeridos sean entendidos y provistos
 - Capacitar a los empleados en la preparación para las emergencias
 - Participar en los ejercicios de contingencia
 - Conocer los procedimientos a ser ejecutados
 - Estar seguros de que los detalles de administración de los gastos y de fondos necesarios para administrar la emergencia sean conocidos.
 - Evaluar la necesidad de medios alternativos de comunicación (otros diferentes a los servicios normales de telefonía), y que los mismos estén disponibles para todos los empleados involucrados
 - Asegurar que las listas actualizadas de medios de transporte viables hasta el lugar alternativo se mantienen tanto en las instalaciones de almacenamiento fuera de sitio y en un apéndice de este plan
 - Asegúrese de que la información de contacto actualizada para el Encargado del Departamento de Prensa y del Departamento de Representación Legal se mantiene tanto en las instalaciones de almacenamiento fuera del sitio y se incluye en un apéndice de este plan
- Posterior al Evento
 - Preparar, coordinar, y obtener aprobación para todos los requerimientos de adquisiciones
 - Coordinación de entregas
 - Procesar requerimientos de pago para todas las facturas relacionadas al incidente
 - Coordinar los viajes y alojamiento de los miembros del equipo
 - Proveer recursos para la adquisición de equipamiento de telefonía y servicios

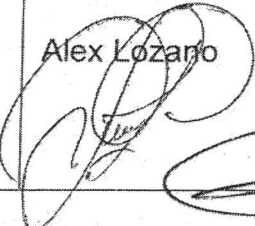
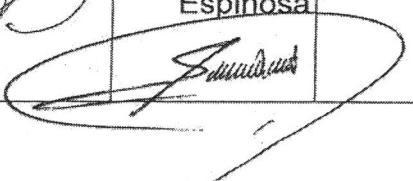
	PLAN DE CONTINGENCIA	FECHA: 13-Mayo-2019
		Versión: 1.0

- Proveer medios alternativos de comunicación entre los equipos en el evento de que el servicio normal de telefonía no esté disponible
- Proveer servicios temporales de telefonía para archivado, y otros servicios administrativos requeridos por los equipos
- Coordinar con otros equipos la provisión de transporte requerido
- Planear, coordinar y proveer transportación a sitios alternos para los equipos de acuerdo a lo requerido en el cumplimiento de sus funciones
- Dar soporte a las actividades de los Departamentos de Relaciones con los Medios y de Representación Legal de acuerdo a lo establecido por el Equipo de Administración de Contingencia

Política de Redes, Comunicaciones, Infraestructura y Seguridad Informática	Elaborado por	Revisado por	Aprobado por	
	Karla Arellano Fabricio Medina	Alex Lozano	Leonidas Espinosa	

POLÍTICAS DE REDES, COMUNICACIONES, INFRAESTRUCTURA Y SEGURIDAD INFORMÁTICA

Fecha: Mayo -2019
Versión: 1.0

Política de Redes, Comunicaciones, Infraestructura y Seguridad Informática	Elaborado por	Revisado por	Aprobado por	
	 Arellano K. Medina F.	 Alex Lozano	 Leonidas Espinosa	

Política de Redes, Comunicaciones, Infraestructura y Seguridad Informática	Elaborado por:	Revisado por	Aprobado por	
	Karla Arellano Fabricio Medina	Alex Lozano	Leonidas Espinosa	

Política de Redes, Comunicaciones, Infraestructura y Seguridad Informática	Elaborado por	Revisado por	Aprobado por	
	Karla Arellano Fabricio Medina	Alex Lozano	Leonidas Espinoza	

Índice

1. Introducción	4
2. Objetivo	4
Objetivos específicos	4
3. Alcance	4
4. Como usar este documento	4
5. Declaración de políticas	5
5.1 POLÍTICAS GENERALES DEL ÁREA DE REDES, COMUNICACIONES, INFRAESTRUCTURA Y SEGURIDAD INFORMÁTICA	5
5.2 OPERACIÓN DEL ÁREA DE REDES, COMUNICACIONES, INFRAESTRUCTURA Y SEGURIDAD INFORMÁTICA	6
5.3. SEGURIDAD PERIMETRAL	7
5.5. NIVELES DE SEGURIDAD LÓGICO Y FÍSICO.	8
5.5. AUTORIZACIÓN, AUTENTICACIÓN, Y ACCESO.	9
5.6. NIVELES DE CONFIDENCIALIDAD DE LA INFORMACIÓN	10
5.7. DE LA SEGURIDAD DE LOS DATOS.	11
5.8. DE LAS ADQUISICIÓN DE EQUIPOS.	12

Política de Redes, Comunicaciones, Infraestructura y Seguridad Informática	Elaborado por	Revisado por	Aprobado por	
	Karla Arellano	Alex Lozano	Leonidas Espinosa	

1. Introducción

El área de Sistemas de Quito Turismo, requiere de la implementación de políticas de Redes, Comunicaciones, Infraestructura y Seguridad de la Información para la empresa.

2. Objetivo

Establecer políticas que normen los procedimientos y actividades del Área de Redes, Comunicaciones, Infraestructura y Seguridad informática, en función del soporte de los servicios que brinda el área de sistemas.

Objetivos específicos

- Establecer políticas generales del Área de Redes, Comunicaciones, Infraestructura y Seguridad Informática
- Establecer políticas para la operación del Área de Redes, Comunicaciones, Infraestructura y Seguridad Informática
- Establecer políticas para el seguimiento
- Establecer políticas para la mejora continua

3. Alcance

Este documento tiene como alcance la implementación de las políticas generales para Redes, Comunicaciones, Infraestructura y Seguridad de la Información de Quito Turismo.

4. Como usar este documento

Política de Redes, Comunicaciones, Infraestructura y Seguridad Informática	Elaborado por	Revisado por	Aprobado por	
	Karla Arellano	Alex Lozano	Leonidas Espinosa	

Este documento es una Guía objetiva sobre los procedimientos actividades y tareas específicas que garantizarán una operación y ejecución de los servicios tecnológicos en el Área de Redes, Comunicaciones, Infraestructura y Seguridad Informática.

5. Declaración de políticas

5.1 POLÍTICAS GENERALES DEL ÁREA DE REDES, COMUNICACIONES, INFRAESTRUCTURA Y SEGURIDAD INFORMÁTICA

Redes.

- Utilización de una tecnología de administración de dominios
- Definir grupos de trabajo
- Determinar las funciones y atribuciones de los grupos de trabajo
 - Establecer si fuera el caso horarios de acceso a los recursos de la red por parte de los grupos de trabajo
- Definir los derechos de uso de los recursos de la red por parte de los grupos de trabajo.
 - Uso de impresoras de red.
 - Carpetas compartidas

Servidores.

- Establecer procedimientos de administración de las claves de acceso a los servidores corporativos.
- Asignación de claves, las mismas que deberán generarse cada mes por seguridad.
- La periodicidad de los cambios en las claves debe ser no mayor a un mes.
- Establecer la persona responsable de mantener en sobre sellado todas las claves de los servidores corporativos.
- Definir el procedimiento para acceder a ésta claves en caso de contingencias, a través de un diagrama de procesos legible y de fácil interpretación.
- Mantener contratos de mantenimiento preventivo y correctivo de los servidores corporativos.

Política de Redes, Comunicaciones, Infraestructura y Seguridad Informática	Elaborado por	Revisado por	Aprobado por	
	Karla Arellano	Alex Lozano	Leonidas Espinosa	

Es responsabilidad del área de sistemas las Redes, Comunicaciones, Infraestructura y Seguridad Informática.

- Garantizar la Continuidad y Disponibilidad de servicios de tecnología de Quito Turismo.
- Administrar los servicios y Servidores de Quito Turismo.
- Proponer soluciones para el mejoramiento de los sistemas y servicios.
- Gestionar Solución a Problemas.
- Administrar proyectos encomendados en el campo de su competencia.
- Diseñar bases técnicas en el campo de su competencia en coordinación con el área técnica.
- Asesorar técnicamente a los usuarios, áreas y direcciones en el campo de Tecnologías de Información
- Investigar las Nuevas tendencias tecnológicas y su posible aplicación en el Área de su competencia

5.2 OPERACIÓN DEL ÁREA DE REDES, COMUNICACIONES, INFRAESTRUCTURA Y SEGURIDAD INFORMATICA

- El Acceso a la administración de los servidores y demás equipos del data center de Quito Turismo son exclusivos e intransferibles para los Funcionarios de Área de Sistemas.
- Las claves de Acceso a los servidores estarán bajo la custodia y son de responsabilidad del área Sistemas y no podrán ser entregadas bajo ningún concepto sin previa autorización por escrito del Gerente Financiero Administrativo.
- La Gestión de las claves es de estricta responsabilidad del Área Sistemas.
- Las Claves serán entregadas a los responsables en un sobre sellado con un acta de entrega Recepción que certifique la entrega y la responsabilidad del que recibe la clave.
- Una vez entregada la clave el cambio de la misma estará bajo la responsabilidad del usuario dueño de la clave.
- La configuración de los Servicios tecnológicos en los ambientes de preproducción y producción así como el paso a producción de las aplicaciones desarrolladas o adquiridas, son de responsabilidad del Área de Sistemas.

Política de Redes, Comunicaciones, Infraestructura y Seguridad Informática	Elaborado por	Revisado por	Aprobado por	
	Karla Arellano	Alex Lozano	Leonidas Espinosa	

- Es responsabilidad del Área de Sistemas monitorear tanto los enlaces de comunicaciones así como los servicios tecnológicos de Quito Turismo. Además de garantizar la continuidad de los servicios y comunicaciones.
- Cualquier Modificación, cambio o problema que se presente en los servicios, servidores que afecten normal funcionamiento de los servicios tecnológicos, deberán comunicarse las fallas y el tiempo de retorno del Servicio, con las Áreas de la Quito Turismo.

5.3. SEGURIDAD PERIMETRAL

- El área de sistemas mantendrá un inventario de las direcciones IP públicas y su uso.
- El área de sistemas, actualizará los parches de seguridad de los servidores corporativos y de los equipos informáticos de los usuarios finales en forma periódica
- El área de sistemas procurará instalar en los servidores corporativos las herramientas de software que permitan:
 - Implementar soluciones de detección de spam, antivirus, anti spyware, phishing en los servidores de mail.
 - Implementar soluciones de detección de intrusos (IDS) y de protección ante intrusos
- (IPS).
 - Los servidores que permitan acceso remoto que normalmente deben estar en la zona desmilitarizada deben mantenerse en constante control y vigilancia y contar con todas las herramientas antes mencionadas.

5.4. SEGURIDAD COMPONENTES ACTIVOS DE CABLEADO.

- Los responsables informáticos evaluarán los sistemas de cableado de Quito Turismo.
- Los componentes activos de la red:
 - La Jefatura de sistemas promoverá el cambio de los hubs existentes en la red por switchces a fin de mantener los estándares de calidad de servicio (QoS) determinados
 - Revisar con una frecuencia trimestral los racks de comunicaciones, la tomas de energía, los reguladores de voltaje, los sistemas

Política de Redes, Comunicaciones, Infraestructura y Seguridad Informática	Elaborado por	Revisado por	Aprobado por	
	Karla Arellano	Alex Lozano	Leonidas Espinosa	

- ininterrumpibles de energía (UPS).
- La Jefatura de sistemas deberá promover el realizar contratos de mantenimiento preventivo y correctivo de los equipos activos de la red de las diferentes unidades administrativas.
- La Jefatura de sistemas deberá evaluar con una periodicidad de un año el crecimiento de la red a fin de estimar la capacidad de los equipos activos y prever su actualización.
- Los usuarios finales de los equipos deben cuidar del buen uso de los componentes de red a los que tienen acceso (puntos de red, toma eléctrica, patch cords, supresores de picos, etc.) y reportar a los encargados informáticos cualquier novedad en los mismos
- Las tomas eléctricas reguladas son de uso específico de los equipos informáticos, por ésta razón por ningún motivo se deben conectar a las tomas eléctricas de red otro tipo de equipos eléctricos y/o electrónicos (cafeteras, celulares, etc.)
- La jefatura de sistemas promoverá la realización de auditorías informáticas a los sistemas y aplicaciones de forma anual, a fin de determinar la idoneidad de uso, la optimización de los recursos.

5.5. NIVELES DE SEGURIDAD LÓGICO Y FÍSICO.

El cuarto de control deberá contar con las seguridades físicas para acceso controlado a la infraestructura y por conexión, que permitan identificar sin repudio los individuos que ingresan a los CPD (Centro de Procesamiento de Datos) que principalmente deberá mantener:

- Seguridad de acceso mediante puertas y cerraduras eléctricas
- Sistemas de aire acondicionado
- UPS
- Sistemas detectores de humo
- Sistemas detectores y extintores de incendio en base a CO2.
- Plan de alternancia de uso de servidores y sistemas por ciclos de mantenimiento.
- Bitácoras de servicio.
- Control de órdenes de cambio y de mejoramiento de sistemas.
- Registro de Usuarios asignados con clave de acceso, por función y autorizados por autoridad competente, así como por período de tiempo de vigencia.
- Diagrama de procesos visible a todos los funcionarios que laboran en la dependencia.

Política de Redes, Comunicaciones, Infraestructura y Seguridad Informática	Elaborado por	Revisado por	Aprobado por	
	Karla Arellano	Alex Lozano	Leonidas Espinosa	

Se utilizarán mecanismos de clave pública en aquellas aplicaciones que así lo permitan, según su Arquitectura Transaccional.

Toda Solución TIC o Servicio Tecnológico debe contener en su diseño de Arquitectura Transaccional el método y mecanismos de acceso controlado a aplicarse.

El acceso controlado a Soluciones TIC y Servicios Tecnológicos contempla: claves de acceso, encriptación de claves (establecidas por fabricantes de productos comerciales o implementadas en la creación de productos a medida para la institución), logs transaccionales de seguimiento.

El acceso lógico y físico debe ser diseñado e implementado considerando necesidades de acceso transaccional interno (intranet) y externo (a través de internet).

Todo servicio publicado al internet, deberá contar con un certificado de seguridad SSL (Securyti Soccer Layer) al menos de 128 bits.

5.5. AUTORIZACIÓN, AUTENTICACIÓN, Y ACCESO.

Se establecen dos formas de acceso a las soluciones y servicios de Quito Turismo: PERSONAL y AUTOMÁTICO; el primero se refiere al acceso que efectúa individualmente una persona (interna o externa a la institución), mientras que el segundo se refiere al acceso que efectúa automáticamente las herramientas tecnológicas entre las diversas Soluciones TIC como parte de su transaccionalidad programada.

Todo acceso a Soluciones TIC y Servicios Tecnológicos están basados en PERFILES DE ACCESO (conjunto de permisos designados para que de manera personal o automática se establezca la conexión y uso de la información y/o recursos tecnológicos), los niveles de acceso, restricciones y claves son de exclusiva responsabilidad de Quito Turismo, a solicitud expresa y por escrito de los Directores respectivos (autorizadores del uso de la información).

El diseño de gestión en el uso de la Solución TIC y Servicios Tecnológicos establecerá formalmente las funciones y responsabilidades de los actores que conformarán y aplicarán la asignación de accesos bajo el esquema de las mejores prácticas de un Sistema de Gestión de Seguridad de la Información.

Política de Redes, Comunicaciones, Infraestructura y Seguridad Informática	Elaborado por	Revisado por	Aprobado por	
	Karla Arellano	Alex Lozano	Leonidas Espinosa	

Los productos de software deberán obligatoriamente validar su acceso contra la Arquitectura Tecnológica de Seguridad vigente, cumpliendo los estándares establecidos oficialmente por Quito Turismo.

Las claves de acceso a Soluciones TIC y Servicios Tecnológicos son información considerada de nivel CONFIDENCIAL; por lo que se debe establecer procedimientos orientados a su creación, entrega, custodia, uso, cambios y eliminaciones. Los procedimientos y mecanismos deben permitir la caducidad de vigencia de las claves de acceso de tal forma que se obligue al cambio periódico de las mismas. No pueden existir claves quemadas (escritas directamente) en códigos de programación que limiten o impidan el cambio periódico de claves.

Para garantizar la idoneidad, funcionalidad, complementariedad e integridad de los sistemas en producción, de forma anual, el área de sistemas convocará a concurso para la ejecución de una Auditoría informática integral de uso de los sistemas, la misma que determinará niveles de servicio alcanzados, eficiencia de los sistemas y demás elementos técnicos propios que garanticen el correcto funcionamiento de los sistemas.

5.6. NIVELES DE CONFIDENCIALIDAD DE LA INFORMACIÓN

El nivel de confidencialidad es un calificador compuesto que tiene cada documento (físico o digital).

Toda información (física o digital), debe establecer claramente el nivel de confidencialidad asignado al documento así como su naturaleza del estado de validez, tales como borrador, versión final, etc.

Todo elemento de gestión de la información (programas, archivos, documentos), deberá tener la referencia de los controles de elaboración y validación del mismo.

Todo elemento de gestión de la información (programas, archivos, documentos), deberá tener la referencia de los controles de elaboración y validación del mismo.

Los niveles generales de confidencialidad de la información serán CONFIDENCIAL (Información de conocimiento y uso exclusivo de la institución

Política de Redes, Comunicaciones, Infraestructura y Seguridad Informática	Elaborado por	Revisado por	Aprobado por	
	Karla Arellano	Alex Lozano	Leonidas Espinosa	

según autorización de acceso establecida), RESERVADA (Información de conocimiento y uso exclusivo de la institución por un periodo de tiempo, luego del cual perderá esa naturaleza si no ha sido reclasificada oficialmente), PUBLICA (Información de conocimiento y uso general a nivel interno y externo).

Todo actor que utilice información considerada como CONFIDENCIAL o RESERVADA deberá suscribir un acuerdo de confidencialidad unilateral de manejo y uso ético de información y para el caso de los funcionarios públicos, quien administre la información deberá mantener vigente, durante el período de sus funciones una caución otorgada.

5.7. DE LA SEGURIDAD DE LOS DATOS.

- Mantener respaldos de la información institucional en los servidores de red interna de Quito Turismo. La frecuencia de los respaldos de la información almacenada en los equipos será diaria; además se deberán conservar las copias de seguridad correspondientes almacenadas en el cuarto de control y ve la posibilidad de tener a fuera, con su respectiva bitácora. Mantener copias de los respaldos debidamente etiquetados, en sitios pre determinados y alejados geográficamente de la dependencia.
- Los respaldos mínimos diarios deberán ser incrementales, y los de fin de semana deberán ser totales.
- Mantener la biblioteca con la documentación de los sistemas de información, productos de aplicación, libros, manuales, colecciones y revistas, así como, disquetes, CD's, cintas y otros dispositivos de almacenamiento de los sistemas y productos de aplicación, de propiedad de la institución y su correspondencia con la bitácora.
- Promover auditorias operativas en forma periódica a fin de verificar el cumplimiento del presente instrumento.
- Los usuarios de los equipos, deberán mantener respaldos de la información existente en su computador asignado. La frecuencia estará de acuerdo al volumen de los cambios a los datos. Se recomienda obtener el respaldo al menos una vez por semana, además deberán conservarse las copias de seguridad correspondientes.
- Los servidores considerados para la obtención de los respaldos deberán ser: (i)
Los servidores de las aplicaciones de misión crítica
 - Los servidores de bases de datos
 - Los servidores de mail.

A ellos se debe sumar equipos alternos en paralelo, que garanticen la interoperabilidad automática en casos fortuitos y catastróficos.

Política de Redes, Comunicaciones, Infraestructura y Seguridad Informática	Elaborado por	Revisado por	Aprobado por	
	Karla Arellano	Alex Lozano	Leonidas Espinosa	

De los datos y los sistemas de procesamiento de datos:

- Contar con manuales automáticos de validación de los datos que son ingresados a los sistemas informáticos, estos procesos deben estar debidamente documentados
- Los procesos automáticos de validación de datos que se deban incorporar en los sistemas informáticos, deberán ser resueltos en forma conjunta.
- Los datos y los resultados de su procesamiento son propiedad institucional y de uso público, con excepción de la información considerada como reservada y/o de uso restringido

5.8. DE LAS ADQUISICIÓN DE EQUIPOS.

Las adquisiciones de recursos informáticos deberán realizarse contra los presupuestos del área, para otros casos, las adquisiciones deberán realizarse contra el presupuesto del área requirente.

La Jefatura de Sistemas será la unidad responsable de analizar los requerimientos de equipos o productos de aplicación informáticos de las áreas. Las adquisiciones podrán ser:

- ADQUISICIONES PLANIFICADAS:** aquellas que deberán constar en el presupuesto de cada año, como resultado de la elaboración del Plan anual de compras, en el que se recogerán los requerimientos formulados por las áreas.

Para generar el Plan Anual de Adquisiciones, los pedidos deberán estar dirigidos a la Gerencia Financiera Administrativa hasta el mes de julio de cada año, para el análisis y elaboración del Informe técnico correspondiente; y,

- ADQUISICIONES NO PLANIFICADAS:** aquellas solicitudes de requerimientos que se enmarcan en proyectos especiales o necesidades que no fueron incluidas en el Plan Anual de compras y serán analizadas por la Gerencia Financiera Administrativa y el área solicitante.

Las solicitudes de requerimientos que correspondan a la adquisición de componentes o repuestos de equipos de computación, lo realizarán desde el área de sistemas.

Política de Redes, Comunicaciones, Infraestructura y Seguridad Informática	Elaborado por	Revisado por	Aprobado por	
	Karla Arellano	Alex Lozano	Leonidas Espinosa	

Los parámetros a considerar en el análisis operativo serán los siguientes:

- El número de equipos instalados y sus características técnicas
- Los productos de aplicación instalados en cada uno de los equipos
- El cumplimiento de normas y procedimientos estándar en vigencia
- Los sistemas y productos de aplicación que se encuentren en uso
- El nivel y las frecuencias de uso de las herramientas y sistemas operativos instalados;
- Las capacidades de memoria y de almacenamiento requeridos para cada uno de los equipos, en función de las tareas que se desarrollan:
 - Los niveles de seguridad en el manejo de equipos y/o información, las seguridades de acceso, las instalaciones físicas y los procedimientos de respaldo;
- Los requerimientos no satisfechos en equipos, en productos, aplicaciones y en seguridades.

La adquisición del software comercial deberá procurarse mediante el establecimiento de convenios corporativos entre los proveedores o distribuidores mayoristas del software a fin de establecer las mejores condiciones técnicas y económicas para Quito Turismo, de acuerdo a 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.

	Elaborado por	Revisado por	Aprobado por	
Procedimiento de Soporte y Mantenimiento Informático	Karla Arellano	Alex Lozano	Leonidas Espinosa	

1. OBJETO

El presente documento tiene por objeto regular el procedimiento a seguir para brindar soporte técnico informático por parte del área de sistemas para QUITO TURISMO.

2. ALCANCE

Este procedimiento es aplicable para el soporte informático que se brinda al hardware y software de las oficinas de Quito Turismo, Unidades de Negocio y centros de información.

3. DEFINICIONES

- **Hardware:** corresponde a todas las partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado
- **Software:** equipamiento lógico o soporte lógico de un computador digital, y comprende el conjunto de los componentes lógicos necesarios para hacer posible la realización de una tarea específica;
- **Bienes informáticos:** computadoras de escritorio, computadores portátiles, infocus, teléfonos, impresoras, programas y paquetes informáticos.
- **Soporte Técnico:** El soporte técnico es una asistencia que brinda el área de sistema para que sus clientes internos o externos puedan hacer uso de sus productos y servicios tecnológicos. La finalidad del soporte técnico es ayudar a los usuarios para que puedan resolver ciertos problemas informáticos, donde se brinda soporte de instalación, mantenimiento, desarrollo, soporte técnico, actualización, entre otros.

	Elaborado por	Revisado por	Aprobado por	
Procedimiento de Soporte y Mantenimiento Informático	Karla Arellano	Alex Lozano	Leonidas Espinosa	

4. RESPONSABILIDAD Y AUTORIDAD

FUNCIÓN	RESPONSABILIDAD	ACTIVIDAD
Usuarios internos	• Informar y solicitar soporte informático a través de la herramienta implementada en Quito Turismo OTRS con el fin de poder atender el requerimiento a la brevedad posible.	
Técnicos Informáticos	• Proporcionar soporte técnico. • Responder a las solicitudes de los usuarios internos y externos • Realizar las rutinas de prevención de incidentes • Dar seguimiento a las solicitudes a los requerimientos de los usuarios hasta que se solucione	Mantenimiento y soporte técnico informático
Responsable Informático	• Supervisar la respuesta oportuna a las solicitudes por usuarios internos o externos. • Asegurar que se lleve a cabo las tareas de prevención. • Brindar asistencia en la coordinación de los proyectos especiales • Asegurar que los técnicos registren apropiadamente los datos de reportes • Manejo de cambios y entregas de equipamiento informáticos	La administración de la configuración mejora la eficacia operativa de sistemas y las futuras actividades de

	Elaborado por	Revisado por	Aprobado por	
Procedimiento de Soporte y Mantenimiento Informático	Karla Arellano	Alex Lozano	Leonidas Espinosa	

5. PROCEDIMIENTO

5.1. *Soporte técnico informático*

5.1.1. Instalación de estaciones de trabajo

La instalación de estaciones de trabajo, se refiere a la ubicación o reubicación física de los equipos informáticos necesarios para desempeñar las actividades laborales (cpu, pantalla, teclados, mouse, parlantes, teléfono y configuración de hardware y software).

Para la instalación de las estaciones de trabajo se necesita la notificación por parte de la Jefatura Administrativa donde especifique el lugar dónde se ubicará o reubicará la estación de trabajo del funcionario, y las necesidades detalladas de hardware y software, de ser el caso.

Una estación de trabajo básica tendrá implementado el siguiente hardware y software:

- Instalación eléctrica, de acuerdo a la ubicación
- Instalación de cableados de datos (Internet y telefonía IP)
- CPU básico
- Monitor
- Teclado
- Mouse
- Teléfono de voz IP
- Configuración de software: Software libre, definición de perfiles de usuario, instalación de impresora.

En caso de necesitar otro tipo de hardware o/y software deberá presentar un informe de necesidad a la Gerencia Financiera Administrativa para el análisis correspondiente y la autorización de acuerdo a la normativa legal vigente.

5.1.2. Asignación de claves de usuario y cuentas de correo electrónico

El área de sistemas será la única autorizada para entregar, registrar o crear claves de usuario para el uso y manejo de equipos o sistemas informáticos pertenecientes a QUITO TURISMO. Excepto aquellos

	Elaborado por	Revisado por	Aprobado por	
Procedimiento de Soporte y Mantenimiento Informático	Karla Arellano	Alex Lozano	Leonidas Espinosa	

creados para el uso público que se manejan a través de alias Ej:
info@quito-turismo.gob.ec, comunicacion@quito-turismo.gob.ec.

Esta política aplica para los siguientes casos.

- Creación de correo electrónico organizacional. Ej.: spuga@quito-turismo.gob.ec
- Claves de usuario para computadores personales
- Claves de usuario para el uso, teléfonos y bases celulares

5.1.3. Soporte técnico para el buen uso de equipos y sistemas informáticos

Los usuarios internos (funcionarios), podrán realizar sus solicitudes de soporte técnico informático mediante comunicación telefónica y/o electrónica.

La asistencia informática se registrará virtualmente a través del sistema Help Desk (**Anexo 1: Funcionamiento Help Desk**)

5.1.4. Soporte técnico en eventos planificados dentro o fuera de la oficina.

Las solicitudes de soporte informático antes, durante o después de un evento, dentro o fuera las oficinas, podrán realizarse mediante comunicación telefónica y/o electrónica.

Dicha asistencia informática se registrará virtualmente a través del sistema Help Desk.

Todo soporte técnico referente al funcionamiento de las aplicaciones informáticas creadas para el uso público deberán canalizarse a través de esta área.

5.2. Mantenimiento Informático

Las actividades de mantenimiento a los equipos informáticos que forman parte de Quito Turismo consisten en la reparación de problemas que presenten éstos

	Elaborado por	Revisado por	Aprobado por	
Procedimiento de Soporte y Mantenimiento Informático	Karla Arellano	Alex Lozano	Leonidas Espinosa	

y en la adecuación de los mismos para trabajar sin ningún inconveniente durante toda la vida útil.

a) Periodicidad

Estas actividades se realizarán dos veces al año.

b) Mantenimiento de Software:

- Análisis del rendimiento del equipo
- Instalación (de ser el caso), actualización y ejecución del antivirus
- Escaneo y defragmentación (de ser necesario) del disco duro

Observaciones

Se debe tener mucho cuidado con la información del usuario. De ser posible, y en casos muy puntuales donde la información del usuario es delicada, se debe realizar un respaldo de dicha información antes del mantenimiento.

Inspección de Funcionamiento de Equipos:

Verificar en todas las áreas de aplicación el correcto funcionamiento de todos los equipos, después de lo cual se procede a registrar en la hoja de control.

c) Mantenimiento de Hardware:

- LIMPIEZA TARJETA MADRE
- LIMPIEZA MEMORIA RAM.
- LIMPIEZA COOLER DEL PROCESADOR
- LIMPIEZA DISIPADOR DEL MICRO
- LIMPIEZA DISCO DURO
- LIMPIEZA TARJETA DE VIDEO
- LIMPIEZA FUENTE DE ALIMENTACIÓN
- LIMPIEZA MONITOR
- LIMPIEZA TECLADO
- LIMPIEZA MOUSE
- LIMPIEZA GABINETE
- DESCONEXIÓN DE LOS CABLES
- SEÑALES DE FALLA FÍSICA EN EL DISCO DURO
- LIMPIEZA DE LA UNIDAD ÓPTICA CD-ROM, CD-RW, DVD
- LIMPIEZA DE IMPRESORAS

	Elaborado por	Revisado por	Aprobado por	
Procedimiento de Soporte y Mantenimiento Informático	Karla Arellano	Alex Lozano	Leonidas Espinosa	

5.3. *Uso de equipos informáticos*

Es responsabilidad del área de sistemas, mantener actualizado el inventario de los recursos informáticos que sea propiedad de Quito Turismo.

La protección física de los equipos es responsabilidad de la persona a quien se ha asignado y es su responsabilidad notificar a los responsables informáticos del área de sistemas sobre cualquier novedad en el funcionamiento del equipo o de alguna de sus partes así como de los movimientos a los que pueda ser sometido.

En lo posible, la persona a quien se le ha asignado un equipo informático debe mantenerlo en condiciones de limpieza adecuadas, siendo responsabilidad de los responsables informáticos realizar Contratos de mantenimiento preventivo y correctivo, que se estimen necesarios, con empresas y/o instituciones especializadas.

El área de sistemas programará los mantenimientos preventivos de los equipos informáticos.

Los responsables informáticos serán los encargados de realizar las notificaciones de los daños en los equipos informáticos así como reportar los equipos que se consideren obsoletos para solicitar el inicio del proceso de baja de los inventarios.

Para mantener actualizado el inventario de los bienes, será necesaria la utilización del sistema de Bienes que se encuentra vigente.

Los responsables de informática, entregarán los equipos a los funcionarios de Quito Turismo en condiciones adecuadas de operación y con el software correspondiente para el desenvolvimiento de las tareas del usuario.

Si mediante informe del análisis técnico, se determina que existen equipos subutilizados o equipos que requieren de mayor capacidad para desarrollar las actividades de un área o tarea específica, se procederá con la redistribución de equipos o racionalización de los productos instalados o adquiridos, con la aprobación de la Gerencia Financiera Administrativa.

La Jefatura de Sistemas está facultada para realizar la REDISTRIBUCION INTERNA o EXTERNA de los recursos informáticos y la racionalización de productos determinada en un informe técnico con la aprobación de la Gerencia Financiera Administrativa.

La REDISTRIBUCION de equipos podrá realizarse antes y/o después de la provisión o

	Elaborado por	Revisado por	Aprobado por	
Procedimiento de Soporte y Mantenimiento Informático	Karla Arellano	Alex Lozano	Leonidas Espinosa	

renovación de equipos

El funcionario será el responsable de los recursos informáticos que se le entregue, la instalación de aplicativos no autorizados será de estricta responsabilidad del funcionario, deslindando al área de sistemas de cualquier responsabilidad por el uso de este material.

Anexos:

Hoja de control de mantenimiento informático
Funcionamiento del Sistema Help Desk

REGISTRO DE MANTENIMIENTO INFORMÁTICO
RMI-TIC-_____

LUGAR Y FECHA: _____

USUARIO: _____

ACCIÓN REALIZADA: _____

DETALLE

Descripción	Marca Modelo	# Código QT	# de Serie	ESTADO
Monitor				
Teclado				
Mouse				
Parlantes				
Teléfono				
CPU				
Regulador				
Impresora				
Swich				
Otros				

OBSERVACIONES: Todos los equipos se encuentran operativos al fecha de la instalación	Software	Estado
	Microsoft Windows	
	Microsoft Office	
	Open Office	
	Antivirus	
	Parche	
	Buscadores	
	Otros	

ENTREGA:

RECIBE:

		Gestión de Respaldos Digitales		TI-BK-001	
Departamento:				Fecha:	
Usuario:					
Yo _____ tengo pleno conocimiento que el Dpto. de Sistemas realiza un respaldo planificado de la carpeta _____ y cualquier información que se encuentre fuera de la misma se encuentra bajo mi responsabilidad NOTA: No se respaldan archivos de música y videos como: mp3, mpg, wmv, acc, mp4					
Observaciones:					
_____ Firma Usuario			_____ Sistemas QUITO TURISMO		

		Gestión de Respaldos Digitales		TI-BK-002	
Departamento:				Fecha:	
Usuario:					
Yo _____ Manejo mis backups en un dispositivo externo y tengo pleno conocimiento que los mismos son de mi responsabilidad NOTA: En caso de que sea necesario respaldar algún archivo en los servidores de la empresa utilizare la carpeta asignada por el departamento de sistemas.					
Observaciones:					
_____ Firma Usuario			_____ Sistemas QUITO TURISMO		



v.1.0

REVISADO POR:

APROBADO POR:

[illegible]