RESOLUCIÓN Nro. GPI-NA-P-02-2023.

Abg. Pablo Aníbal Jurado Moreno
PREFECTO DE LA PROVINCIA DE IMBABURA

Considerando:

Que, el artículo 66 de la Constitución de la República del Ecuador establece "*Se reconoce y garantizará a las personas:*

(…)
19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.
(…)";

Que, el artículo 227 de la Constitución de la República del Ecuador, preceptúa que "*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 238 de Ia Constitución de la República del Ecuador establece que: "*Los gobiernos autónomos descentralizados gozarán de autonomía política, administrativa y financiera (…);*

Que, el artículo 314 de Ia Constitución de la República del Ecuador establece: "*El Estado garantizará que los servicios públicos y su provisión respondan a los principios de obligatoriedad, generalidad, uniformidad, eficiencia, responsabilidad, universalidad, accesibilidad, regularidad, continuidad y calidad (...)";*

Que, el artículo 393 de Ia Constitución de la República del Ecuador establece: "*El Estado garantizará la seguridad humana a través de políticas y acciones integradas, para asegurar la convivencia pacífica de las personas, promover una cultura de paz y prevenir las formas de violencia y discriminación y la comisión de infracciones y delitos. La planificación y aplicación de estas políticas se encargará a órganos especializados en los diferentes niveles de gobierno (...)*";

Que, el artículo 5 del Código Orgánico de Organización Territorial, Autonomía y Descentralización, preceptúa que "*La autonomía política, administrativa y financiera de los gobiernos autónomos descentralizados y regímenes especiales previstos en la Constitución comprende el derecho y la capacidad efectiva de estos niveles de gobierno para regirse mediante normas y órganos de gobierno propios, en sus respectivas circunscripciones territoriales, bajo su responsabilidad, sin intervención de otro nivel de gobierno y en beneficio de sus habitantes (...)*";

Que, el artículo 361 del Código Orgánico de Organización Territorial, Autonomía y Descentralización dispone que, en relación con la prestación de servicios, los gobiernos autónomos descentralizados, con el apoyo de sus respectivas entidades asociativas, emprenderán un proceso progresivo de aplicación de los sistemas de gobierno y democracia digital, aprovechando las tecnologías disponibles;

Que, el artículo 54 del Código Orgánico Administrativo determina que: "*Los órganos colegiados se integran en número impar y con un mínimo de tres personas naturales o jurídicas. Pueden ser permanentes o temporales. Ejercen únicamente las competencias que se les atribuya en el acto de creación*";

Que, el artículo 130 del Código Orgánico Administrativo, respecto de la competencia normativa de carácter administrativo, dispone: "*Las máximas autoridades administrativas tienen competencia normativa de carácter administrativo únicamente para regular los asuntos internos del órgano a su cargo, salvo los casos en los que la ley prevea esta competencia para la máxima autoridad legislativa de una administración pública. La competencia regulatoria de las actuaciones de las personas debe estar expresamente atribuida en la ley*";

Que, el artículo 76 de la Ley Orgánica de Telecomunicaciones en referencia a las medidas técnicas de seguridad e invulnerabilidad dispone que "*Las y los prestadores de servicios ya sea que usen red propia o la de un tercero, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes. Dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente*";

Que, el artículo 38 de la Ley Orgánica de Protección de Datos Personales respecto de las medidas de seguridad en el ámbito del sector público, dispone que el mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deben implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales;

Que, el artículo 9 de la Ley Orgánica de la Controlaría General del Estado establece que: "*El control interno (…) proporciona seguridad razonable de que se protegen los recursos públicos para alcanzar los objetivos institucionales. Constituyen elementos del control interno: el entorno de control, la organización, la idoneidad del personal, el cumplimiento de los objetivos institucionales, los riesgos institucionales y las medidas adoptadas para afrontarlos, el sistema de información, el cumplimiento de las normas jurídicas y técnicas y la corrección oportuna de las deficiencias de control*";

Que, la Contraloría General del Estado mediante Acuerdo N°. 039-CG, publicado en el Suplemento del Registro Oficial N° 87, del 14 de diciembre de 2009, expidió las Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que dispongan de Recursos Públicos;

Que, la Norma de Control Interno "*100-01 Control Interno*", dispone que el control interno será responsabilidad de cada institución del Estado y de las personas jurídicas de derecho privado que dispongan de recursos públicos y tendrá como finalidad crear las condiciones para el ejercicio del control;

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

Que, la Norma de Control Interno "*100-03 Responsables del control interno*", dispone que el diseño, establecimiento, mantenimiento, funcionamiento, perfeccionamiento, y evaluación del control interno es responsabilidad de la máxima autoridad, de los directivos y demás servidoras y servidores de la entidad, de acuerdo con sus competencias;

Que, las Normas de Control Interno "*300 EVALUACIÓN DEL RIESGO*", señala que "*La máxima autoridad establecerá los mecanismos necesarios para identificar, analizar y tratar los riesgos a los que está expuesta la organización para el logro de sus objetivos.*

El riesgo es la probabilidad de ocurrencia de un evento no deseado que podría perjudicar o afectar adversamente a la entidad o su entorno. La máxima autoridad, el nivel directivo y todo el personal de la entidad serán responsables de efectuar el proceso de administración de riesgos, que implica la metodología, estrategias, técnicas y procedimientos, a través de los cuales las unidades administrativas identificarán, analizarán y tratarán los potenciales eventos que pudieran afectar la ejecución de sus procesos y el logro de sus objetivos";

Que, por su parte la norma "*410-04 Políticas y procedimientos*", del mismo cuerpo normativo, dispone que *"(...) Temas como la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, entre otros, serán considerados dentro de las políticas y procedimientos a definir, los cuales además, estarán alineados con las leyes conexas emitidas por los organismos competentes y estándares de tecnología de información (...)*";

Que, la norma de control interno "*500-01 Controles sobre sistemas de información*" dispone que "*Los sistemas de información contarán con controles adecuados para garantizar confiabilidad, seguridad y una clara administración de los niveles de acceso a la información y datos sensibles*.

En función de la naturaleza y tamaño de la entidad, los sistemas de información serán manuales o automatizados, estarán constituidos por los métodos establecidos para registrar, procesar, resumir e informar sobre las operaciones administrativas y financieras de una entidad y mantendrán controles apropiados que garanticen la integridad y confiabilidad de la información.

La utilización de sistemas automatizados para procesar la información implica varios riesgos que necesitan ser considerados por la administración de la entidad. Estos riesgos están asociados especialmente con los cambios tecnológicos por lo que se deben establecer controles generales, de aplicación y de operación que garanticen la protección de la información según su grado de sensibilidad y confidencialidad, así como su disponibilidad, accesibilidad y oportunidad.

Las servidoras y servidores a cuyo cargo se encuentre la administración de los sistemas de información, establecerán los controles pertinentes para que garanticen razonablemente la calidad de la información y de la comunicación";

Que, la Sección Tercera del Código Orgánico Integral Penal, COIP, respecto de los Delitos contra la seguridad de los activos de los sistemas de información y comunicación, establece sanciones con pena privativa de libertad para delitos como la revelación ilegal de base de datos, interceptación ilegal de datos, transferencia electrónica de activo patrimonial, ataque a la integridad de sistemas informáticos, delitos contra la

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

información pública reservada legalmente, y el acceso no consentido a un sistema informático, telemático o de telecomunicaciones;

Que, el artículo 2 de la Ley de Seguridad Pública y del Estado, respecto de los ámbitos de la ley, establece que: "*Al amparo de esta ley se establecerán e implementarán políticas, planes, estrategias y acciones oportunas para garantizar la soberanía e integridad territorial, la seguridad de las personas, comunidades, pueblos, nacionalidades y colectivos, e instituciones, la convivencia ciudadana de una manera integral, multidimensional, permanente, la complementariedad entre lo público y lo privado, la iniciativa y aporte ciudadanos, y se establecerán estrategias de prevención para tiempos de crisis o grave conmoción social.*

Se protegerá el patrimonio cultural, la diversidad biológica, los recursos genéticos, los recursos naturales, la calidad de vida ciudadana, la soberanía alimentaria; y en el ámbito de la seguridad del Estado la protección y control de los riesgos tecnológicos y científicos, la tecnología e industria militar, el material bélico, tenencia y porte de armas, materiales, sustancias biológicas y radioactivas, etc.";

Que, el artículo de la Ley Orgánica de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, respecto de la Confidencialidad y reserva, reglamenta que: "*Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia (…)";*

Que, según la normativa de Control Interno y de acuerdo con las observaciones y recomendaciones emitidas por la Contraloría General del Estado, es imperativa la aprobación y aplicación de las políticas de seguridad de la información;

Que, en cumplimiento de la base legal y normativa precitadas, así como de las observaciones y recomendaciones efectuadas por el Órgano de Control del Estado, es preciso que el Gobierno Autónomo Descentralizado Provincial de Imbabura (GPI) apruebe y disponga la aplicación de las políticas de seguridad de la información, anexas a la presente resolución.

En ejercicio de sus atribuciones y facultades legales previstas en el artículo 50 del Código Orgánico de Organización Territorial, Autonomía y Descentralización, COOTAD:

RESUELVE:

ESTABLECER LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO PROVINCIAL DE IMBABURA.

Artículo. 1.- Objeto. – La presente Resolución tiene por objeto establecer las Políticas de Seguridad de la Información del Gobierno Autónomo Descentralizado Provincial de Imbabura, como marco normativo para la gestión de la información institucional, entendida como la información generada y custodiada tanto de manera física como en medios electrónicos.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

Artículo. 2.- Ámbito. – Las disposiciones establecidas en esta Resolución son aplicables en la gestión interna; y, serán de obligatorio cumplimiento para los servidores públicos y trabajadores de la Institución.

DISPOSICIONES GENERALES

PRIMERA. - La Secretaría General, será la responsable de difundir la presente resolución a los servidores y trabajadores del GAD Provincial de Imbabura, a través de los canales institucionales.

SEGUNDA. – El Oficial de Seguridad de la Información será responsable de la socialización, control y cumplimiento de la presente resolución, y reportará su incumplimiento a la Máxima Autoridad de la Institución, para los fines pertinentes.

DISPOSICIONES FINALES

PRIMERA. - La presente Resolución entrará en vigencia a partir de su suscripción.

Dado en la ciudad de Ibarra, en el despacho de la Prefectura de Imbabura, a los diez días del mes de febrero del año 2023.

Firmado electrónicamente por:
PABLO ANIBAL JURADO MORENO

Abg. Pablo Aníbal Jurado Moreno
PREFECTO DE IMBABURA

CERTIFICO. - Que, la presente Resolución fue dictada y suscrita por el señor Prefecto de Imbabura, a los diez días del mes de febrero del año 2023.

Firmado electrónicamente por:
FERNANDO JAVIER MORENO BENAVIDES

Abg. Fernando Moreno Benavides
SECRETARIO GENERAL

Elaborado por: OSI

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

PREFECTURA DE IMBABURA

Imbabura Geoparque Mundial

GOBIERNO PROVINCIAL DE IMBABURA

REGLAMENTO INTERNO DE CREACIÓN Y FUNCIONAMIENTO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

RESOLUCIÓN ADMINISTRATIVA
Nro. GPI-NA-P-53-2022
12 páginas
Ibarra, 04 de octubre de 2022

ACTA DE CONFORMACIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (CSI), NOMBRAMIENTO DEL PRESIDENTE DEL CSI, DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN (OSI) Y APROBACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

ACTA Nro. 01-CSI-GPI- 2022
4 páginas
Ibarra, 04 de octubre de 2022

SUMARIO:

GPI-NA-P-53-2022

Confórmese el Comité de Seguridad de la Información del Gobierno Autónomo Descentralizado Provincial de Imbabura, como instancia de la gestión institucional encargada de garantizar y facilitar la implementación de las iniciativas de seguridad de la información de la institución, entendida como la información generada y custodiada tanto de manera física como electrónica.

ACTA Nro. 01-CSI-GPI- 2022

SEGUNDA. El Comité de Seguridad de la Información estará presidido por el delegado del Prefecto, el Ing. Carlos Ernesto Merizalde Leiton.

TERCERA. Se designa de forma temporal como Oficial de Seguridad de la Información a la Ing. Diana Elizabeth Coba Yépez.

CUARTA. Se aprueba las Políticas de Seguridad.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La Constitución de la República del Ecuador garantiza la libre comunicación de las personas, la inviolabilidad de la información, la protección de los datos personales y el derecho a la intimidad, en concordancia con la Ley Orgánica de Telecomunicaciones y la Ley de Protección de Datos Personales. Así también garantiza la seguridad integral y la prevención de riesgos y amenazas de todo orden, en concordancia con la Ley de Seguridad Pública y del Estado.
Confianza en la gestión de la información.

Contenido

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

1. CONTEXTO

Las Políticas van orientadas a la protección de los activos de información, estos pueden ser primarios y de soporte:

Activos Primarios

Son los activos esenciales para el desarrollo de las funciones del Gobierno Provincial de Imbabura, en esta categoría se catalogan: La información, los procesos y procedimientos.

Activos de Soporte

En esta categoría se clasifican los activos que permiten dar tratamiento a la información atendiendo a las recomendaciones que formulan las normas técnicas de gestión de la seguridad de la información, se destacan:

- El Hardware. En esta sección encontramos todo dispositivo físico como computadores portátiles tabletas, teléfonos inteligentes, estaciones de trabajo y demás equipos de procesamiento de información, impresoras, scanner, cámaras fotográficas, lectoras de datos, discos extraíbles, entre otros.

- El Software. Sistemas para el procesamiento de información como: utilitarios para el usuario final, correo electrónico, antivirus, herramientas de desarrollo de software, software para control de inventarios, sistemas financieros, sistemas para gestión de talento humano, software para gestión de bases de datos, sitios web, etc.

- La Infraestructura de servidores y seguridades. Toda la infraestructura del centro de datos como UPS, aire acondicionado, control de acceso, sensores de humedad, temperatura, servidores, sistemas de almacenamiento, etc.

- La Infraestructura de redes. En esta categoría están los medios de transmisión que soportan a las redes y los equipos activos que permiten la transmisión de datos sobre las redes.

- El Personal. Funcionarios y trabajadores del GAD Provincial de Imbabura.

- La Infraestructura física. Edificios, maquinaria, equipamiento y menaje de la institución.

- Y finalmente la Estructura Organizacional del GPI.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

La generación de procedimientos e instructivos, así como la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información, se encaminan a asegurar que la información que se custodia y que es generada por parte de los servidores públicos y/o trabajadores, estén acordes a los siguientes objetivos de seguridad de la información:

- Minimizar el riesgo de los procesos críticos de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Cumplir con las normas de control interno de la Contraloría General del Estado (CGE) y ley aplicable vigente.
- Mantener la confianza de los servidores públicos, trabajadores, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los servidores públicos, trabajadores, aprendices, practicantes y ciudadanía que hace uso de los servicios que presta el GPI.
- Garantizar la continuidad operativa frente a incidentes.

Este documento establece las políticas de seguridad de la información, las cuales tienen el objetivo de entregar lineamientos de seguridad claros para optimizar y mejorar los procesos, de forma que se contribuya al cumplimiento de la misión y objetivos estratégicos del GPI, con eficiencia operacional y seguridad de la información (confiabilidad, disponibilidad e integridad).

2. ALCANCE

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

El presente documento es aplicable a todos los colaboradores del GPI: servidores públicos y/o trabajadores, consultores, contratistas, practicantes, incluyendo a todo el personal externo que en algún momento cuente con acceso a los recursos informáticos o información del GPI.

Las políticas definidas deberán estar en concordancia con los estatutos y reglamentos internos del GPI, asegurando la seguridad y optimización de los sistemas tecnológicos, brindándole al usuario garantías básicas.

3. OBJETIVO

Brindar la información necesaria a los servidores públicos y/o trabajadores acerca de las normas y mecanismos que deben cumplir y utilizar para proteger los activos de información primarios y de soporte.

Planear, organizar, dirigir y controlar las actividades para mantener y garantizar la confiabilidad, disponibilidad e integridad de los activos de información del GPI.

3.1. Objetivos específicos

1. Establecer las políticas para resguardo y garantía de acceso apropiado de la información.
2. Vigilar que el GPI cuente con los recursos de software legal necesarios para su funcionamiento.
3. Adquirir tecnología acorde a las necesidades del GPI aprovechando al máximo, las capacidades de los servidores públicos y/o trabajadores, así como el presupuesto asignado para esta materia.

4. PRINCIPIOS DE SEGURIDAD

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

Confidencialidad: La información sólo podrá ser accedida, modificada y/o eliminada por quienes estén autorizados para ello.

Disponibilidad: La información deberá estar accesible siempre que se requiera.

Integridad: La información deberá preservar su veracidad y fidelidad a la fuente, independientemente del lugar y de la forma de almacenamiento y transmisión.

5. OBLIGACIONES

Las políticas de seguridad de la información son de obligatorio cumplimiento para todos los servidores públicos y trabajadores, permanentes o que tengan acceso a la información y a los servicios tecnológicos del GPI.

6. COMPROMISO DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (CSI)

El Comité de Seguridad de la Información encabezado por la máxima autoridad del GPI, declaran ser responsables con la información, un bien catalogado como el activo más importante dentro de la institución, por lo tanto, manifiestan su total compromiso con el establecimiento, implementación y gestión de un Sistema de Seguridad de la Información que incluye el diseño e implementación de un plan de continuidad y recuperación ante desastres.

El CSI demostrará su compromiso a través de:

- La revisión y aprobación de las políticas contenidas en este documento.
- La socialización de estas políticas a todos los servidores públicos y trabajadores del GPI.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de Seguridad de la Información.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

7. DEFINICIONES

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

SERCOP: Entidad del estado la cual entrega los lineamientos para que todas las instituciones del estado puedan realizar las adquisiciones de los bienes y servicios.

MINTEL: Ministerio de Telecomunicaciones y de la sociedad de la Información, ente rector de Gobierno Electrónico.

CGE: Organismo de control del Estado encargado de realizar auditoría a todos los procesos que se realiza para ejecución de actividades a todas las Instituciones del Estado sean estas autónomas o dependientes de otras.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, locación/edificio, personas) que tenga valor para la organización. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Confidencialidad: Es la garantía de que la información no generada de la institución no está disponible o divulgada a personas, entidades o procesos no autorizados.

Integridad: Es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente.

Disponibilidad: Es la garantía de que los servidores públicos y trabajadores autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

Seguridad perimetral: La seguridad perimetral es un concepto emergente asume la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusos en instalaciones especialmente sensibles.

Plan de recuperación de desastres (DRP): Se entiende por plan de contingencia el conjunto de procedimientos alternativos a la operación normal en una organización, cuyo objetivo principal es permitir el continuo funcionamiento y desarrollo normal de sus operaciones, preparándose para superar cualquier eventualidad ante accidentes de origen interno o externo, que ocasionen pérdidas importantes de información.

RPO (Recovery Point Objetive): Se refiere al volumen de datos en riesgo de pérdida que la organización considera tolerable. ¿Las transacciones de cuánto tiempo estamos dispuestos a perder, o a tener que reintroducir al sistema?

RTO (Recovery Time Objetive): Expresa el tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad operativa.

CSI (Comité de Seguridad de la Información): Es el comité responsable de la confiabilidad, disponibilidad e integridad de la información de los activos de información que tiene el GPI mediante la aprobación de políticas de seguridad y la implementación del esquema de seguridad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información.

OSI: Oficial de Seguridad de la Información.

8. ASPECTOS REGLAMENTARIOS

1. Registro Oficial Suplemento No. 459 de 26 de mayo de 2021 se publicó la Ley Orgánica de Protección de Datos Personales.
2. Registro Oficial Suplemento 87 de 14-dic.-2009, la Contraloría General del Estado publica las normas de control interno para las entidades, organismos

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos. Normas de control interno 100, 300, 410 y 500.

3. Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27001, para la Gestión de la Seguridad de la Información, en las que está basado el EGSI (Esquema Gubernamental de Seguridad de la Información) expedido por el MINTEL.
4. Código Orgánico Integral Penal (COIP), Sección tercera “Delitos contra la seguridad de los activos de los sistemas de información y comunicación”.

9. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se desarrollan las políticas específicas asociadas directamente a los objetivos de control del Esquema de Gestión de Seguridad de la Información emitido por el MINTEL, basado en las normas ecuatorianas NTE INEN-ISO/IEC 27001 de seguridad de la Información, que especifican la conducta aceptada por el GPI como mecanismo gubernamental de seguridad de la información para la gestión de su información.

9.1. POLÍTICAS GENERALES

9.1.1. Los recursos informáticos sólo pueden ser utilizados por los colaboradores del GPI: servidores públicos o trabajadores, practicantes, pasantes y contratistas que cuentan con la debida autorización de la Máxima Autoridad, o de la Dirección General a la cual pertenecen o están vinculados.

9.1.2. Las políticas de seguridad de la Información serán aprobadas por el Comité de Seguridad de la información Comité de Seguridad de la Información.

9.1.3. La socialización de la Políticas de Seguridad de la información será viabilizada por el Oficial de Seguridad de la Información, a través de los medios digitales existentes en la institución o mediante procesos de capacitación continua y de inducción cuando exista incorporación de nuevos servidores públicos y/o trabajadores; de igual forma se

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

notificará a todo el personal cuando existan cambios o mejoras en las políticas.

9.1.4. El desarrollo de nuevos proyectos que involucren el uso de recursos tecnológicos será realizado y liderado por la Dirección General de TI.

9.1.5. La adquisición de bienes y/o servicios, donde se incluyan equipos informáticos como parte integrante o complementaria de otros procesos, será realizada y validada por la Dirección General de TI.

9.1.6. La Dirección General de TI autorizará la conexión de cualquier elemento electrónico en la red de datos interna del GPI en base a autorización del Director General de TI y de la Dirección a la cual pertenece el solicitante de este requerimiento presentando su respectiva justificación.

9.1.7. La Dirección General de TI verificará que los equipos tecnológicos tengan: disponibilidad de energía eléctrica, cableado estructurado y mantengan las condiciones físicas aceptables y adecuadas de temperatura, entre otros para su normal funcionamiento de acuerdo con las especificaciones técnicas del fabricante, siempre que se cumplan los ítems 9.1.4 al 9.1.6.

9.1.8. La Dirección General de TI debe velar por la debida privacidad y confidencialidad de los datos personales registrados de los servidores públicos, trabajadores o usuarios ciudadanos en los sistemas de información del GPI y solo se permitirá el acceso a ésta, previo consentimiento de la parte involucrada o por pedido de una autoridad competente, dentro de un proceso legal, si fuera el caso, solicitado de manera formal y avalado por la Dirección Requirente y la Dirección propietaria de la información, presentando el respectivo informe de justificación y las firmas de autorización para éste acceso.

9.1.9. Todo servidor público y trabajador que genere o consuma información del GPI, tiene la responsabilidad de respaldarla, siguiendo los lineamientos entregados por la Dirección General de TI para este efecto.

9.1.10. El acceso a los servicios ofrecidos por la Dirección General de TI, para el consumo de información, navegación, etc., se solicitará de

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

manera formal a través del sistema de gestión documental con la respectiva justificación y responsabilidad a la Dirección General requirente, requisito principal es la firma del acuerdo de confidencialidad aprobado y publicado para este fin.

9.1.11. La Dirección General de TI dentro de sus responsabilidades está la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información digitalizados, el mismo que se lo realizará de forma automatizada en general.

9.2. RESPONSABILIDADES DE SERVIDORES PÚBLICOS Y TRABAJADORES

9.2.1. El equipo asignado es de uso personal por lo tanto cada servidor público o trabajador es responsable de este y del buen uso que le dé.

9.2.2. Los servidores públicos o trabajadores tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.

9.2.3. No realizar cambios en las configuraciones de hardware o software instalado en los equipos de cómputo ya que este solo lo realiza el área de tecnología informática.

9.2.4. No divulgar la clave de acceso ya que esta es de uso personal e intransferible, como consecuencia se entiende para todos los efectos que solo la conoce el responsable del equipo.

9.2.5. El usuario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo a la Dirección General de TI lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática, incidente que deberá ser registrado en el módulo de

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

"Mesa de Ayuda", del GRP institucional, con la categoría de "Alerta de Seguridad".

9.2.6. Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin autorización, el usuario deberá notificar al Oficial de Seguridad de la Información, vía correo electrónico. Quien a su vez registrará el incidente para su verificación, mitigación y/o sanción, de acuerdo con el impacto y posterior monitoreo de alertas.

9.2.7. Cualquier incidente generado durante la utilización u operación de los activos de soporte de información debe ser reportado en el módulo de "Mesa de Ayuda", del GRP institucional, con la categoría de "Alerta de Seguridad".

9.2.8. El servidor público o trabajador tiene la obligación de almacenar la información según el proceso establecido por la Dirección General de TI.

9.2.9. Los servidores públicos o trabajadores no deben interferir en los procesos computacionales del GPI, ni en el buen funcionamiento de los servicios y recursos de estos, mediante acciones deliberadas que disminuyan el desempeño, la capacidad o la seguridad de los equipos instalados. Se considerará justa causa de terminación del contrato el manejo indebido de los sistemas de tecnología.

9.2.10. Está prohibido mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, o retirar sellos de estos. Lo anterior es responsabilidad exclusiva de la Dirección General de TI, por lo tanto, en caso de requerir este servicio deberá solicitarlo a través del módulo de "Mesa de ayuda".

9.2.11. Todos los ordenadores y equipos portátiles situados en lugares abiertos de oficina deberán estar dotados con dispositivos antihurto (candados de seguridad).

9.2.12. Es responsabilidad del usuario hacer uso del antivirus antes de copiar o ejecutar archivos para que los equipos no sean infectados. Los servidores públicos o trabajadores pueden pedir apoyo al departamento de sistemas para el uso de antivirus.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.2.13. Los servidores públicos o trabajadores no pueden asignar equipos tecnológicos que están bajo su responsabilidad a otros compañeros de trabajo, en el caso de no necesitarlos deben seguir el procedimiento estipulado para la entrega del equipo a bodega bajo los procesos establecidos.

9.2.14. Es obligación del servidor público o trabajador seguir los lineamientos de uso de credenciales establecido por la Dirección General de TI.

9.2.15. Está prohibido la instalación de software no autorizado por el GPI, es responsabilidad el controlar y reportar, cuando se detecte una acción de esta índole.

9.2.16. El correo electrónico institucional, será empleado únicamente para comunicaciones del servidor público o trabajador, que atiendan al desenvolvimiento de sus actividades dentro del GPI y no para gestiones de tipo personal (registro de cuentas bancarias, redes sociales, facturas..).

Siendo el principal medio de comunicación institucional. Es responsabilidad del usuario las comunicaciones que emite a través de este medio, recordando que tienen valor probatorio dentro de un proceso legal. Los mensajes transmitidos no pueden comprometer la confidencialidad e integridad de la información.

Tomar en cuenta que el envío de copias de archivos dentro de la red interna del GPI, puede generar información duplicada innecesaria, que puede comprometer la integridad del documento o archivo original.

Está prohibido la apertura de correos electrónicos de fuentes desconocidas e inclusive la apertura de los documentos o archivos adjuntos, ya que puedan comprometer el equipo del usuario y la red de la institución.

9.2.17. En la actualidad, los virus pueden dispersarse fácilmente no sólo en los archivos de programa, sino también en los archivos de datos. Dentro de los síntomas de infección de virus, se encuentran un tiempo

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

de respuesta más lento, pérdida inexplicable de archivos, cambio de fechas de archivos, aumento del tamaño de los archivos y fallo total de los ordenadores personales y servidores.

Con el fin de asegurar un servicio continuado tanto para los ordenadores, como para los sistemas en red, todos los usuarios de ordenadores personales deberán tener una versión actualizada del software antivirus aprobado instalado en sus ordenadores. Estos sistemas de detección de virus deben emplearse para comprobar todos los archivos y software que provienen tanto de terceras personas como de otros grupos dentro de la institución. La comprobación pertinente deberá realizarse antes de abrir los archivos o ejecutar el software. Los empleados nunca deberán omitir estos sistemas, dado el peligro de infección de virus.

9.2.18. Si un servidor público o trabajador, sospecha de infección de virus, inmediatamente debe dejar de utilizar el ordenador en cuestión y ponerse en contacto con el módulo de “Mesa de ayuda”, para que el área de soporte realice la tarea de mitigación, reduciendo al máximo la destrucción de información, así como el tiempo de caída del sistema. Además, el ordenador deberá ser aislado de los sistemas en red. Los medios de almacenamiento que hayan sido utilizados en el ordenador infectado no deben ser utilizados en ningún otro ordenador hasta que el virus haya sido eliminado. Los usuarios nunca deben intentar eliminar el virus por sí mismos.

9.2.19. Está prohibido el ingreso de sesión dentro de las máquinas de propiedad de GPI con cuentas de usuario que no son de propiedad de los servidores públicos o trabajadores entregados por la Dirección General de TI.

9.2.20. Los servidores públicos o trabajadores deben bloquear los equipos informáticos designados para su uso cuando no estén presentes en sus puestos de trabajo, de forma que no sean accesibles sin el ingreso de una contraseña.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.2.21. Los servidores públicos o trabajadores deberán pedir autorización a sus Direcciones y a la Dirección General de TI para hacer uso de sus computadores personales en la red interna de datos del GPI.

9.3. LICENCIAMIENTO DE SOFTWARE

9.3.1. Todo software adquirido para el uso del GPI debe estar debidamente licenciado y es responsabilidad directa de la Dirección General de TI hacer cumplir con la norma.

9.3.2. La adquisición de cualquier software debe tener el aval y aprobación de la Dirección General de TI.

9.3.3. La Dirección General de TI debe realizar al menos una vez al año inspecciones a los equipos del GPI para asegurarse que el software instalado en los computadores se encuentre debidamente licenciado.

9.3.4. Todos los productos de software que se utilicen deberán contar con la licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos que no cuenten con el debido licenciamiento.

9.4. DERECHOS DE AUTOR

9.4.1. Para asegurarse de no violar los derechos de autor, no está permitido a los servidores públicos o trabajadores instalar programas en los computadores del GPI bajo ninguna circunstancia sin la autorización escrita de la Dirección General de TI.

9.4.2. Está prohibido cargar o descargar programas informáticos no autorizados de Internet, (Ej. Skype, TeamViewer, etc.).

9.4.3. Está prohibido realizar intercambios o descargas de archivos digitales que no son productivos para las Dirección Generales a la cual

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

pertenecen dentro del GPI, e incluso mantener archivos o programas de los cuales no es el autor o bien no posee los derechos de distribución del mismo.

9.4.4. Si un servidor público o trabajador desea utilizar programas informáticos autorizados por el GPI en su hogar, debe consultar a la Dirección General de TI para asegurarse de que ese uso esté permitido por la licencia del fabricante.

9.4.5. Los servidores públicos o trabajadores utilizarán los programas informáticos sólo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de los programas informáticos comerciales sobre computadores de propiedad del GPI.

9.4.6. Según las leyes vigentes de derechos de autor, las personas involucradas en la reproducción ilegal de programas informáticos pueden estar sujetas a sanciones civiles y penales, incluidas multas y prisión. No se permite la duplicación ilegal de programas informáticos sobre los recursos de hardware y software del GPI.

9.4.7. En el caso de desarrollo de software en la institución, los servidores públicos o quienes cumplan servicios profesionales ceden exclusivamente al GPI los derechos de patentes, reproducción e inventos u otra propiedad intelectual que ellos originen y/o desarrollen. Todos los programas y documentación generada o facilitada por los desarrolladores para beneficio del GPI se consideran propiedad de la institución. La institución asume todos los derechos legales de propiedad de los contenidos de todos los sistemas informáticos bajo su control. Por lo tanto, la institución se reserva el derecho de acceso y uso de su información.

9.4.8. Para el caso de software de terceros se deberá solicitar el Certificado de Registro de Programa de Ordenador y Base de Datos, expedido por la institución de registro de derechos de autor a nivel nacional.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.5. SOPORTE

9.5.1. Todo requerimiento de soporte técnico de equipos informáticos, software propio o de terceros, telefonía y demás bienes y servicios tecnológicos institucionales, se realizará a través del módulo de “Mesa de ayuda” del GRP institucional.

9.5.2. Para las tareas de soporte técnico, el GPI pondrá a disposición del servicio de mesa de ayuda, servidores públicos que tendrán las siguientes atribuciones y/o responsabilidades:

- ✓ Podrán ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del custodio del equipo de cómputo, y con los programas remotos autorizados por la Dirección General de TI (AnyDesk).
- ✓ Deben actualizar la información de los recursos de cómputo del GPI, cada vez que se adquiera e instale equipos o software.
- ✓ Deben auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la inexistencia de archivos no autorizados, música, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.
- ✓ Realizar la instalación o adaptación de sistemas de cómputo de acuerdo con los lineamientos en materia de seguridad, establecidos en los ítems anteriores.
- ✓ Reportar a la Dirección de TI los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo en el módulo de “Mesa de ayuda” o vía correo electrónico al Oficial de Seguridad de la Información.

9.6. EQUIPO DE COMPUTO

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.6.1. Para el correcto funcionamiento del equipo de cómputo deberá realizarse como mínimo mantenimientos preventivos cada año, de acuerdo con el plan de mantenimiento preventivo elaborado por la Dirección General de TI.

9.6.2. La Dirección General de TI será la responsable de asignar, preparar y distribuir el equipo de cómputo a los servidores públicos o trabajadores de GPI.

9.6.3. La Dirección General de TI de acuerdo con la normativa y leyes existentes deberá determinar la vida útil de los equipos de informática, con la finalidad de optimizar su uso.

9.6.4. La Dirección General de TI instalará todas las aplicaciones de los equipos y programas informáticos utilizados por el GPI.

9.6.5. La Dirección General de TI verificará y exigirá que los proveedores de soluciones tecnológicas suministren los manuales e instructivos correspondientes al funcionamiento de los equipos o programas especializados, como transferencia tecnológica de los bienes y/o servicios.

9.7. DESARROLLOS DE SISTEMAS DE INFORMACIÓN

9.7.1. Para los proyectos de desarrollo de sistemas de información de terceros, deberá seguirse el procedimiento de compras y contratación pública determinado por los lineamientos del SERCOP, y los reglamentos y leyes que rigen dentro de la Contraloría General del Estado que permita las condiciones de la contratación, considerar las tecnologías a utilizar y los mecanismos de control a establecerse.

9.7.2. Las solicitudes de nuevos sistemas de información o aplicaciones a desarrollar en la modalidad de externalización o con personal propio, deberán ser formalmente presentadas por la Dirección General de TI, en forma escrita e indicando en éstas los requerimientos generales por cubrir, mediante el cual la Jefatura de Software y Web realizará un

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

estudio de prefactibilidad en el cual se determinarán tiempo y costos de la solicitud, información que permitirá definir por parte de la Dirección si es viable o no dicho requerimiento.

Estos requerimientos deberán contener la especificación tanto de riesgos, como de controles de seguridad (incluyendo acceso a los sistemas de seguridad y planes de emergencia). La especificación debe formar parte de un acuerdo entre la unidad requirente y la Jefatura de Software y Web.

9.7.3. El control y monitoreo del avance de proyectos de desarrollo o de adquisición de nuevos sistemas de información por “outsourcing” o recursos propios del GPI, estará a cargo de la Dirección General de TI.

9.7.4. Todos los sistemas desarrollados emplearán control documentado del proceso de cambios.

9.7.5. Toda actividad de producción, desarrollo y mantenimiento de software llevado a cabo por empleados de la institución debe cumplir con los estándares, procedimientos y otras normativas del Departamento General de Tecnologías de la Información. Entre otros, estos estándares incluyen los procedimientos de evaluación, formación y documentación adecuados.

9.7.6. Toda aplicación desarrollada deberá ser probada en su ambiente de preproducción antes de entrar a producción y debe cumplir con todos los requisitos y aprobaciones para pasar a producción.

9.7.7. Bajo ningún concepto los usuarios deberán copiar el software facilitado por la institución en ningún tipo de soporte informático, transferirlo a otro ordenador o entregarlo a terceros sin la correspondiente autorización.

9.7.8. La data que se utilice para ambientes de prueba debe haber pasado por un proceso de enmascaramiento, respetando su estructura, pero garantizando que la información sensible o identificable del ciudadano, empleado o persona jurídica no esté disponible fuera del entorno de producción.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.7.9. La Dirección General de TI será la responsable de generar un proceso para la entrega de los sistemas de información desarrollados por la Jefatura de Software y WEB de manera formal y debidamente documentada a la Jefatura de Operaciones y Servicios, para su administración.

9.7.10. La Dirección General de TI será la responsable de manejar los sistemas, aplicaciones o servicios que son vendidos o desarrollados por proveedores externos de acuerdo con las especificaciones contractuales y a entera satisfacción para que sean administrados y operados por la Jefatura de Operaciones y Servicios.

9.7.11. Con el fin de asegurar la compatibilidad del nuevo software con los ordenadores y sistemas en red de la institución y para facilitar a la dirección el control de licencias, todas las órdenes de compra de software se realizarán a través de la Dirección General de TI.

9.7.12. La Dirección General de TI, estará pendiente de que las empresas contratadas para realizar un desarrollo de sistemas de información, brinden una capacitación adecuada a sus servidores públicos o trabajadores, para el uso y mantenimiento del nuevo sistema de información e incluso a otras áreas de la Dirección General de TI para el mantenimiento del mismo.

9.8. SEGURIDAD

9.8.1. Seguridad del recurso humano

9.8.1.1. La Dirección General de Talento Humano, debe considerar y proyectar dentro de su contratación anual de recursos humanos un aprovisionamiento del presupuesto para la adquisición de los recursos tecnológicos con la respectiva coordinación con la Dirección de TI.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.8.1.2. Todo el personal nuevo que ingrese a la Institución deberá ser notificado a la Dirección General de TI por la Dirección Talento Humano de tal forma que se asigne los recursos correspondientes en base al formulario de requerimientos tecnológicos firmado por la Dirección Solicitante del recurso en el cual se detalla de forma clara el software que va a utilizar y las aplicaciones que necesita para desarrollar su trabajo.

9.8.1.3. El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.

9.8.1.4. Todos los servidores públicos o trabajadores empleados, contratistas y terceras personas deberán devolver todos los activos de información del GPI que tengan a su cargo a la terminación de su empleo, contrato o acuerdo.

9.8.1.5. Todo servidor público o trabajador que hace uso de la Información generada o consumida que corresponde al GPI, tiene la responsabilidad de resguardar o informar a la Dirección General de TI cuando ésta se vea comprometida en lo que respecta a su confiabilidad, integridad y disponibilidad.

9.8.1.6. La Dirección General de Talento Humano, debe comunicar los procesos disciplinarios que tiene el GPI cuando se haya producido un incidente de seguridad por no acatar las políticas de seguridad de la información.

9.8.1.7. La Dirección General de Talento Humano es responsable de tener el perfil de las funciones y responsabilidades de cada uno de los puestos de trabajo definidos en el organigrama de la Institución.

9.8.1.8. Todo servidor público o trabajador debe firmar un acuerdo de confidencialidad, en el que se compromete al buen uso de la información que se genere o consuma a través de sus funciones en el GPI y al cumplimiento de las políticas de seguridad de la información, el mismo tendrá vigencia durante la permanencia de este servidor público o trabajador en la Institución y hasta dos años posteriores al finiquito.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.8.1.9. Los acuerdos de confidencialidad o no divulgación deben considerar los siguientes elementos:

- ✓ Una definición de la información a protegerse.
- ✓ Responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada.
- ✓ Propiedad de la información, propiedad intelectual, y cómo se relaciona esto con la protección de la información confidencial.
- ✓ Uso permitido de la información confidencial y los derechos del firmante para utilizar la información.

Toda la información relacionada con las medidas y políticas de seguridad para ordenadores y sistemas en red de la institución es confidencial, y, por lo tanto, no podrá ser comunicada a personas ajenas al sistema en cuestión, sin el debido permiso de Seguridad Informática.

9.8.1.10. Los proveedores de desarrollos de software externos también estarán sujetos a la firma de un acuerdo de confidencialidad, en el que la entrega de bases de datos de los sistemas en cuestión será considerada como información altamente confidencial.

Motivo por el cual se debe asumir el compromiso irrevocable de que dicha información se mantendrá estrictamente con carácter confidencial y que no será divulgada, vendida, comercializada, publicada, ni revelada de ningún modo a terceros, incluyendo reproducciones de ningún tipo, y que será utilizada únicamente con los fines establecidos en el presente convenio.

Al término del uso de los datos para el fin establecido, éstos deberán ser restituidos al Gobierno Provincial de Imbabura, o dar fe de su destrucción, estableciéndose como plazo un mes, al tiempo que emitirán un certificado firmado por el representante legal en el que se acredite la acción de restitución o destrucción de la información confiada.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.8.2. Centro de datos

9.8.2.1. El acceso físico al centro de datos es restringido y solo personal autorizado por la Dirección General de TI puede tener acceso a él.

9.8.2.2. Todo acceso físico al centro de datos debe ser registrado, identificando a las personas que acceden a éste por lo menos con nombres completos, hora, día, mes, año, actividad que realizaron y su respectiva firma, este registro debe ser realizado de forma manual o automática.

9.8.2.3. El acceso a los servidores del GPI ya sea usando la consola de administración local o una consola de administración remota es restringido al personal autorizado por la Dirección General de TI

9.8.2.4. Se debe realizar un aseo al menos una vez por trimestre, que permita mantener libre de polvo a racks, equipos, aire acondicionado y piso del centro de datos.

9.8.2.5. Verificar y mantener en buen estado contactos e instalaciones eléctricas.

9.8.2.6. El Centro de datos debe mantener la temperatura del aire acondicionado entre 17 a 21 grados centígrados.

9.8.2.7. Debe tener un control de temperatura automático de tal forma que cuando la temperatura suba a más de 21 grados centígrados pueda enviar una alerta a los correos electrónicos del administrador, Jefaturas y el Director General de TI o responsables, con el fin de evitar daños en los equipos o en peores casos incidentes relacionados con fuego.

9.8.2.8. Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.

9.8.2.9. Contar con planes de contingencia que aseguren la continuidad del servicio.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.8.2.10. Contar por lo menos con un sistema de protección de incendios que permita mitigar este a segundos de haber ocurrido el incidente, con el fin de evitar daños en los equipos y pérdida de información.

9.8.2.11. El centro de datos debe contar con un sistema de videovigilancia integrado al sistema de videovigilancia implementado en el GPI.

9.8.2.12. El acceso físico debe contar con sistemas seguros y automáticos, control de accesos, puerta antivandálica, paredes reforzadas.

9.8.3. Seguridad perimetral o red

9.8.3.1. Los equipos electrónicos de gestión e infraestructura de la red del GPI serán instalados, configurados y mantenidos exclusivamente por el área de la Dirección TI.

9.8.3.2. No es permitido a ningún servidor público o trabajador, excepto a los responsables de la Dirección General de TI, manipular los componentes activos de la red (switches, routers, dispositivos inalámbricos, cableado, etc.).

9.8.3.3. La Dirección General de TI es la responsable de proporcionar a los servidores públicos o trabajadores el acceso a los recursos de conectividad.

9.8.3.4. La Institución debe tener una arquitectura de salida a Internet debidamente segmentada que permita la publicación de servicios de Internet de forma segura sin comprometer servicios e información Interna.

9.8.3.5. Todo ambiente de desarrollo, pruebas de aplicaciones desarrolladas, bases de datos, telefonía deben estar debidamente segmentados con el fin de entregar un nivel de seguridad a nivel de capa de aplicación.

9.8.3.6. Todos los componentes de conectividad sean estos Firewalls, Switches, routers, AP, etc. deben tener planes de contingencia que permitan la recuperación de estos servicios en el menor tiempo posible.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.8.3.7. La Dirección General de TI debe tener los diagramas de conexión lógicos y físicos debidamente actualizados.

9.8.3.8. Con el fin de asegurar el cumplimiento de la normativa, las leyes y regulaciones aplicables y la seguridad de sus colaboradores, el GPI se reserva el derecho a inspeccionar en cualquier momento y llevar un seguimiento de todos los sistemas informáticos de la institución. Tal inspección puede tener lugar con o sin el consentimiento, con o sin la presencia de los servidores públicos o trabajadores implicados. Los sistemas informáticos sujetos a inspección incluyen, sin limitación: los archivos de sistema de correo electrónico, archivos del disco duro de ordenadores personales, archivos de buzón de voz, archivos de impresoras, cajones del escritorio y áreas de almacenamiento. Estas inspecciones se llevarán a cabo tras haber sido aprobadas por el Comité de Seguridad de la Información. Dado que los ordenadores y sistemas de la institución se ponen a disposición de sus empleados únicamente para uso operativo de las actividades del cargo en función en la institución, no existe privacidad asociada a información de tipo personal en la información que se almacene o gestione a través de estos sistemas informáticos. La institución además se reserva el derecho de eliminar de sus sistemas informáticos cualquier material que considere ofensivo o potencialmente ilegal.

9.8.3.9. La Dirección General de TI se reserva cualquier derecho a revocar los privilegios de sistemas de cualquier usuario en cualquier momento, cuando se identifique una conducta inapropiada que interfiera con el ritmo habitual y adecuado de los sistemas informáticos de la institución, o que impida a otros utilizar estos sistemas o bien que sea peligroso u ofensivo.

9.8.3.10. Salvo concesión de la correspondiente autorización por parte de Seguridad Informática, los empleados de la institución bajo ningún concepto deberán adquirir, poseer, negociar o utilizar

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

herramientas de hardware o software que pudieran ser empleadas para evaluar o comprometer los sistemas de seguridad informática. Asimismo, sin el permiso adecuado, se prohíbe a los empleados utilizar rastreadores u otro tipo de hardware o software que detecte tráfico de un sistema en red o la actividad de un ordenador. Los incidentes relacionados con la piratería informática, descubrimiento de contraseñas, decodificación de archivos, y otras actividades que supongan una amenaza para las medidas de seguridad, o sean ilegales se considerarán violaciones graves de la normativa interna de la institución. También está terminantemente prohibido el uso de sistemas de baipás que pongan en riesgo los sistemas de protección.

9.8.4. Seguridad de la información

9.8.4.1. Los servidores públicos o trabajadores deben guardar la información en las carpetas asignadas y de acuerdo con las tablas de retención documental, en el proceso que corresponda y de acuerdo con la política de archivo, para garantizar que dicha información sea respaldada.

9.8.4.2. De forma periódica se realizarán respaldos de la información de los servidores públicos o trabajadores de forma automática de la información almacenada en las carpetas designadas por la Dirección General de TI según los mecanismos establecidos en el procedimiento de “seguridad de la información”.

9.8.4.3. Las contraseñas son información confidencial, de uso personal, que viabiliza la autenticación en un recurso en particular, las modificaciones que se lleven a cabo con el usuario son de exclusiva responsabilidad de este, por lo que se debe guardar la información de forma secreta.

9.8.4.4. Los equipos deberán contar con protector de pantallas protegido por contraseña con un tiempo de espera de 5 minutos tras

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

detectar un determinado periodo sin actividad, configurado a través de Active Directory, para evitar accesos no autorizados.

9.8.4.5. Todos los accesos a los programas principales (CRM, GRP, YUPAK, etc.) estarán protegidos mediante un mecanismo de usuario y contraseña. Los usuarios de correo electrónico y Windows estarán integrados al AD, el que también asignará los permisos de navegación en internet.

9.8.4.6. Para la carpeta compartida que dispone cada usuario, se accederá de acuerdo con la matriz de seguridad**.**

9.8.4.7. Los servidores públicos o trabajadores deberán abstenerse de divulgar o compartir sus datos de acceso a los programas y sesiones de Windows.

9.8.4.8. No es responsabilidad de la Dirección General de TI la pérdida de información personal que se encuentre en cada equipo de los usuarios, ya que es responsabilidad del funcionario respaldar dicha información, para lo cual deberá solicitar apoyo a la DGTI para poder salvaguardar su información crítica en los medios establecidos por la institución.

9.8.4.9. Todo acceso a la información del GPI deberá tener las respectivas autorizaciones y accesos, que garanticen seguridad, integridad y confidencialidad en la información almacenada.

9.8.4.10. Toda la información a la que un servidor público o trabajador tiene acceso o que genere como parte de las actividades diarias que realiza en GPI, es propiedad de la Institución y esta no puede ser compartida o divulgada sin autorización, no puede ser adulterada y debe estar siempre disponible, para lo cual se debe contar con un mecanismo de respaldo automático.

9.8.4.11. A excepción de la información generada por la institución y clasificada como pública, toda la información interna debe ser protegida contra su difusión a terceras personas. Sólo se permitirá acceso a la información interna cuando exista una necesidad de su conocimiento demostrable, cuando se haya firmado un acuerdo de no-revelar, o cuando haya sido autorizado

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

expresamente por el propietario de la información de la dirección o unidad administrativa en cuestión. En caso de pérdida o revelación de información confidencial a personas no autorizadas o sospechosas de estas acciones, se deberá notificar inmediatamente al Propietario y al Oficial de Seguridad de la Información.

9.8.4.12. Salvo que la Dirección o unidad administrativa Propietaria de la Información haya concedido permiso para hacer pública cierta información, todas las peticiones de información de la institución y sus actividades deben remitirse a la dirección de Comunicación Estratégica. Tales peticiones incluyen formularios, encuestas y entrevistas en prensa, entre otros formularios de estudio. En caso de que un empleado, en nombre de la institución, reciba información confidencial de terceras partes, tal recepción estará precedida por el correspondiente formulario de autorización.

9.8.4.13. Los servidores públicos o trabajadores deben realizar revisiones periódicas de su información almacenada con el fin de no mantener información innecesaria o duplicada, a fin de hacer un uso responsable de los recursos de almacenamiento de la institución.

9.8.4.14. Ninguna información almacenada en las bases de datos puede ser modificada salvo la respectiva autorización avalada con firma electrónica del área Propietaria de la información con el respectivo justificativo, a través del sistema de gestión documental.

9.8.4.15. Toda conexión de red que se realice entre servidores, bases de datos y aplicaciones debe ser controlada a través del equipo de seguridad perimetral, el cual permitirá el acceso entre ellos siempre que exista la debida autorización.

9.8.4.16. Toda información que resida dentro de una base de datos permanecerá íntegra y no puede ser modificada de forma manual o directa por el administrador de base de datos, sin que preceda una autorización del área propietaria de la información con un

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

documento legalizado que justifique el cambio de esta información, previo a cualquier modificación autorizada, el administrador realizará un respaldo de la base de datos.

9.8.4.17. El Procedimiento de obtención periódica de respaldos de datos debe cumplir un cronograma definido y aprobado que esté orientado a garantizar los objetivos de punto de recuperación (RPO) mediante copias de respaldos inmutables, que permitan recuperación con restauraciones completas o a un punto en el tiempo, según la criticidad del servicio, cumpliendo con la regla 3-2-1-1-0, traducido a contar con al menos tres copias de los datos, almacenados en dos ubicaciones distintas, y al menos una de ellas en un lugar geográficamente diferente, que deberá contar con una verificación periódica de recuperación de los respaldos con cero errores, al menos una vez cada 3 meses.

9.8.4.18. El GPI debe tener definidos los procesos y procedimientos de todas las Direcciones que lo conforman para que en base a estos se pueda desarrollar e implementar el Sistema de Gestión de Seguridad de la Información (SGSI).

9.8.4.19. El GPI debe implementar un Sistema de Gestión de Seguridad de la Información bajo los lineamientos y estándares de los órganos de control, leyes y reglamentos determinados por el Estado ecuatoriano.

9.8.4.20. El GPI debe levantar y aplicar todos los procesos y procedimientos dentro de las Direcciones que lo componen.

9.8.4.21. El GPI debe desarrollar una evaluación del riesgo tecnológico, plan de mitigación y contingencias.

9.8.4.22. Al dar de baja equipos tecnológicos o documentos físicos, la información contenida en éstos debe seguir la política de destrucción de la información, para el fin debe existir una solicitud formal firmada por el responsable del activo de información, donde conste el código de referencia, versión, fecha de versión, fecha de creación, fecha de aprobación y el nivel de confidencialidad.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.8.4.23. Todas las supuestas violaciones de la normativa, intrusiones al sistema, infecciones de virus y otras condiciones que supongan, un riesgo para la información o los sistemas informáticos de la institución, deberán ser inmediatamente notificadas al Oficial de Seguridad de la Información por vía correo electrónico. Los usuarios no deben comprobar o intentar comprometer las medidas de seguridad de un ordenador o sistema de comunicación a no ser que tal acción haya sido previamente aprobada, por escrito, por el Comité de Seguridad de la Información. Los incidentes relacionados con la piratería informática, descubrimiento de contraseñas, decodificación de archivos y otras actividades que supongan una amenaza para las medidas de seguridad, o sean ilegales se considerarán violaciones graves de la normativa interna de la institución. También está terminantemente prohibido el uso de sistemas de bypass, cuyo objetivo es evitar las medidas de protección que pongan en riesgo los sistemas de protección.

9.8.5. Ambiente de desarrollo de pruebas y test

9.8.5.1. Toda base de datos que contenga información de producción con fines de pruebas de ambientes de desarrollo deberá ser enmascarada con el fin de salvaguardar la confidencialidad de la información.

9.8.5.2. Todo código fuente debe ser respaldado y encriptado en medios de almacenamiento y debidamente versionado.

9.8.6. Restauración de las copias de seguridad

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.8.6.1. El Comité de Seguridad de la Información (CSI) deberá definir el tiempo en el cual el GPI tolera la pérdida de información (RPO) y el tiempo en cual tolera que sus sistemas dejen de funcionar (RTO), términos que deberán ser tomados en cuenta a la hora de definir la frecuencia de los respaldos y el establecimiento de los planes de mitigación y contingencia de los sistemas.

9.8.6.2. Las copias de seguridad se restaurarán de forma aleatoria con una frecuencia determinada por RPO y RTO.

9.8.6.3. La DTI es responsable de validar la integridad de los datos respaldados y el buen funcionamiento de las aplicaciones.

9.8.6.4. Para proceder a la restauración de las actividades habituales de un ordenador personal tras una infección de virus, todo el software debe ser copiado antes de iniciar su utilización, y las copias deberán ser debidamente almacenadas en un lugar seguro. La copia maestra, en lugar de ser utilizada para actividades ordinarias, se reservará para ser recuperada tras la infección de virus, caída del disco duro y otros problemas.

9.9. CONTINUIDAD DE LOS SERVICIOS TI

9.9.1.1. El GPI desarrollará un plan integral de continuidad de servicios de TI, y realizará mejoras de forma periódica o ante cambios significativos tales como procesos, cumplimiento normativo legal y/o tecnología; para lo cual deberán participar activamente en dicha revisión las distintas áreas de los procesos identificados como críticos.

9.9.1.2. Se debe tener disponibilidad de plataformas computacionales, comunicaciones e información, necesarias para soportar las operaciones definidas como de misión crítica del GPI en los tiempos esperados y acordados.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.9.1.3. La Dirección General de TI debe tener actualizada la documentación de roles detallados y tareas para cada una de las personas involucradas en la ejecución del plan de continuidad de servicios TI.

9.9.1.4. La Dirección General de TI debe realizar un plan anual para probar el funcionamiento de los planes de contingencia.

9.9.1.5. La estrategia de continuidad de servicios de tecnologías de información y recuperación del GPI deberá diseñar e implementar actividades de prevención y de recuperación que ofrezcan las garantías necesarias para el restablecimiento de las operaciones del GPI después de un desastre.

9.9.1.6. Se debe establecer el tiempo aceptable para recuperar los datos que tiene la GPI en caso de una interrupción o desastre (RPO), y garantizar una recuperación eficaz.

9.9.1.7. Se debe garantizar la divulgación y concientización de las políticas y del plan de continuidad de servicios de TI y recuperación de desastres dentro del GPI.

9.9.1.8. Se debe realizar copias de seguridad (Respaldos) de las aplicaciones, bases de datos y bodegas de archivos alojados en servidores, con el propósito de salvaguardar la información. Estas se deben realizar periódicamente por la Dirección General de TI de acuerdo con las indicaciones establecidas en el plan de continuidad y se deberán almacenar en un sitio alterno fuera del edificio.

9.10. USO DE INTERNET

9.10.1. A los servidores públicos y trabajadores se les facilita el acceso a Internet para realizar sus actividades laborales. Sin embargo, este acceso puede ser denegado en cualquier momento, dado que se identifique un uso inadecuado del servicio, como el contactar con

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

páginas web que no tengan relación alguna con su trabajo, y sin cerciorarse que se cumplen las normativas de seguridad. Los servidores públicos y trabajadores no deben representar a la institución en una discusión en grupo en Internet u otros foros públicos, al menos que previamente hayan recibido un permiso de la Dirección General de Comunicación Estratégica. Asimismo, los servidores públicos y trabajadores no depositarán material de la institución (software, comunicados internos, notas de prensa, bases de datos, etc.) en ningún sistema informático de acceso público en Internet, a menos que tal acción haya sido previamente aprobada tanto por la Dirección o unidad administrativa Propietaria de la Información como por el Comité de Seguridad de la Información. El establecimiento de páginas web se gestiona de forma independiente por un proceso de aprobación en el que está implicado la Dirección General de Comunicación Estratégica. Del mismo modo, se prohíbe establecer acuerdos comerciales electrónicos a través de Internet sin la correspondiente evaluación y aprobación de los departamentos de Tecnologías de la Información y el área de Seguridad Informática. Por otra parte, nunca se enviará información confidencial, vía Internet, que no esté encriptada o codificada.

9.10.2. En caso de que se identifique que algún acceso que se solicite comprometa la seguridad de la información del GPI no se concederán los permisos, tales como accesos remotos, VPN externas, carpetas públicas, etc.

9.10.3. Toda aplicación que se publique en el Internet debe utilizar protocolos seguros como HTTPS, SSL y TLS.

9.10.4. Prohibiciones de internet.

9.10.4.1. El servicio de navegación a internet será restringido mediante grupos de usuarios, la asignación para cada servidor público o trabajador será de acuerdo con las necesidades que defina el Director

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

General de cada área con el respectivo justificativo por escrito, acceso que será evaluado por la Dirección General TI.

9.10.4.2. Todo servidor público o trabajador será responsable del uso de los recursos de internet, en el caso de tener eventos de seguridad al hacer uso de este servicio, se realizará un análisis para determinar las responsabilidades con el respectivo justificativo.

9.10.4.3. No está permitido descargar ninguna aplicación sin autorización del área de tecnología.

9.10.5. Navegación.

9.10.5.1. El GPI a través de los responsables de la seguridad de la información debe definir máximo hasta dos navegadores que serán los oficiales para el uso de los colaboradores.

9.10.5.2. Los navegadores de los servidores públicos o trabajadores deben tener la prohibición de aceptar cookies, caso contrario los servidores públicos o trabajadores solicitarán que se active esta funcionalidad aceptando su responsabilidad en el buen uso de estos recursos, que son partes funcionales de ciertos sitios Web que pueden contener código malicioso.

9.10.5.3. El GPI debe realizar charlas a los servidores públicos o trabajadores de concientización del uso de Internet y los peligros que se puedan dar o encontrar.

9.10.5.4. Todos los servidores públicos o trabajadores al navegar en el Internet deben hacerlo con responsabilidad de tal forma que se evite la contaminación de programas malignos dentro de la red de la Institución.

9.10.5.5. Todo servidor público o trabajador debe evitar marcar la opción de recordar contraseña al momento del ingreso de credenciales.

9.10.5.6. Todo servidor público o trabajador debe percatarse y analizar los sitios web a los que está ingresando y verificar que tengan protocolo seguro y que su certificado corresponda al sitio que está ingresando.

9.10.5.7. Evitar poner credenciales débiles en sitios web importantes.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.10.5.8. Evitar el uso de subida de archivos masivos hacia el internet y verificar que no sea información sensible a la institución.

9.11. CORREO ELECTRÓNICO

9.11.1. El correo electrónico es una herramienta que provee el GPI al personal para el desarrollo de la comunicación interna y externa institucional, la información comunicada y almacenada, incluyendo las copias de seguridad de este, son de propiedad del GPI.

9.11.2. El manejo del correo se realizará de acuerdo con la política de revisión de programas malignos establecido en los componentes de ciberseguridad implementados en la Institución.

9.11.3. El correo electrónico permite el envío de archivos e información con un límite de hasta 10 MB.

9.11.4. Se informará de la prohibición del uso del correo corporativo con fines personales que no tengan que ver con el GPI.

9.11.5. El contenido del correo deberá cumplir con las políticas de seguridad de la información aquí definidas, su uso inadecuado podrá conllevar sanciones.

9.11.6. El correo corporativo puede ser supervisado por la Dirección General de TI, según cláusula normativa dispuesta en el Acta de confidencialidad.

9.11.7. La Institución instalará aplicaciones antimalware y activará filtros antispam tanto en el servidor como en el cliente de correo según la Política Antimalware establecida, estos filtros permitirán que los correos maliciosos sean identificados y no lleguen a la bandeja de entrada evitando así su posible infiltración.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.11.8. El correo electrónico debe tener instalado una tecnología de firma digital para proteger la información asegurando la autenticidad del remitente.

9.11.9. Desactivar el formato HTML, la ejecución de macros y la descarga de imágenes.

9.11.10. Los servidores públicos o trabajadores no deben publicar las direcciones de correo corporativas en páginas web ni en redes sociales a no ser que estén debidamente autorizados por la máxima autoridad del GPI.

9.11.11. Para socializar la dirección de correo electrónico se debe crear una imagen de este a la hora de ser publicado en lugar de introducir el correo como texto.

9.11.12. Implementar contraseña segura con un nivel de dificultad medio de 12 caracteres en el cual debe tener al menos un carácter especial, mayúsculas, minúsculas y números, que sean fáciles de recordar y difíciles de adivinar.

9.11.13. Las contraseñas no deben almacenarse en ningún medio legible donde puedan ser descubiertas por personas sin autorización.

9.11.14. Se debe implementar doble factor de autenticación para las cuentas críticas.

9.11.15. El servidor público o trabajador debe tener precaución cuando accede al correo desde una interfaz web, el no marcar la opción de recordar contraseña.

9.11.16. Los servidores públicos o trabajadores deben aprender a identificar correos fraudulentos y sospechar de acciones que estén fuera del lugar, y de los que puedan resultar atentados para la seguridad de la institución.

9.11.17. Los servidores públicos o trabajadores del GPI deben utilizar pie de firmas y logotipos estándares y autorizados por la Institución.

9.11.18. Mediante el correo electrónico el funcionario no puede enviar información sensible para la Institución.

9.11.19. El servidor público o trabajador no abrirá un correo sin identificar el remitente.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.11.20. El servidor público o trabajador al recibir un mensaje con un adjunto, este se debe analizar cuidadosamente antes de abrirlo.

9.11.21. El servidor público o trabajador debe evitar adjuntos cuyo nombre incite a descargas, por ser habitual o porque creer que tiene un contenido atractivo.

9.11.22. Si el servidor público o trabajador recibe un correo con la extensión .exe debe informar al Dirección TI para que este sea analizado.

9.11.23. El servidor público o trabajador debe evitar la entrega de permisos para habilitar opciones que están deshabilitadas por defecto como el uso de macros.

9.11.24. El servidor público o trabajador debe evitar la apertura de links que llevan a páginas WEB externas.

9.11.25. Se debe borrar los correos que corresponden a remitentes desconocidos o evitar responder al spam (correo basura).

9.12. RENOVACIÓN DE EQUIPOS

9.12.1. Se deberán definir los tiempos estimados de vida útil de los equipos de cómputo y telecomunicaciones para programar con anticipación su renovación.

9.12.2. La Dirección General de TI debe tener un inventario de los equipos tecnológicos que están siendo utilizados por la Institución con su respectivo registro de obsolescencia y fin de soporte por parte del fabricante, así como la vigencia de su mantenimiento anual.

9.12.3. Todo equipo que esté funcionando y esté en producción debe tener su soporte de fabricante y su vigencia tecnológica que está determinado por el propio fabricante.

9.12.4. Siempre que se compren equipos, se deberá establecer su criticidad e incorporar su respectivo plan de contingencia.

9.12.5. La Dirección General de TI será la responsable de analizar y validar la obsolescencia tecnológica que tiene el GPI y determinar la

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

renovación del parque tecnológico de acuerdo con lo que determina la ley y normativa vigente.

9.12.6. El soporte del fabricante de los componentes de Hardware y Software será determinado por la vigencia tecnológica de los fabricantes de acuerdo con el ciclo de vida publicado en los portales Web, lo que dependerá que la Dirección General de TI determine si se puede o no adquirir el respectivo soporte.

9.13. ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS

9.13.1. El acceso a servidores y aplicaciones por parte de los administradores o proveedores deberá realizarlo a través de protocolos seguros como son SSL, SSH, etc.

9.13.2. Se prohíbe el uso de accesos remotos gráficos con RDP de Windows que no sean seguros o licenciados con accesos seguros.

9.13.3. El acceso a los servidores, equipos de networking, equipos de ciberseguridad por parte de los administradores deberán realizarlo a través de la red de administración.

9.13.4. La Dirección de TI debe designar un administrador de todas las bases de datos de producción, quien será responsable de su administración, disponibilidad, confiabilidad e integridad de la información que permanece dentro de estas.

9.14. TELETRABAJO

9.14.1. Los servidores públicos o trabajadores que estén en Teletrabajo obligatoriamente deberán utilizar equipos institucionales con acceso VPN, para el efecto se deberá notificar a la Dirección General de TI para su habilitación. No es permisible el uso de equipos personales, y está prohibido transferir la información de la institución a medios externos sin autorización previa por escrito.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

9.14.2. Los servidores públicos y trabajadores que soliciten el teletrabajo deberán cumplir con los siguientes prerrequisitos:

a. Disponer un computador entregado por la Institución y configurado con todos los controles de seguridad determinados en las políticas de seguridad por parte de la Dirección General de TI.
b. Cumplir con la capacitación de concientización de la seguridad de la información, y su respectiva aprobación.
c. Realizar la solicitud respectiva a su Dirección General la misma que debe validar que cuente con los recursos necesarios para salvaguardar la información, como es un computador de la Institución, el cual debe tener los componentes de seguridad establecidos por la DGTI.
d. La Dirección General de TI, debe entregar computadores, credenciales y perfiles de acceso a los servidores públicos o trabajadores que realizan Teletrabajo para que cumplan con las siguientes políticas:
    - ✓ Toda la información que pertenece a la Institución debe estar encriptada.
    - ✓ Se debe configurar permitir perfiles de acceso a las aplicaciones de la Institución por cada usuario a través del concentrador de VPN´s.
    - ✓ Debe contar con software de encriptación de datos sobre el canal (VPN cliente)
    - ✓ El acceso de los usuarios debe cumplir con un doble factor de autenticación.
    - ✓ Garantizar que los recursos de hardware del concentrador de VPN´s soporte la carga de las VPN-clientes concurrentes por lo menos que supere dos veces la capacidad de servidores públicos o trabajadores que tiene la Institución.
    - ✓ Por lo menos uno de los métodos de autenticación debe ser con las credenciales del Directorio Activo.
    - ✓ El cambio de contraseñas debe ser más frecuente por lo menos una vez al mes.
    - ✓ El computador de la Institución debe contar con un software de seguridad de punto final en donde esté activado el antivirus, antimalware, anti-ransomware, firewall, IPS y las demás características de configuración en especial el envío de logs y alertas.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

- ✓ La información que sea generada y consumida cuando el servidor público o trabajador esté en teletrabajo, debe ser respaldada tan pronto como se conecte a la red corporativa bajo los lineamientos determinados por la Dirección General TI.
- ✓ En el caso de usar computadores personales de los servidores públicos o trabajadores, estos deben tener todos los componentes de seguridad que tienen implementados los computadores corporativos del GPI y cumplir con las políticas indicadas anteriormente.

9.15. DISPOSITIVOS MÓVILES

9.15.1. Los servidores públicos o trabajadores no pueden hacer uso de sus dispositivos móviles personales para el manejo de la información del GPI, si fuese requerido, deberán solicitar la respectiva autorización a la máxima autoridad, al Director General de su departamento y notificar a la Dirección General de TI para que se entregue los lineamientos aprobados por la Institución para el uso de información dentro de estos equipos.

9.15.2. En el caso que se apruebe el uso de los dispositivos móviles para el manejo de información de la Institución es necesario que estos equipos cuenten con software de encriptación de la información y software de detección de programas malignos y virus.

10. SANCIONES

En el caso de incumplimiento de las políticas de seguridad, los servidores públicos o trabajadores estarán sujetos a las sanciones y multas, de acuerdo con el procedimiento establecido en la Ley Orgánica del Servicio Público, su Reglamento General, Código de Trabajo y Reglamentos internos de administración de talento humano para servidores públicos y trabajadores.

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec

Y lo establecido en las normas de control interno de la Contraloría General del Estado y a lo establecido por la Ley Orgánica de Protección de Datos Personales.

CONTROL DE VERSIONES					
Código	Versión	Fecha	Descripción de Cambios	Elaborado por	Aprobó
DTI-SI-01	1.0	06/08/2021	Primera Versión	DGTI	Ing. Roberto López
DTI-SI-02	2.0	04/10/2022	Segunda Versión	DGTI	Ing. Elizabeth Coba

Ibarra
Bolivar y Oviedo, esq.
Telfs.:(593 6) 2955 225
2955 832, 2950 939
www.imbabura.gob.ec
Fax.: (593 6) 2955 430
email: info@imbabura.gob.ec