

REPÚBLICA DEL ECUADOR
INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS

RESOLUCIÓN No. 004-DIREJ-DIJU-NI-2021

Que, el numeral 2 del artículo 18 de la Constitución de la República del Ecuador, consagra como uno de los derechos de las personas: “(...) 2. *Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información*”;

Que, el numeral 19 del artículo 66 de la Constitución de la República del Ecuador, dispone: “*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 226 de la Constitución de la República del Ecuador, 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 del Ecuador, determina: “*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 inciso primero del artículo 233 de la Constitución de la República del Ecuador, dispone: “*Ninguna servidora ni servidor público estará exento de responsabilidades por los actos realizados en el ejercicio de sus funciones, o por sus omisiones, y serán responsables administrativa, civil y penalmente por el manejo y administración de fondos, bienes o recursos públicos (...)*”;

Que, el inciso segundo del artículo 314 de la Constitución de la República del Ecuador, señala: “*(...) 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. El Estado dispondrá que los precios y tarifas de los servicios públicos sean equitativos, y establecerá su control y regulación*”;

Que, el artículo 1 de la Ley Orgánica de Transparencia y Acceso a la Información

Pública, establece: *“Principio de Publicidad de la Información Pública. - El acceso a la información pública es un derecho de las personas que garantiza el Estado.*

Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema materia de la información tengan participación del Estado o sean concesionarios de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONGs), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley”;

Que, el artículo 5 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, indica: *“Información Pública. - Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado”;*

Que, el artículo 6 de la Ley ibídem, señala: *“Información Confidencial. - Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales (...);”*

Que, el artículo 10 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, reza: *“Custodia de la Información.- Es responsabilidad de las instituciones públicas, personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley, crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción.*

Quienes administren, manejen, archiven o conserven información pública, serán personalmente responsables, solidariamente con la autoridad de la dependencia a la que pertenece dicha información y/o documentación, por las consecuencias civiles, administrativas o penales a que pudiera haber lugar, por sus acciones u omisiones, en la ocultación, alteración, pérdida y/o desmembración de documentación e información pública. Los documentos originales deberán permanecer en las dependencias a las que pertenezcan, hasta que sean transferidas a los archivos generales o Archivo Nacional (...);”

Que, el artículo 19 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, indica: *“De la Solicitud y sus Requisitos.- El interesado a acceder a la información pública que reposa, manejan o producen las personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley, deberá hacerlo mediante solicitud escrita ante el titular de la institución.*

En dicha solicitud deberá constar en forma clara la identificación del solicitante y la ubicación de los datos o temas motivo de la solicitud, la cual será contestada en el plazo señalado en el

artículo 9 de esta Ley”;

Que, el artículo 20 de la Ley ibídem, expresa: “(...) La solicitud de acceso a la información no implica la obligación de las entidades de la administración pública y demás entes señalados en el artículo 1 de la presente Ley, a crear o producir información, con la que no dispongan o no tengan obligación de contar al momento de efectuarse el pedido. En este caso, la institución o entidad, comunicará por escrito que la denegación de la solicitud se debe a la inexistencia de datos en su poder, respecto de la información solicitada. Esta Ley tampoco faculta a los peticionarios a exigir a las entidades que efectúen evaluaciones o análisis de la información que posean, salvo aquellos que por sus objetivos institucionales deban producir (...)”;

Que, el artículo 4 de la Ley del Sistema Nacional de Registro de Datos Públicos, prescribe: “Responsabilidad de la información. - Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información.

Las personas afectadas por información falsa o imprecisa, difundida o certificada por registradoras o registradores, tendrán derecho a las indemnizaciones correspondientes, previo el ejercicio de la respectiva acción legal. (...)”;

Que, el artículo 6 de la Ley del Sistema Nacional de Registro de Datos Públicos dispone: “Accesibilidad y confidencialidad.- Son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales.

El acceso a estos datos sólo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial.

También son confidenciales los datos cuya reserva haya sido declarada por la autoridad competente, los que estén amparados bajo sigilo bancario o bursátil, y los que pudieren afectar la seguridad interna o externa del Estado.

La autoridad o funcionario que por la naturaleza de sus funciones custodie datos de carácter personal, deberá adoptar las medidas de seguridad necesarias para proteger y garantizar la reserva de la información que reposa en sus archivos.

Para acceder a la información sobre el patrimonio de las personas el solicitante deberá justificar y motivar su requerimiento, declarar el uso que hará de la misma y consignar sus datos básicos de identidad, tales como: nombres y apellidos completos, número del documento de identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo reglamento se determinen. Un uso distinto al declarado dará lugar a la determinación de responsabilidades,

sin perjuicio de las acciones legales que el/la titular de la información pueda ejercer.

La Directora o Director Nacional de Registro de Datos Públicos, definirá los demás datos que integrarán el sistema nacional y el tipo de reserva y accesibilidad”;

Que, el literal d) del artículo 10 de la Ley de Estadística, señala: *“Al Instituto Nacional de Estadística y Censos le corresponde: (...) d) operar como centro oficial general de información de datos estadísticos del país”;*

Que, el artículo 11 de la Ley de Estadística dispone que el Director General, actualmente Director Ejecutivo, es el representante legal del Instituto Nacional de Estadística y Censos y el responsable de su gestión técnica, económica y administrativa;

Que, el artículo 21 de la Ley de Estadística, establece: *“Los datos individuales que se obtengan para efecto de estadística y censos son de carácter reservado; en consecuencia, no podrán darse a conocer informaciones individuales de ninguna especie, ni podrán ser utilizados para otros fines como de tributación o conscripción, investigaciones judiciales y, en general, para cualquier objeto distinto del propiamente estadístico o censal. Solo se darán a conocer los resúmenes numéricos, las concentraciones globales, las totalizaciones y, en general, los datos impersonales”;*

Que, el artículo 128 del Código Orgánico Administrativo, prescribe: *“Acto normativo de carácter administrativo. - Es toda declaración unilateral efectuada en ejercicio de una competencia administrativa que produce efectos jurídicos generales, que no se agota con su cumplimiento y de forma directa”;*

Que, el artículo 130 del Código Orgánico Administrativo, señala: *“Competencia normativa de carácter administrativo. 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”;*

Que, el artículo 4 del Decreto Ejecutivo No. 77 de 15 de agosto de 2013, publicado en el Registro Oficial No. 81 de 16 de septiembre de 2013, dispone: *“Las instituciones que tengan a su cargo registros administrativos o catastros útiles para la generación e investigación estadística, deberán remitirlos oportuna, gratuita y obligatoriamente al Instituto Nacional de Estadística y Censos, en los formatos y periodicidad que éste establezca para el efecto. Los registros administrativos y catastros se utilizarán únicamente con fines estadísticos o analíticos”;*

Que, el numeral 2 del artículo 3 del indicado Decreto Ejecutivo 77, establece: *“El Instituto Nacional de Estadística y Censos tendrá entre otras funciones, además de las contempladas en la Ley de Estadística, la función de: (...) 2. Establecer normas, estándares, protocolos y lineamientos, a las que se sujetarán aquellas instituciones públicas que integran el Sistema Estadístico Nacional (...)”;*

- Que,** a través de Acuerdo Ministerial No. 011-2018 de 8 de agosto de 2018, el Ministerio de Telecomunicaciones y de la Sociedad de la Información, expidió el *“Plan de Gobierno Electrónico 2018-2021”*, dentro del cual se establece en la estrategia 3. *“Impulsar la protección de la información y datos personales”*; y, se contempla como iniciativa el *“Emitir norma que estandarice los instrumentos de la participación electrónica”*, en la Administración Pública Central;
- Que,** mediante Acuerdo Ministerial No. 012-2019 de 11 de junio de 2019, el Ministerio de Telecomunicaciones y Sociedad de la Información, expidió la *“Guía para el tratamiento de datos personales en la Administración Pública Central”*;
- Que,** el artículo 4 del Acuerdo Ministerial No. 025-2019 de 20 de septiembre de 2019, mediante el cual se expidió el Esquema Gubernamental de Seguridad de la Información-EGSI, señala: *“Las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, actualizarán o implementarán el Esquema Gubernamental de Seguridad de la Información EGSI en un plazo de doce (12) meses contados a partir de la publicación del presente Acuerdo Ministerial en el Registro Oficial (...)”*;
- Que,** el artículo 5 del Acuerdo Ministerial No. 025-2019, prescribe: *“La máxima autoridad designará al interior de su Institución, un Comité de Seguridad de la Información (CSI), que estará integrado por los responsables de las siguientes áreas o quienes hagan sus veces: Talento Humano, Administrativa, Planificación y Gestión Estratégica, Comunicación Social, Tecnología de la Información, Unidades Agregadores de Valor y el Área Jurídica participará como asesor (...)”*;
- Que,** el literal a) del artículo 6 del Acuerdo Ministerial No. 025-2019, establece: *“El Comité de Seguridad de la Información, tendrá las siguientes responsabilidades: a) Gestionar la aprobación de la política y normas institucionales en materia de seguridad de la información, por parte de la máxima autoridad de la Institución”*;
- Que,** mediante Resolución No. 011-DIREJ-DIJU-NI-2015 de 20 de febrero de 2015, publicada en el Registro Oficial No. 325 de 11 de junio de 2015, el Director Ejecutivo del Instituto Nacional de Estadística y Censos, resolvió expedir el Estatuto Orgánico de Gestión Organizacional por Procesos del Instituto Nacional de Estadística y Censos – INEC”;
- Que,** a través de Resolución No. 007-DIREJ-DIJU-NI-2020 de 07 de febrero de 2020, se creó el *“Comité de Seguridad de la Información (CSI) del Instituto Nacional de Estadística y Censos”*; mismo que en su artículo 1 señala: *“OBJETO.- El Comité de Seguridad de la Información tiene como objeto garantizar y facilitar la implementación de las iniciativas de seguridad de la información en la Institución, a fin de preservar la confidencialidad, integridad y disponibilidad de la información que maneja el INEC”*;
- Que,** con memorando Nro. INEC-CTPES-2021-0004-M de 07 de enero de 2021, el Coordinador General Técnico de Planificación Normativas de Calidad Estadística Encargado, solicitó al Director Ejecutivo: *“(...) se sirva autorizar a*

quien corresponda la ejecución de las gestiones pertinentes para la elaboración de la “Resolución para la Política de Gestión de Seguridad de la Información”;

Que, mediante memorando Nro. INEC-INEC-2021-0015-M de 14 de enero de 2021, el Director Ejecutivo, indicó a la Dirección de Asesoría Jurídica: *“(...) se procede a autorizar la elaboración de la mencionada Resolución y se dispone a la unidad pertinente dar el trámite correspondiente de acuerdo a la normativa legal vigente (...)”.*

En ejercicio de las facultades constitucionales, legales y reglamentarias antes singularizadas y con sustento en las consideraciones expuestas,

RESUELVE:

Artículo 1.- Expedir la *“POLÍTICA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS”*

Artículo 2.- Objeto: Establecer las directrices para la gestión de seguridad de la información en el Instituto Nacional de Estadística y Censos – INEC a nivel nacional, que garanticen la confidencialidad, integridad y disponibilidad de datos e información.

Artículo 3.- Ámbito: La presente resolución, así como la Política de Gestión de Seguridad de la Información del INEC, son de cumplimiento obligatorio para todos los servidores y servidoras del INEC a nivel nacional; cubre, además, procesos y proyectos en los cuales intervengan personas naturales o jurídicas que no forman parte del INEC y que por intermedio de convenios, acuerdos o contratos manejen información del INEC.

Artículo 4.- Integración: Forma parte integrante de la presente resolución, la *“Política de Gestión de Seguridad de la Información del Instituto Nacional de Estadística y Censos, elaborada por el Oficial de Seguridad, revisada por el Comité de Seguridad de la Información y aprobada por el Director Ejecutivo, del Instituto Nacional de Estadística y Censos, junto con sus Anexos 1 – Roles y Responsabilidades; y, 2 – Clasificación de la Información”*, (Apéndice 1). Aprobado por el Comité de Seguridad de la Información, de forma unánime, mediante ACTA RESOLUTIVA DE SESIÓN EXTRAORDINARIA DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN NO. 011-2020; y, autorizada por el Director Ejecutivo, a través del memorando Nro. INEC-INEC-2021-0015-M de 14 de enero de 2021.

DISPOSICIONES GENERALES:

PRIMERA. - La presente Resolución entrará en vigencia a partir de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

SEGUNDA. - De la correcta ejecución de la presente resolución, encárguese al Comité de Seguridad de la Información (CSI) y al Oficial de Seguridad de la Información.

COMUNÍQUESE Y PUBLÍQUESE.

Dado en Quito, Distrito Metropolitano a, los 20 días del mes de enero de 2021.

Econ. Diego Andrade Ortiz
DIRECTOR EJECUTIVO
INSTITUTO NACIONAL DE ESTADÍSTICA Y CENSOS

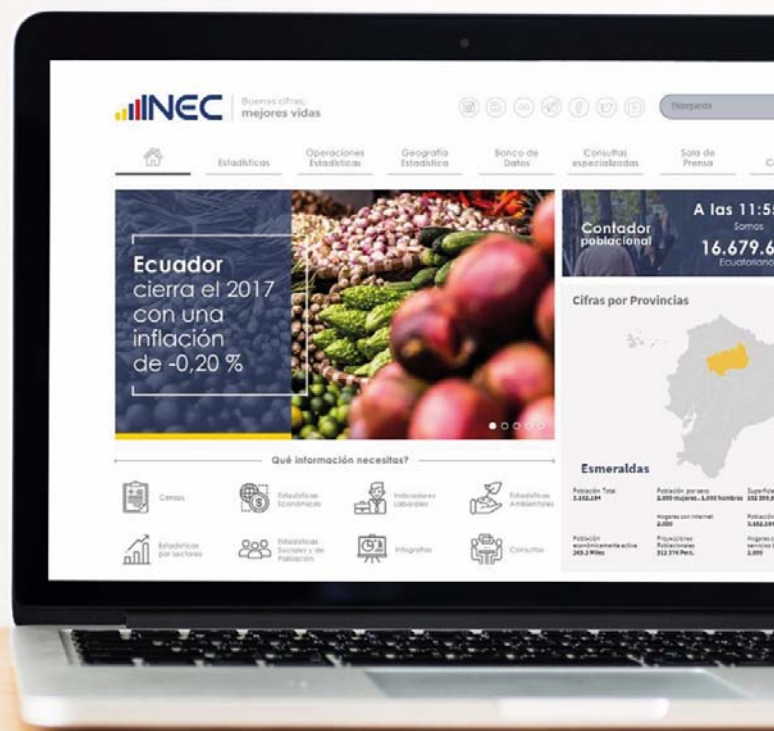
ELABORADO POR:	ABG. MARIBEL MUÑOZ	MIEMBRO DE EQUIPO
REVISADO Y APROBADO POR:	AB. MARIA EUGENIA MORALES	DIRECTORA DE ASESORIA JURÍDICA



APÉNDICE 1

POLÍTICA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Octubre, 2020



Versión:	0.2
Fecha de la versión:	15.09.2020
Creado por:	Oficial de Seguridad
Revisado por:	Comité de Seguridad de la Información
Aprobado por:	Director Ejecutivo
Fecha de aprobación:	15.10.2020
Nivel de confidencialidad:	Bajo – Uso Público
Referencia:	<ul style="list-style-type: none"> • Acuerdo Ministerial No. 025-2019 • Esquema Gubernamental de Seguridad de la Información (EGSI V2.0) • Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000

Historial de cambios

Fecha	Versión	Actualización realizada	Elaborado
21-oct-2019	0.1	Propuesta original.	William Franco
15-oct-2020	0.2	Revisión y actualización acorde al Acuerdo Ministerial No. 025-2019.	Jenny Delgado

Tabla de contenido

1. Declaración y Compromiso de la Dirección Ejecutiva	4
2. Antecedentes	5
3. Definiciones	6
4. Objetivos	6
4.1. Objetivo General.....	6
4.2. Objetivos específicos	6
5. Alcance	6
6. Actualización a la Política de Seguridad de la Información	7
7. Política orgánica de seguridad de la información	7
8. Políticas particulares.....	7
8.1. Generales:	7
8.2. Responsables de la Seguridad de la Información	8
8.3. Gestión del Riesgo.....	8
8.4. Gestión de Activos.....	9
8.5. Seguridad de los recursos humanos.....	9
8.6. Seguridad física y del entorno.....	10
8.7. Gestión de comunicaciones y operaciones.....	11
8.8. Control del acceso	11
8.9. Adquisición, desarrollo y mantenimiento de sistemas de información.....	12
8.10. Gestión de los incidentes de la seguridad de la información	12
8.11. Gestión de la continuidad del negocio.....	12
8.12. Cumplimiento.....	13
9. Aceptación del Riesgo (Excepciones y autorizaciones)	13
10. Glosario de términos.....	13
11. Anexos	20
12. Aprobación.....	20
13. Registro de firmas.....	20

1. Declaración y Compromiso de la Dirección Ejecutiva

A todos los colaboradores del Instituto Nacional de Estadística y Censos

La información es un activo esencial para el desarrollo de las actividades del INEC. Dependemos estrictamente de datos e información para el cumplimiento de nuestra misión institucional, lo que nos faculta para proveer de un insumo oficial, indispensable para la toma de decisiones en cuanto política pública; un mínimo descuido en la protección de datos podría redundar en la pérdida de confianza y, consecuentemente, socavar la razón de ser del INEC.

Con la sofisticación de la tecnología, los datos e información están en un entorno interconectado que apoyan notablemente para que el INEC oriente de mejor manera sus servicios al alcance de todos los habitantes del Ecuador. Con la capacidad del internet su cobertura llega a escala mundial.

Así como los datos e información pueden ser utilizados de manera positiva, existe la posibilidad de que personas o grupos la utilicen con fines contrarios a la ley; y, para lograr su objetivo podrían utilizar a las instituciones aprovechándose de vulnerabilidades, amenazas o debilidades en los procesos, procedimientos, personas o tecnologías.

Los datos e información se concentran en documentos impresos, escritos, conversaciones, Infraestructura tecnológica y dispositivos electrónicos, en portales web, correo electrónico, redes sociales, incluso en la memoria de las personas; por lo que debemos alinearnos prudentemente para garantizar la confidencialidad, integridad y disponibilidad de los mismos. Si por la antigüedad de ciertos sistemas se adolece de algunas protecciones, las direcciones responsables de ellos deben soportarlos con una gestión eficiente y prudente; con procedimientos apropiados de control que cubran las protecciones o acciones faltantes.

Como regla general deben garantizar la confidencialidad de los datos e información de carácter personal; de la información que no está sujeta al principio de publicidad y de los derechos de propiedad intelectual, por lo que la identificación de los controles que se deberían establecer -ya sean manuales o automatizados- requieren de planificación y atención cuidadosa a los detalles, así como su cumplimiento y continuidad, lo que implica la participación de cada funcionario.

Tendremos una actitud de cero tolerancia al incumplimiento de la política, normas, procesos y procedimientos de seguridad de la información. Participe en las capacitaciones e involúcrese en la protección de los datos e información bajo su custodia; y, ante cualquier duda en la toma de decisiones en términos de seguridad de la información, consulte oportunamente con el Oficial de Seguridad de la Información.

Contamos con tu apoyo.

Director Ejecutivo

2. Antecedentes

El 20 de septiembre de 2019, el Ministro de Telecomunicaciones y Sociedad de la Información emitió el Acuerdo Ministerial No. 025-2019, publicado en la Edición Especial del Registro Oficial No. 228 de 10 de enero de 2020, mediante el cual acordó: *“Expedir el Esquema Gubernamental de Seguridad de la Información -EGSI-, el cual es de implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, que se encuentra como Anexo al presente Acuerdo Ministerial”*.

El artículo 2 del Acuerdo Ministerial No. 025-2019, señala: *“Las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, realizarán la Evaluación de Riesgos sobre sus activos de información críticos y diseñarán el plan para el tratamiento de los riesgos de su Institución, utilizando como referencia la “GUIA PARA LA GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACION” que es parte del Anexo del presente Acuerdo Ministerial, previo a la actualización o implementación de los controles de seguridad”*.

El artículo 3 del Acuerdo Ministerial No. 025-2019, establece: *“Recomendar a las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, utilicen como guía las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información”*.

El artículo 4 del Acuerdo Ministerial No. 025-2019, prescribe: *“Las Instituciones de la Administración Pública, Institucional y que dependen de la Función Ejecutiva, actualizarán o implementarán el Esquema Gubernamental de Seguridad de la Información (EGSI) en un plazo de doce (12) meses contados a partir de la publicación del presente Acuerdo Ministerial en el Registro Oficial. La Evaluación de Riesgos y el plan para el tratamiento de los riesgos de cada institución se realizarán un plazo de cinco (5) meses y la actualización o implementación de los controles del Esquema Gubernamental de Seguridad de la Información (EGSI) se realizarán en un plazo siete (7) meses. La actualización o implementación, se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información”*.

En el acápite 1.1.1 del numeral 1. Políticas de Seguridad de la Información, de la Guía para la Implementación de controles de Seguridad de la Información en el Esquema Gubernamental de Seguridad de la Información versión 2 anexo al Acuerdo Ministerial No. 025-2019, señala: *“Elaborar, implementar y socializar las políticas de seguridad de la información, definidas para la institución, debidamente aprobada por la máxima autoridad o su delegado”,* teniendo como recomendaciones los siguientes numerales: 1.1.1.1 *“La máxima autoridad dispondrá la implementación de este Esquema Gubernamental de Seguridad de la Información (EGSI) en su institución”,* 1.1.1.2 *“Difundir la siguiente política de seguridad de la información como referencia: ‘Las instituciones de la Administración Pública Central, Dependiente e Institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera”,* 1.1.1.3 *“Las instituciones públicas podrán especificar una política de seguridad más amplia o específica en armonía con la Constitución, leyes y demás normativa legal propia o relacionada así como su misión y competencias”*.

En el acápite 1.1.2 del numeral 1. Políticas de Seguridad de la Información de la Guía para la Implementación de controles de Seguridad de la Información en el Esquema Gubernamental de Seguridad de la Información versión 2, anexo al Acuerdo Ministerial No. 025-2019 señala: *“Para garantizar la vigencia de la política de seguridad de la información en la institución, esta debe ser revisada anualmente o cuando se produzcan cambios significativos a nivel operativo, legal, tecnológica, económico, entre otros; los cuales deben ser documentados y versionados”*.

3. Definiciones

- a. **Servidor público:** Todas las personas que en cualquier forma o cualquier título trabajen, presten servicios o ejerzan un cargo, función o dignidad dentro de sector público.
- b. **Trabajador público:** Todas las personas que trabajan en el sector público y que se encuentran sujetos al Código del Trabajo.

4. Objetivos

4.1. Objetivo General

Establecer directrices para la gestión de seguridad de la información en el Instituto Nacional de Estadística y Censos-INEC a nivel nacional, que garanticen la confidencialidad, integridad y disponibilidad de datos e información.

4.2. Objetivos específicos

- a. Proteger los activos de la información incluso ante la provisión de servicios de partes externas.
- b. Asegurar que los servidores, contratistas y usuarios de terceras partes entienden sus responsabilidades y sean aptos para las funciones para las cuales están considerados, y reducir el riesgo de posibles amenazas y de error humano.
- c. Garantizar el acceso físico apropiado para la protección de documentos e infraestructura tecnológica.
- d. Asegurar el acceso autorizado de usuarios con la operación correcta y segura de los servicios de procesamiento de información.
- e. Detectar actividades de procesamiento de la información no autorizadas y evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información.
- f. Asegurar la comunicación y gestión efectiva ante eventos, debilidades e incidentes de seguridad de la información.
- g. Contrarrestar las interrupciones en las actividades de la institución y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.
- h. Establecer las normas, procedimientos, e instructivos en materia de Seguridad de la Información.
- i. Asegurar el cumplimiento de la ley, de obligaciones estatutarias, reglamentarias o contractuales.

5. Alcance

Esta política es de aplicación obligatoria para todos los servidores y servidoras del INEC a nivel nacional; cubre además, procesos y proyectos en los cuales intervengan personas naturales o jurídicas que no forman parte del INEC y que por intermedio de convenios, acuerdos o contratos manejen información del INEC.

6. Actualización a la Política de Seguridad de la Información

- a. En cualquier momento las servidoras y servidores del INEC podrán proponer al Oficial de Seguridad de la Información actualizaciones a la política y normas sustentándola a través de la utilización de la metodología de gestión de riesgos, la propuesta debe estar por escrito y debe venir aprobada por la Dirección o Coordinación de su gestión; y, el Oficial de Seguridad de la Información estará obligado a receptar todas las propuestas, para analizar su factibilidad validando la posible reducción del riesgo. Si el análisis de factibilidad resulta en una negativa, se justificará únicamente cuando el riesgo residual de la propuesta se mantiene igual o superior al riesgo actual.
- b. El Oficial de Seguridad de la Información podrá directamente proponer actualizaciones a la política y normas, ya sea por iniciativa propia de mejores prácticas, como resultado de revisiones independientes, por disposiciones normativas o por cambios en los procesos.
- c. Además de las propuestas de actualización que pueden remitirse en cualquier momento, la política y normas de seguridad de la información serán revisadas regularmente con periodicidad anual en el tercer trimestre de cada año, con la finalidad de validar su aplicabilidad a la realidad vigente del INEC.
- d. Las propuestas de actualizaciones a la política y normas serán canalizadas, a través del Oficial de Seguridad de la Información, al Comité de Seguridad de la Información para su posterior aprobación por parte de la Dirección Ejecutiva.

7. Política orgánica de seguridad de la información

El INEC garantizará la confidencialidad, integridad y disponibilidad de la información que genera, utiliza, procesa, comparte, transmite y almacena en medio electrónico o escrito.

8. Políticas particulares

8.1. Generales:

- a. El INEC establecerá Acuerdos de Uso y confidencialidad o de “No divulgación” de la información con personas naturales y personas jurídicas con quienes suscribirán o mantienen contratos o convenios.
- b. Todo el personal del INEC deberá estar actualizado en sus conocimientos de seguridad de la información, por lo que se deberá publicar al interior de la institución la política, normas, procedimientos y material relacionado a seguridad de la información.
- c. Todo el personal empleará un prudente proceso de control interno en sus áreas, garantizando la calidad de sus propias actividades orientada a la protección de la información del INEC.
- d. El INEC motivará la revisión independiente por parte de Auditoría Interna o una tercera parte, al menos con periodicidad anual para evaluar oportunidades de mejora y la necesidad de cambios en el enfoque de seguridad de la información.
- e. Todo servicio de procesamiento de información realizado por partes externas debe ser expuesto a una evaluación de riesgos, de tal manera que de acuerdo al mismo y a la

confidencialidad de la información, se requerirá las protecciones necesarias cubiertas bajo un contrato o convenio suscrito entre las partes incluyendo partes subcontratadas. La evaluación será realizada por el dueño del proceso con el acompañamiento del Oficial de Seguridad de la Información del INEC.

- f. Todos los procesos con actividades manuales y/o a través de sistemas informáticos, deben asegurar una correcta segregación de funciones de tal manera que la ejecución, revisión, autorización y seguimiento se efectúa por parte de distintos cargos.
- g. La finalización de un contrato o el cambio de funciones, implica el cumplimiento de los procesos de entrega de activos de información y remoción de privilegios sobre las plataformas tecnológicas del INEC.
- h. Todos los empleados, pasantes, personal contratado bajo modalidad civil: servicios profesionales, técnicos especializados y proveedores de servicios usarán los recursos del INEC para propósitos de cumplimiento de sus funciones encomendadas y/o contratadas por el INEC, con lo que se prohíbe el uso de los recursos del INEC para propósitos personales o cualquier otro propósito que sea contrario a los derechos humanos, a la Constitución y las leyes vigentes.
- i. El incumplimiento de esta Política de Seguridad de la Información así como las normas, procedimientos y formatos relacionados, provoque un incidente de seguridad, se aplicará un proceso disciplinario y de ser necesario las acciones legales correspondientes, dentro del marco legal vigente.

8.2. Responsables de la Seguridad de la Información

- a. Todos somos responsables de la protección de activos de información, que llegan a nuestro control, custodia y conocimiento.
- b. La organización interna de seguridad de la información (ANEXO 1. ROLES Y RESPONSABILIDADES) debe garantizar la definición, la ejecución y el control de la implementación de la seguridad de la información dentro del INEC.
- c. La seguridad de la información y los servicios de procesamiento de información del INEC no deben afectarse por participación de partes externas ya sea en el acceso, procesamiento, administración o comunicaciones realizadas por éstas.
- d. Se establecerán normas específicas de seguridad para relaciones con partes externas de cumplimiento obligatorio para ese tipo de relaciones.

8.3. Gestión del Riesgo

- a. El INEC gestionará los riesgos de seguridad de la información como base para establecer las protecciones diferenciadas a cada activo de información.
- b. La aplicación de una evaluación de riesgos periódica, denotará los criterios para la identificación y la priorización en el marco del cumplimiento de la estrategia institucional; lo que, orientará al tratamiento adecuado de los mismos que eviten una exposición a los activos de información.

- c. El INEC aplicará el GSI-PR-01 Procedimiento de evaluación y tratamiento de riesgos para la identificación de amenazas, vulnerabilidades, definición de la criticidad, riesgo inherente, controles, riesgo actual, tratamiento y acciones correctivas que disminuyan el riesgo al nivel más bajo aceptable por la institución.
- d. Cada Dirección deberá mantener actualizada la matriz de riesgo de la información y dar cumplimiento a los planes de acción establecidos

8.4. Gestión de Activos

- a. Cada uno de los activos de información debe tener una persona designada como responsable de mantener actualizado el inventario de activos de información, la clasificación de la información, evaluación de riesgos y de determinar los controles adecuados en términos de seguridad de la información.
- b. La información se debería clasificar tomando en cuenta su grado de sensibilidad e importancia conforme disposiciones legales, necesidad, prioridades, protección, entre otras en las siguientes categorías (ANEXO 2. CLASIFICACIÓN DE LA INFORMACIÓN):
 - Información publicada
 - Información interna
 - Información confidencial
 - Información reservada
- c. Sobre la base de la clasificación de la información y del nivel de riesgos de los activos se establecerán los controles necesarios y oportunos, tomando en cuenta incluso la factibilidad de cifrado para el envío y conservación de los mismos.
- d. Para la gestión de activos se establecerán normas específicas de cumplimiento obligatorio.

8.5. Seguridad de los recursos humanos

- a. Previo a la contratación laboral, los servidores, trabajadores, contratistas y usuarios de terceras partes deben ser aptos para las funciones para las cuales están siendo considerados y deberán conocer las responsabilidades del cargo a desempeñar.
- b. Durante la vigencia del contrato laboral los servidores, trabajadores, contratistas y usuarios de terceras partes estarán conscientes de las amenazas y preocupaciones a mitigar o solventar respecto a seguridad de la información, sus responsabilidades y roles, cumplimiento de la política, normas y procedimientos de seguridad de la información para el desempeño de su cargo, al igual que reducir el riesgo de un posible error humano.
- c. A la terminación de la contratación laboral o cambio de funciones de los servidores, trabajadores, los contratistas y los usuarios de terceras partes, se aplicará un proceso ordenado de salida o cambio para proteger los activos de información del INEC.
- d. El proceso disciplinario ante alguna violación de la seguridad de la información tomará en cuenta un trato imparcial y correcto e iniciará luego de haberse verificado y sustentado la violación de la seguridad, y de haber evaluado la motivación, la gravedad de la violación, su impacto en el negocio, recurrencia, capacitación recibida, legislación

vigente, entre otros factores. Todos los casos se sancionarán conforme las disposiciones normativas vigentes.

- e. Es imperante el cumplimiento de las normas para seguridad de los recursos humanos que se establezcan.

8.6. Seguridad física y del entorno

- a. Los edificios u oficinas que gestionen información confidencial, reservada e interna del INEC deben tener un perímetro seguro que impida el acceso no autorizado o sin control a las instalaciones que garanticen la confidencialidad, integridad y disponibilidad de la información.
- b. Los edificios u oficinas que gestione información del INEC deben proteger las áreas seguras con controles de acceso apropiados, para asegurar que sólo se permita el acceso a personal autorizado e impedir que desde las áreas de acceso al público se tenga fácil acceso a áreas críticas de tratamiento de información.
- c. Los edificios u oficinas que gestione información del INEC deben aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial; incluso, para el acceso al estacionamiento o áreas de carga y otros puntos por donde podrían ingresar personas no autorizadas.
- d. Los equipos deberán estar ubicados en áreas seguras y protegidas, es decir áreas que reduzcan el riesgo de acceso no autorizado; y, protegerse contra fallas del suministro de energía y agua. Así mismo el cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información deben estar protegidos contra interceptaciones o daños. Los equipos deben recibir mantenimiento adecuado para asegurar la disponibilidad constante.
- e. Se debe dar la seguridad a las áreas de procesamiento de información. Se entiende por área donde se procesa la información los siguientes:
 - Centros de Procesamiento normales o de emergencia.
 - Áreas con servidores, ya sean de procesamiento o dispositivos de comunicación.
 - Áreas donde se encuentren concentrados dispositivos de información.
 - Áreas donde se almacenen y guarden elementos de respaldo datos (CD, Discos Duros, Cintas etc.)
- f. Los equipos que son trasladados fuera de las instalaciones deben mantener controles que eviten pérdida de información, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones seguras de la institución.
- g. El INEC establecerá normas particulares de seguridad física y del entorno en términos de seguridad de la información para cumplimiento obligatorio institucional.

8.7. Gestión de comunicaciones y operaciones

- a. El INEC debe asegurar la operación correcta y segura de los servicios de procesamiento de información, aplicando incluso la opción de cifrado para transacciones, canal de comunicaciones y servicios en red.
- b. Para la operación correcta y segura de los servicios de procesamiento de información debe efectuarse acuerdos estrictos de servicios con terceros, una planificación de requerimientos tecnológicos para determinar la capacidad futura de los recursos informáticos, evitar y detectar la introducción de códigos maliciosos y códigos móviles no autorizados, una estrategia de respaldos, protecciones apropiadas a la red y a la infraestructura tecnológica, dispositivos de respaldos de la información, documentación técnica, bases de datos, intercambio de información y de información en tránsito, transacciones en línea, información publicada; y, efectuar el monitoreo de los sistemas y el registro de eventos de seguridad.
- c. Las normas de gestión de comunicaciones y operaciones serán aplicadas de manera inexcusable.

8.8. Control del acceso

- a. El acceso a la información, a los servicios de procesamiento de información y a los procesos de la Institución se debe controlar, de igual manera la asignación de los derechos de acceso a los sistemas y servicios de información; y, el acceso a los servicios de red tanto internos como externos.
- b. Se deberá concientizar a los usuarios sobre sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular con relación al uso de contraseñas y a la seguridad del equipo del usuario.
- c. Es recomendable implementar una política de escritorio y pantalla despejados, para reducir el riesgo de acceso no autorizado o daño de reportes, medios y servicios de procesamiento de información.
- d. El acceso de usuarios a los sistemas operativos, a aplicaciones y sistemas debe ser controlado a través de medios o mecanismos de seguridad apropiados. El acceso lógico al software de aplicación y a la información se debe limitar a usuarios autorizados.
- e. Cuando se utilizan dispositivos de computación móviles y de trabajo remoto debe implementarse protecciones adecuadas que impidan que esta forma de trabajo genere posibles amenazas o vulnerabilidades.
- f. Debe distinguirse la opción de cifrado de información en computadoras de escritorio, carpetas y para el acceso remoto.
- g. Es imperativa la aplicación de las normas de control de acceso establecidas en términos de seguridad de la información.

8.9. Adquisición, desarrollo y mantenimiento de sistemas de información

- a. Los sistemas de información adquiridos, obtenidos gratuitamente y desarrollados interna o externamente deben cumplir con los requisitos de seguridad de la información establecidos en la institución. Los nuevos sistemas cumplirán con requerimientos de seguridad de la información, previa a la compra, implementación o desarrollo respectivamente.
- b. Para garantizar el procesamiento correcto de un sistema de información, es requerido el cumplimiento de controles, validación, cifrado, firma electrónica para evitar errores, pérdidas o robo, acceso o modificaciones no autorizadas y uso inadecuado de la información; los que deben exponerse a procesos de pruebas, de evaluación de vulnerabilidades técnicas y de calidad.
- c. La aplicación de las normas para la adquisición, desarrollo y mantenimiento de sistemas de información deben ser observadas por todas las áreas que efectúan tareas de gestión relacionadas.

8.10. Gestión de los incidentes de la seguridad de la información

- a. Todos los empleados, contratistas, proveedores y otras personas que mantienen relación con el INEC deben comunicar, mediante mecanismos oportunos previamente establecidos, los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información de forma tal que permiten tomar las acciones correctivas oportunamente.
- b. Se aplicará un procedimiento formal con el señalamiento de las personas responsables para atender y solventar oportunamente los eventos y debilidades de seguridad de la información, así como la recolección de evidencias suficientes, monitoreo y planes de acción.
- c. Todo incidente de seguridad tomará en cuenta la aplicación de las normas de gestión de incidentes de la seguridad de la información establecidas en términos de seguridad de la información.

8.11. Gestión de la continuidad del negocio

- a. El INEC debe implementar un proceso de gestión de continuidad del negocio para minimizar el impacto ante desastres naturales, incendio, fallas operativas y funcionales, accidentes o acciones deliberadas, paros, huelgas, entre otros.
- b. Para la gestión de continuidad de negocio la institución debe efectuar un análisis de impacto sobre las posibles consecuencias que pudiera ocasionar los desastres, las fallas de la seguridad, la pérdida de activos y la disponibilidad del servicio.
- c. La gestión de la continuidad del negocio debe garantizar la disponibilidad de la información requerida para los procesos del negocio, por lo que la seguridad de la información debe ser una parte integral de todo el proceso de continuidad del negocio.
- d. Las normas de gestión de continuidad de negocio establecidas debe ser llevado a cabo por todos los procesos del INEC.

8.12. Cumplimiento

- a. Todos los servidores y servidoras cumplirán las disposiciones legales, estatutarias, reglamentarias, contractuales y otras formas legales relacionadas a seguridad de la información.
- b. Todos los servidores y servidoras cumplirán las disposiciones emanadas en las políticas, normas y procedimientos aprobados de seguridad de la información.
- c. El cumplimiento de todas las disposiciones debe ser evaluada anualmente por un tercero independiente que brinde claridad sobre la situación actual del INEC en términos de Seguridad de la Información.
- d. Las normas para la gestión de cumplimiento serán cumplidas en función de un adecuado control interno institucional.

9. Aceptación del Riesgo (Excepciones y autorizaciones)

- a. Toda excepción debe estar autorizada por un Director o Coordinador dentro de sus áreas de responsabilidad, con la implicancia de que fue evaluada previamente por el citado funcionario sobre el posible impacto y riesgo que esa excepción podría provocar en el INEC, en tal sentido, el Director o Coordinador asume el riesgo o vulnerabilidad que está ocasionando y será responsable de la materialización del/la mismo(a).
- b. Cuando la excepción tiende a la posibilidad de afectar a toda la institución o a su reputación, el Comité de Seguridad de la Información debe conocerla antes de que se habilite lo requerido en la excepción y su pronunciamiento se registrará en el acta correspondiente.
- c. Si como consecuencia de la autorización de una excepción se materializa una amenaza o una vulnerabilidad, sin que el comité la haya conocido, el comité de seguridad de la información solicitará la aplicación de las acciones disciplinarias al Director o Coordinador que autorizó la misma y la hará constar en el acta respectiva.
- d. Para el caso particular de que la autorización de excepción haya sido emitida por el Director(a) Ejecutivo(a) o su delegado(a), sin que el comité lo haya conocido previamente, el comité emitirá su pronunciamiento en el acta de reunión.

10. Glosario de términos

Fuente: ISO/IEC 27000

Término	Significado
Acción correctiva	(Inglés: Corrective action). Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

Término	Significado
Acción preventiva	(Inglés: Preventive action). Medida de tipo pro-activo orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001:2005. En ISO 27001:2013, ya no se emplea; ha quedado englobada en Riesgos y Oportunidades.
Aceptación del riesgo	(Inglés: Risk acceptance). Decisión informada de asumir un riesgo concreto.
Activo	(Inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
Alcance	(Inglés: Scope). Ámbito de la organización que queda sometido al SGSI.
Amenaza	(Inglés: Threat). Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
Análisis de riesgos	(Inglés: Risk analysis). Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
Análisis de riesgos cualitativo	(Inglés: Qualitative risk analysis). Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.
Análisis de riesgos cuantitativo	(Inglés: Quantitative risk analysis). Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.
Auditor	(Inglés: Auditor). Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.
Auditoría	(Inglés: Audit). Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.
Autenticidad	(Inglés: Authenticity). Propiedad de que una entidad es lo que afirma ser.
Cifrado, cifrar	(Inglés; encrypt). El cifrado de datos es el proceso por el que una información legible se transforma mediante un algoritmo (llamado cifra) en información ilegible, llamada criptograma o secreto. Esta información ilegible se puede enviar a un destinatario con muchos menos riesgos de ser leída por terceras partes. El destinatario puede volver a hacer legible la información, descifrarla, introduciendo la clave del cifrado. A menudo se denomina “encriptación” a este proceso, pero es incorrecto, ya que esta palabra no

Término	Significado
	existe en castellano; se ha importado del inglés “encrypt”, que se debe traducir como “cifrar”, y por tanto el proceso se debe denominar “cifrado”. Fuente: Wiki -Ekonsulta
Compromiso de la Dirección	(Inglés: Management commitment). Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. La versión de 2013 de ISO 27001 lo engloba bajo la cláusula de Liderazgo.
Confidencialidad	(Inglés: Confidentiality). Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
Contramedida	(Inglés: Countermeasure). Véase: Control.
Control	Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
Control correctivo	(Inglés: Corrective control). Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.
Control detectivo	(Inglés: Detective control). Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.
Control disuasorio	(Inglés: Deterrent control). Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.
Control preventivo	(Inglés: Preventive control). Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Término	Significado
Corrección	(Inglés: Correction). Acción para eliminar una no conformidad detectada. Si lo que se elimina es la causa de la no conformidad, véase acción correctiva.
Declaración de aplicabilidad	(Inglés: Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.
Desastre	(Inglés: Disaster). Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.
Directiva o directriz	(Inglés: Guideline). Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.
Disponibilidad	(Inglés: Availability). Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
Entidad de acreditación	(Inglés: Accreditation body). Un organismo oficial que acredita a las entidades certificadoras como aptas para certificar según diversas normas. Suele haber una por país. Son ejemplos de entidades de acreditación: ENAC (España), UKAS (Reino Unido), EMA (México), OAA (Argentina), etc. En nuestra sección Normalización y Acreditación figuran todas las de países de habla hispana.
Entidad de certificación	(Inglés: Certification body). Una empresa u organismo acreditado por una entidad de acreditación para auditar y certificar según diversas normas (ISO 27001, ISO 9001, ISO 14000, etc.) a empresas usuarias de sistemas de gestión.
Entidad de normalización	(Inglés: Standards body). Un organismo oficial que genera y publica normas. Suele haber una por país. Son ejemplos de entidades de normalización: AENOR (España), BSI (Reino Unido), DGN (México), IRAM (Argentina), etc. En nuestra sección Normalización y Acreditación figuran todas las de países de habla hispana.

Término	Significado
Estimación de riesgos	(Inglés: Risk evaluation). Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.
Evaluación de riesgos	(Inglés: Risk assessment). Proceso global de identificación, análisis y estimación de riesgos.
Evidencia objetiva	(Inglés: Objective evidence). Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.
Gestión de claves	(Inglés: Key management). Controles referidos a la gestión de claves criptográficas.
Gestión de incidentes de seguridad de la información	(Inglés: Information security incident management). Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
Gestión de riesgos	(Inglés: Risk management). Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
Identificación de riesgos	(Inglés: Risk identification). Proceso de encontrar, reconocer y describir riesgos.
IEC	International Electrotechnical Commission. Organización internacional que publica estándares relacionados con todo tipo de tecnologías eléctricas y electrónicas.
Impacto	(Inglés: Impact). El coste para la empresa de un incidente - de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc-.
Incidente de seguridad de la información	(Inglés: Information security incident). Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Integridad	(Inglés: Integrity). Propiedad de la información relativa a su exactitud y completitud.

Término	Significado
Inventario de activos	(Inglés: Assets inventory). Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
ISO	Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).
ISO/IEC 27001	Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.
ISO/IEC 27002	Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.
No conformidad	(Inglés: Nonconformity). Incumplimiento de un requisito.
No repudio	Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.
Objetivo	(Inglés: Objective). Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.
Parte interesada	(Inglés: Interested party / Stakeholder). Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
PDCA	Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.

Término	Significado
Plan de continuidad del negocio	(Inglés: Business Continuity Plan). Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.
Plan de tratamiento de riesgos	(Inglés: Risk treatment plan). Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
Política de escritorio despejado	(Inglés: Clear desk policy). La política de la empresa que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.
Proceso	(Inglés: Process). Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.
Propietario del riesgo	(Inglés: Risk owner). Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.
Recursos de tratamiento de información	(Inglés: Information processing facilities). Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.
Riesgo	(Inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
Riesgo residual	(Inglés: Residual risk). El riesgo que permanece tras el tratamiento del riesgo.
Salvaguarda	(Inglés: Safeguard). Véase: Control.
Segregación de tareas	(Inglés: Segregation of duties). Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.
Seguridad de la información	(Inglés: Information security). Preservación de la confidencialidad, integridad y disponibilidad de la información.
Selección de controles	(Inglés: Control selection). Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.
SGSI	(Inglés: ISMS). Véase: Sistema de Gestión de la Seguridad de la Información.

Término	Significado
Sistema de Gestión de la Seguridad de la Información	(Inglés: Information Security Management System). Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
Tratamiento de riesgos	(Inglés: Risk treatment). Proceso de modificar el riesgo, mediante la implementación de controles.
Trazabilidad	(Inglés: Accountability). Según [CESID:1997]: Calidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
Vulnerabilidad	(Inglés: Vulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas.

11. Anexos




ANEXO 1 - Roles y Responsabilidades

ANEXO 2 – Clasificación de la Información

12. Aprobación

Fecha final de aprobación: Quito DM, 15 de octubre de 2020.

13. Registro de firmas

Nombre	Cargo	Firma
Econ. Diego Andrade	Director Ejecutivo INEC	 Firmado electrónicamente por: DIEGO OSWALDO ANDRADE ORTIZ
Mat. Víctor Bucheli	Subdirector General	 Firmado electrónicamente por: VICTOR HUGO BUCHELI LEON
Mgs. David Muñoz	Coordinador General Técnico de Planificación Normativas de Calidad Estadística, Encargado y Presidente Comité de Seguridad de la Información	 Firmado electrónicamente por: ALEJANDRO DAVID MUNOZ BRICENO

Nombre	Cargo	Firma
Mgs. Jenny Delgado Enríquez	Oficial de Seguridad de la Información	JENNY ELIZABETH DELGADO ENRIQUEZ Digitally signed by JENNY ELIZABETH DELGADO ENRIQUEZ Date: 2020.10.16 16:10:38 -05'00'
Abg. María Eugenia Morales	Directora de Asesoría Jurídica	MARIA EUGENIA MORALES CORTEZ - 1721997193 Firmado digitalmente por MARIA EUGENIA MORALES CORTEZ - 1721997193 Fecha: 2020.10.16 18:36:49 -05'00'
Mgs. Diana Soriano	Directora de Comunicación Social	 Firmado electrónicamente por: DIANA DEL ROCIO SORIANO ONA
Sra. Yolanda Rosero	Directora de Planificación y Gestión Estratégica Subrogante	 Firmado electrónicamente por: YOLANDA MARISELA ROSERO ORDONEZ
Ing. Paulina Suárez	Directora de Tecnologías de la Información y Comunicación	 Firmado electrónicamente por: MERY PAULINA SUAREZ LEON
Sra. Diana Molina	Coordinadora General Administrativa Financiera	 Firmado electrónicamente por: DIANA GABRIELA MOLINA CARRERA
Sra. María Fernanda Cifuentes	Directora Administrativa	 Firmado electrónicamente por: MARIA FERNANDA CIFUENTES GARCIA
Sra. Silvana Guambuete	Directora Financiera, Encargada	 Firmado electrónicamente por: SILVANA FAVIOLA GUAMBUGUETE PAREDES
Abg. María José Arrobo	Directora de Administración de Recursos Humanos	 Firmado electrónicamente por: MARIA JOSE ARROBO BARRAGAN
Srta. Mónica Alexandra Torres	Directora de Planificación Estadística del SEN, Subrogante	 Firmado electrónicamente por: MONICA ALEXANDRA TORRES ROSERO
Srta. Ivonne Benítez	Directora de Normativas Estandarización y Calidad Estadística Encargada	 Firmado electrónicamente por: IVONNE VANESSA BENITEZ MALACATUS
Sr. David Sánchez	Coordinador General Técnico de Producción Estadística	DAVID SANTIAGO SANCHEZ SORIA Firmado digitalmente por DAVID SANTIAGO SANCHEZ SORIA Fecha: 2020.10.26 10:40:37 -05'00'
Ing. David Caín	Director de Registros Administrativos, Encargado	 Firmado electrónicamente por: VICTOR DAVID CAIN URQUIZO

Nombre	Cargo	Firma
Ing. Christian Garcés	Director de Infraestructura Estadística y Muestreo	 Firmado electrónicamente por: CHRISTIAN MARCELO GARCÉS MAYORGA
Srta. Viviana Ruiz	Directora de Cartografía Estadística y Operaciones de Campo	 Firmado electrónicamente por: VIVIANA CAROLINA RUIZ VILLAFUERTE
Sra. María Soledad Carrera	Directora de Estadísticas Socio-Demográficas Encargada	 Firmado electrónicamente por: MARIA SOLEDAD CARRERA CLAVIJO
Econ. Darío Vélez	Director de Estadísticas Económicas	FAUSTO DARIO VELEZ JARA Firmado digitalmente por FAUSTO DARIO VELEZ JARA Fecha: 2020.10.30 11:27:15 -05'00'
Econ. David Salazar	Director de Estadísticas Agropecuarias y Ambientales	 Firmado electrónicamente por: ARMANDO DAVID SALAZAR MENDEZ
Sra. María Isabel García	Coordinadora General Técnica de Innovación en Métricas y Análisis de la Información Encargada	 Firmado electrónicamente por: MARIA ISABEL GARCIA MOSQUERA
Sra. Natalia Garzón	Directora de Estudios y Análisis de la Información Subrogante	 Firmado electrónicamente por: NATALIA CAROLINA GARZON DURANGO
Ing. Fernando Goyes	Coordinador Zonal 3 - Centro, Encargado	 Firmado electrónicamente por: LUIS FERNANDO GOYES MORALES
Mgs. Joffre León	Coordinador Zonal 8 INEC (E)	 Firmado electrónicamente por: JOFFRE LUIS LEON
Lcdo. José Ayala	Coordinador Zonal 6 - Sur (Enc)	 Firmado electrónicamente por: JOSE ROSENDO AYALA CHICAIZA

CADA HECHO DE TU VIDA *Cuenta*



@ecuadorencifras



@InecEcuador



t.me/ecuadorencifras



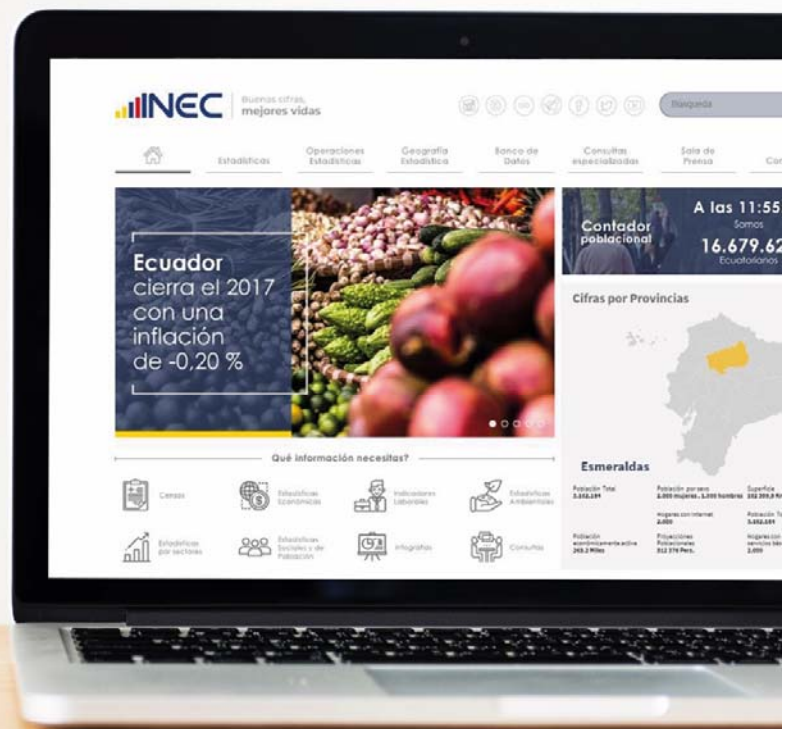
INEC/Ecuador



INECEcuador



INEC Ecuador



ANEXO 1

ROLES Y RESPONSABILIDADES

Política relacionada superior: Política de Seguridad de la Información

Además de las responsabilidades establecidas en el Estatuto Orgánico de Gestión Organizacional por Procesos y otras resoluciones, se incluyen los siguientes roles y responsabilidades.

Historial de cambios:

Fecha	Cambios realizados al documento	Elaborado por:
21-oct-2019	Propuesta inicial	Willian Franco
15-oct-2020	Actualización	Jenny Delgado E.

Contenido

1. Para servidores, trabajadores y proveedores:	3
2. Para la persona responsable de cada proceso o proyecto:	3
3. Para la Dirección de Administración de Recursos Humanos.....	4
4. Para la Dirección Administrativa	4
5. Para la Dirección de Asesoría Jurídica	5
6. Para la persona responsable de la Seguridad Informática.....	5
7. Para el Oficial de Seguridad de la Información:	6
8. Para el Comité de Seguridad de la Información (CSI)	7
9. Para Auditoría Interna.....	8
10. Para el Director Ejecutivo	8
11. Para personas que no forman parte del INEC.....	9

1. Para servidores, trabajadores y proveedores:

La seguridad de la información es responsabilidad de todos los servidores y trabajadores de la institución, proveedores de servicios, pasantes y personal contratado bajo la modalidad de servicios profesionales o técnicos especializados. En el INEC existen diferentes cargos y roles que deben desempeñar en la gestión de un proceso de seguridad efectivo para su cumplimiento. Todos los servidores deben poner en práctica y recomendar las disposiciones de seguridad de la información en sus actividades cotidianas, incluso cuando participen en reuniones o en comités. Entre sus funciones están:

- a. Cumplir las disposiciones de la política de seguridad de la información.
- b. Utilizar los recursos del INEC únicamente para propósitos de ejecución de su cargo o contrato.
- c. Participar obligatoriamente en programas de capacitación y concienciación.
- d. Actuar activa y proactivamente para garantizar la confidencialidad, integridad y disponibilidad de la información.
- e. Concienciar y alegar la protección de la información aun cuando no sea de su responsabilidad directa.
- f. Reportar eventos, debilidades, vulnerabilidades e incidentes de seguridad física y seguridad informática al Oficial de Seguridad de la Información.

2. Para la persona responsable de cada proceso o proyecto:

Los Coordinadores, Directores y sus delegados formales, serán responsables del control interno respecto al cumplimiento de seguridad de la información en su respectiva dirección, tendrán las siguientes funciones:

- a. Mantener un inventario actualizado de los activos de información.
- b. Evaluación del riesgo de seguridad de la información de sus activos de información.
- c. Clasificación de la información de datos e información bajo su responsabilidad.
- d. Reportar eventos o incidentes de seguridad suscitados en su Dirección.
- e. Verificar el cumplimiento de la política, normas, procesos y procedimientos de seguridad de la información y de la incorporación de controles en sus propias políticas y procedimientos de gestión de área.
- f. Involucrar al Oficial de Seguridad de la Información en la actualización de sus procesos, procedimientos, productos y servicios con la finalidad de que las políticas, normas y procedimientos de seguridad de la información sean considerados.
- g. Autorizar los productos y servicios, y los sistemas de información bajo su responsabilidad requeridos en su proceso.
- h. Apoyar en la concienciación de su personal en términos de seguridad de la información.
- i. Autorizar la creación, modificación y eliminación de los accesos a los sistemas de información de su responsabilidad y revisar al menos anualmente los accesos vigentes.
- j. Responsabilizarse del riesgo y asumir las consecuencias al permitir o evitar actividades o controles contrarias a las definidas en políticas, normas, procedimientos, metodologías u otra relacionada.
- k. Formalizar la entrega de bienes, equipos, software, documentación e información por parte de servidores, servidoras, pasantes, proveedores, consultores entre otros, ante la finalización del contrato y posteriormente requerir formalmente la eliminación de

información del INEC localizada en equipos, almacenamiento en el internet y/o en las instalaciones de propiedad de las personas antes citadas.

- l. En caso de desvinculación o cambio de funciones de los servidores(as) que tienen la custodia de información confidencial, acceso directo a base de datos, custodia y uso de usuarios genéricos con privilegios de administración, deberán firmar una declaración que no mantienen copias personales de información y que los usuarios genéricos privilegiados con sus contraseñas los mantendrán en reserva y no serán utilizados.
- m. Monitorear las actividades del personal bajo su supervisión con comportamiento inusual en el manejo de datos e información.
- n. Garantizar que toda actividad o práctica de gestión de los servidores, servidoras, proveedores y contratistas quede registrada en procedimientos, instructivos, guías o metodologías.
- o. Llenar y entregar un check-list mensual de cumplimiento por parte de cada Dirección.

3. Para la Dirección de Administración de Recursos Humanos

- a. Verificar la información presentada del personal seleccionado, previo a su contratación, tales como: referencias profesionales y personales, certificado de antecedentes penales, la que consta en su hoja de vida, títulos, experiencia, entre otros.
- b. Entregar formalmente a los servidores y servidoras sus funciones y responsabilidades.
- c. Establecer conjuntamente con las Direcciones y Coordinaciones del INEC los perfiles de acceso para todos los cargos del INEC y direccionar a DITIC el listado de esos perfiles.
- d. Reportar anticipadamente a DITIC la salida y cambio de funciones de los servidores y servidoras del INEC.
- e. Formalizar un acuerdo de uso de información y confidencialidad o no-divulgación de la información con los empleados, pasantes y otro tipo de contratación, antes de que tengan acceso a la información.
- f. Establecer un proceso disciplinario formal ante el cometimiento de violaciones comprobadas a la seguridad de la información.
- g. Implementar el uso de una identificación visible para todo el personal.
- h. Verificar que las firmas en el formulario de Paz y Salvo se haya suscrito por las distintas áreas antes de iniciar el proceso de desvinculación, y posterior archivo.
- i. Llenar y entregar un checklist mensual de cumplimiento.

4. Para la Dirección Administrativa

- a. Establecer un adecuado control de acceso físico para personas que ingresan al edificio y para el ingreso a áreas críticas; incluso, para el ingreso de vehículos propios o de terceros.
- b. Establecer mecanismos de alarmas de incendio y protecciones contra descargas eléctricas, así como el direccionamiento a puertas que faciliten un adecuado proceso de evacuación del edificio.
- c. Establecer mecanismos de vigilancia ya sea por circuito cerrado de televisión, equipos de grabación, cámaras, equipos de video y audio, etc., propios y/o de terceros.
- d. Establecer el uso obligatorio de una identificación visible para todos los visitantes.
- e. Prohibir el uso de materiales combustibles, inflamables o peligrosos en áreas críticas; así como la de comer, beber y fumar en esas áreas.
- f. Establecer mecanismos para salvaguardar la falta de suministro de energía eléctrica (UPS y generador)

- g. Establecer un mecanismo para monitoreo de humedad, aire acondicionado, agua, electricidad, calefacción y ventilación.
- h. Implementar procedimientos para el ingreso y salida de cualquier equipo, bien o dispositivo informático fijo o móvil.
- i. Establecer mecanismo y procedimiento para la protección del cableado de la red contra interceptación y daño, y controlar el acceso a los módulos de cableado de conexión (patch panel) y cuartos de cableado.
- j. Monitorear y verificar el cumplimiento de las normas de Seguridad Física y del entorno.
- k. Llenado y entrega de un check-list mensual de cumplimiento por parte de cada Dirección.

5. Para la Dirección de Asesoría Jurídica

- a. Brindar soporte de índole jurídico ante la protección de datos e información establecida en leyes, resoluciones y otros.
- b. Apoyar en la revisión de políticas y normas conforme lo dicte la normativa vigente.
- c. Apoyar en la elaboración del formato de Acuerdos de confidencialidad.
- d. Apoyar en la elaboración del formato en el que cada servidor, servidora, pasante y otro tipo de contrato confirma haber leído la política y normas de seguridad de la información y se comprometen a cumplirla.

6. Para la persona responsable de la Seguridad Informática

Es el servidor o servidora responsable o encargada de la Gestión de Seguridad Informática, cuya principal actividad es evaluar, revisar y monitorear en términos de seguridad las actividades realizadas al interior de la Dirección de Tecnologías de la Información y Comunicación el cumplimiento de las disposiciones de políticas, normas, procesos y procedimientos de seguridad de la información.

- a. Consolidar y proporcionar el inventario de activos de información de tecnología al Oficial de Seguridad de la Información.
- b. Verificar que el inventario de activos de información de tecnología se encuentre actualizado.
- c. Obtener del Oficial de Seguridad de la Información o de la persona responsable de cada proceso el riesgo y clasificación de la información de los activos y distribuirlo al interior de DITIC para que se implementen los niveles de protección y contingencia apropiados de acuerdo a los planes de acción establecidos por los dueños de los procesos en coordinación con DITIC y el Oficial de Seguridad de la Información.
- d. Emitir consultas al Oficial de Seguridad de la Información respecto a las disposiciones vigentes de seguridad de tecnologías actuales y nuevas tecnologías.
- e. Verificar que DITIC disponga de políticas, normas, procedimientos e instructivos de sus actividades inherentes a tecnología – soporte, infraestructura, desarrollo - y apoyar a que las disposiciones relacionadas a seguridad de la información se hayan incluido en las mismas.
- f. Involucrarse en el proceso de ciclo de vida de desarrollo de software y en el proceso de control de cambios para la evaluación del posible impacto operativo a nivel de seguridad de los cambios previstos a sistemas, equipamiento, comunicación y red, para confirmar la compatibilidad de hardware y software, para la definición de las actividades y responsables en ese proceso y para verificar su correcta implementación.

- g. Establecer y evaluar la independencia de ambientes de desarrollo, pruebas y producción.
- h. Consolidar de las áreas de DITIC la necesidad de capacidad de recursos informáticos y de comunicaciones actuales y proyectadas a 2 años relacionadas a hardware y software obligatorio para la protección de seguridad informática.
- i. Conocer y monitorear la obtención de respaldo de información y copias que realice DITIC a los datos e información del INEC.
- j. Evaluar y verificar el cumplimiento de un procedimiento que brinde protección y control para la generación y custodia de respaldos y copias de información en DITIC
- k. Revisar el registro de actividades (log) para todos los recursos informáticos críticos, al menos de personal operativo y personal con privilegios de administración.
- l. Verificar y coordinar el cumplimiento de la política, normas, procesos y procedimientos relacionados a seguridad de la información en DITIC.
- m. Gestionar el cierre de incidentes de seguridad de la información relacionados a recursos de tecnología.
- n. Controlar que se realice el cambio de contraseñas de usuarios genéricos con privilegios de administración (root, admin, administrator, etc.) y contraseñas de equipos de seguridad hayan sido cambiados en un plazo máximo de 48 horas ante la salida de alguno de los custodios de esos usuarios.
- o. Presentar un checklist mensual al Oficial de Seguridad de la Información de cumplimiento en términos de seguridad informática.
- p. Otras actividades que por naturaleza de su cargo de “seguridad informática” deban ser realizadas, previa comunicación del Oficial de Seguridad de la Información.

7. Para el Oficial de Seguridad de la Información:

7.1. Responsabilidades

- a. Generar propuestas para la elaboración de la documentación esencial del Esquema Gubernamental de Seguridad de la información.
- b. Establecer e incluir metodologías, formatos y criterios en términos de seguridad de la información.
- c. Proponer la elaboración de procedimientos en términos de seguridad de la información, como procedimientos para respuesta a incidentes, control de cambios, monitoreo, evaluaciones independientes, capacitación, continuidad de negocio, entre otros.
- d. Asesorar a los funcionarios en la ejecución del Estudio de Gestión de Riesgos de Seguridad de la Información en las diferentes áreas-
- e. Verificar el cumplimiento de las normas, procedimientos y controles de seguridad institucionales establecidos.
- f. Establecer planes de capacitación y concienciación en términos de seguridad de la información y continuidad de negocio.
- g. Elaborar el material y brindar la concienciación y capacitación a los empleados; y, autorizar el material de capacitación de proveedores.
- h. Verificar y autorizar ejercicios de Ethical Hacking o ejercicios para tratar de vulnerar prácticas internas.
- i. Apoyar en la definición e implementación de controles a nivel de procedimientos en los distintos procesos y proyectos de la institución, propios o efectuados por terceros, en función de las políticas, normas y procedimientos de seguridad de la información.

- j. Tomar como referencia la serie de normas técnicas ecuatorianas INEN ISO/IEC 27000, según el ámbito de cada norma, para las propuestas de política, normas, procedimientos, controles, entre otras.
 - k. Informar al Comité de Seguridad de la información, el avance de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), así como las alertas que impidan su implementación.
 - l. Previa terminación de sus funciones el Oficial de Seguridad realizará la transferencia de la documentación e información de la que fue responsable al nuevo Oficial de seguridad, en caso de ausencia, al Comité de Seguridad de la Información.
- 7.2. En caso de ausencia temporal o definitiva del Oficial de Seguridad de la Información, el cargo será cubierto temporalmente por la persona que presida el CSI o su delegado.
- 7.3. Por segregación de funciones, el Oficial de Seguridad de la Información no debe formar parte del equipo de DITIC, puesto que deberá mantener su independencia para observar las necesidades de seguridad entre la estrategia de la Institución y tecnología.

8. Para el Comité de Seguridad de la Información (CSI)

- 8.1. Estará conformado obligatoriamente por:
- a. El Coordinador/a General Técnico de Planificación, Normativas y Calidad Estadística, quien lo presidirá.
 - b. El Coordinador/a General Técnico de Producción Estadística
 - c. Coordinador/a General Técnico de Innovación en Métricas y Análisis de la Información
 - d. Coordinador/a General Administrativo Financiero
 - e. Los Coordinadores Zonales
 - f. El Director/a de Planificación y Gestión Estratégica
 - g. El Director/a de Comunicación Social
 - h. El Director/a de Tecnologías de la Información y Comunicación.
- 8.2. En las reuniones del CSI, los miembros mencionados en el literal 8.1 participaran con voz y voto en la toma de cualquier decisión.
- 8.3. El voto dirimente será el del Presidente o Presidenta del Comité de Seguridad de la Información
- 8.4. En el CSI participarán el Oficial de Seguridad de la Información y el Director/a de Asesoría Jurídica, en calidad de asesor, quienes tendrán voz pero no voto.
- 8.5. Las funciones del Comité de Seguridad de la Información (CSI) serán:
- a. Revisar la versión inicial y las actualizaciones de la política y normas de seguridad de la información previa a trasladarlo a la Máxima Autoridad. La política y normas deben ser revisadas al menos por la Dirección Jurídica en términos de cumplimiento legal, Dirección de Tecnologías de la Información y Comunicación en términos de cumplimiento tecnológico, la Dirección de Recursos Humanos en términos de cumplimiento de la contratación de empleados, la Dirección Administrativa en términos de cumplimiento de la seguridad física.

- b. Gestionar la aprobación de las políticas y normas institucionales en materia de seguridad de la información, ante la Máxima Autoridad de la Institución.
- c. Realizar el seguimiento de los cambios significativos de los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- d. Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información, con nivel de impacto alto.
- e. Coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, en base al EGSi.
- f. Promover la difusión de la seguridad de la información dentro de la institución.
- g. Coordinar el proceso de gestión de la continuidad de la operación de los servicios y sistemas de información de la institución frente a incidentes de seguridad imprevistos.
- h. Presentar bimensualmente al Director Ejecutivo un informe de gestión, precisando las acciones adoptadas para la actualización y mejora del Esquema Gubernamental de Seguridad de la Información (EGSi).
- i. Reportar a la máxima autoridad las alertas que impidan la implementación del Esquema Gubernamental de Seguridad de la Información (EGSi).
- j. Designar formalmente a un servidor/a como Oficial de Seguridad de la Información, quien no pertenecerá al área de Tecnologías de la Información y reportará al Comité de Seguridad de la Información y a la Máxima autoridad de la Institución.
- k. Nombrar de sus miembros al servidor/a quien actuará como secretario y será el responsable de levantar un acta por cada una de las reuniones.
- l. Recomendar a la máxima autoridad mecanismos que viabilicen la implementación del Esquema Gubernamental de Seguridad de la Información (EGSi).
- m. Velar por el cumplimiento de las demás disposiciones que sobre la materia llegare a emitir el Ministerio de Telecomunicaciones y de la Sociedad de la Información.

8.6. El Director Ejecutivo, mediante resolución, podrá asignar la responsabilidad y las funciones del CSI descritas en éste apartado, a otra(s) instancia(s) del INEC.

9. Para Auditoría Interna

- a. Incorporar en su plan de trabajo anual, revisiones independientes de la gestión de seguridad por parte de cada uno de los responsables establecidos en este documento.
- b. Efectuar la revisión independiente y comunicar los resultados de la misma.
- c. Registrar y conservar los resultados de las revisiones y las acciones correctivas solicitadas y llevadas a cabo.

10. Para el Director Ejecutivo

- a. Aprobar la política y normas de seguridad de la información.
- b. Disponer la publicación de ésta política y sus normas.
- c. Conocer el estado de cumplimiento de la política, normas, procesos y procedimientos de seguridad de la información a través de las actas suscritas por el CSI.
- d. Pronunciarse sobre las prácticas de seguridad de la información.

11. Para personas que no forman parte del INEC

Son las personas naturales o jurídicas que requieren el servicio del INEC en la provisión de datos e información y los proveedores que gestionan los datos e información del INEC.

- a. Guardar absoluta reserva sobre los datos e información que se entrega.
- b. Solamente podrán publicar la información que el INEC lo autorice, siempre y cuando la misma esté sujeta al principio de publicidad.
- c. Todo dato e información proporcionada por el INEC y que haya sido publicada, debe referir en la publicación que fue obtenida del INEC y garantizar los derechos reservados.
- d. Todo dato e información proporcionado por el INEC de manera particular, no debe ser expuesto en una publicación que directamente lucre de la misma.
- e. El acceso al laboratorio de procesamiento de datos del INEC debe tener previamente una evaluación técnica de factibilidad y firmado el respectivo acuerdo de acceso.
- f. Si es un proveedor de servicios para el tratamiento de la información del INEC, debe garantizar la protección de la misma sobre la base de políticas, normas y procedimientos de seguridad de la información.
- g. El proveedor de servicios y su personal deben firmar el convenio o Acuerdo de Uso de Información y de confidencialidad proporcionado por el INEC, previo a proveer el servicio.
- h. El proveedor de servicios debe evaluar sus prácticas de seguridad de la información sobre la base de la matriz de evaluación proporcionada por el INEC y establecer planes de acción correctiva a corto plazo para aquellos temas de incumplimiento.
- i. Al terminar el servicio por parte del proveedor, debe garantizar la devolución y entrega de la información al INEC y la eliminación segura de la misma de los equipos e instalaciones del proveedor con la presencia de un representante del INEC.

Este documento puede ser actualizado con la aprobación del Comité de Seguridad de la Información siempre y cuando no altere las responsabilidades del CSI y del Director Ejecutivo, cambios de responsabilidades a estas instancias las aprueba únicamente el Director Ejecutivo.

ANEXO 2

CLASIFICACIÓN DE LA INFORMACIÓN

Política relacionada superior: Política de Seguridad de la Información

Historial de cambios:

Fecha	Cambios realizados al documento	Elaborado por:
21-oct-2019	Propuesta inicial	Willian Franco
15-oct-2020	Actualización	Jenny Delgado

Contenido

1.	ANÁLISIS:	3
I.	De la información Pública	3
II.	De la Información que está sujeta al principio de publicidad.....	3
III.	De la información Reservada	5
IV.	De la información Confidencial	6
V.	De otro tipo de información.....	7
VI.	Conclusión del Análisis	8

1. ANÁLISIS:

I. De la información Pública:

El numeral 2 del artículo 18 de la Constitución de la República del Ecuador, dispone: *“Todas las personas, en forma individual o colectiva, tiene derecho a: (...) 2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información”*.

El Principio de Publicidad de la Información Pública establecido en el artículo 1 de la *“Ley Orgánica de Transparencia y Acceso a la Información Pública”*, dispone: *“El acceso a la información pública es un derecho de las personas que garantiza el Estado. Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema materia de la información tengan participación del Estado o sean concesionarios de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONGs), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley”*. En concordancia a lo señalado en el artículo 5 de la misma Ley Orgánica, que establece: *“Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado”*.

El artículo 4 de la Ley Orgánica del Sistema Nacional de Datos Públicos: *“Responsabilidad de la información.- Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información (...)”*.

II. De la Información que está sujeta al principio de publicidad:

La Ley Orgánica de Transparencia y Acceso a la Información Pública”, establece:

- *“Art. 5.- Información Pública.- Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado.”*
- *“Art. 7.- Difusión de la Información Pública.- Por la transparencia en la gestión administrativa que están obligadas a observar todas las instituciones del Estado que conforman el sector público en los términos del artículo 118 de la Constitución Política de la República y demás entes señalados en el artículo 1 de la presente Ley, difundirán a través de un portal de información o página web, así como de los medios necesarios a*

disposición del público, implementados en la misma institución, la siguiente información mínima actualizada, que para efectos de esta Ley, se la considera de naturaleza obligatoria:

- a) Estructura orgánica funcional, base legal que la rige, regulaciones y procedimientos internos aplicables a la entidad; las metas y objetivos de las unidades administrativas de conformidad con sus programas operativos;
- b) El directorio completo de la institución, así como su distributivo de personal;
- c) La remuneración mensual por puesto y todo ingreso adicional, incluso el sistema de compensación, según lo establezcan las disposiciones correspondientes;
- d) Los servicios que ofrece y las formas de acceder a ellos, horarios de atención y demás indicaciones necesarias, para que la ciudadanía pueda ejercer sus derechos y cumplir sus obligaciones;
- e) Texto íntegro de todos los contratos colectivos vigentes en la institución, así como sus anexos y reformas;
- f) Se publicarán los formularios o formatos de solicitudes que se requieran para los trámites inherentes a su campo de acción;
- g) Información total sobre el presupuesto anual que administra la institución, especificando ingresos, gastos, financiamiento y resultados operativos de conformidad con los clasificadores presupuestales, así como liquidación del presupuesto, especificando destinatarios de la entrega de recursos públicos;
- h) Los resultados de las auditorías internas y gubernamentales al ejercicio presupuestal;
- i) Información completa y detallada sobre los procesos precontractuales, contractuales, de adjudicación y liquidación, de las contrataciones de obras, adquisición de bienes, prestación de servicios, arrendamientos mercantiles, etc., celebrados por la institución con personas naturales o jurídicas, incluidos concesiones, permisos o autorizaciones;
- j) Un listado de las empresas y personas que han incumplido contratos con dicha institución;
- k) Planes y programas de la institución en ejecución;
- l) El detalle de los contratos de crédito externos o internos; se señalará la fuente de los fondos con los que se pagarán esos créditos. Cuando se trate de préstamos o contratos de financiamiento, se hará constar, como lo prevé la Ley Orgánica de Administración Financiera y Control, Ley Orgánica de la Contraloría General del Estado y la Ley Orgánica de Responsabilidad y Transparencia Fiscal, las operaciones y contratos de crédito, los montos, plazo, costos financieros o tipos de interés;
- m) Mecanismos de rendición de cuentas a la ciudadanía, tales como metas e informes de gestión e indicadores de desempeño;
- n) Los viáticos, informes de trabajo y justificativos de movilización nacional o internacional de las autoridades, dignatarios y funcionarios públicos;
- o) El nombre, dirección de la oficina, apartado postal y dirección electrónica del responsable de atender la información pública de que trata esta Ley;
- p) La Función Judicial y el Tribunal Constitucional, adicionalmente, publicarán el texto íntegro de las sentencias ejecutoriadas, producidas en todas sus jurisdicciones;
- q) Los organismos de control del Estado, adicionalmente, publicarán el texto íntegro de las resoluciones ejecutoriadas, así como sus informes, producidos en todas sus jurisdicciones;
- r) El Banco Central, adicionalmente, publicará los indicadores e información relevante de su competencia de modo asequible y de fácil comprensión para la población en general;

- s) *Los organismos seccionales, informarán oportunamente a la ciudadanía de las resoluciones que adoptaren, mediante la publicación de las actas de las respectivas sesiones de estos cuerpos colegiados, así como sus planes de desarrollo local; y,*
- t) *El Tribunal de lo Contencioso Administrativo, adicionalmente, publicará el texto íntegro de sus sentencias ejecutoriadas, producidas en todas sus jurisdicciones. La información deberá ser publicada, organizándola por temas, items, orden secuencial o cronológico, etc., sin agrupar o generalizar, de tal manera que el ciudadano pueda ser informado correctamente y sin confusiones”.*

Por su parte, el artículo 5 de la Ley Orgánica del Sistema Nacional de Datos Públicos, establece: *“Publicidad.- El Estado, de conformidad con la Ley, pondrá en conocimiento de las ciudadanas o ciudadanos, la existencia de registros o bases de datos de personas y bienes y en lo aplicable, la celebración de actos sobre los mismos, con la finalidad de que las interesadas o interesados y terceros conozcan de dicha existencia y los impugnen en caso de afectar a sus derechos”.*

Con lo que se concluye y se sustenta que esta categoría de información puede ser nombrada como “Información Publicada”.

III. De la información Reservada:

El numeral 19 del artículo 66 de la Constitución de la República del Ecuador, establece: *“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”.*

El artículo 91 de la Constitución de la República del Ecuador, dispone: *“La acción de acceso a la información pública tendrá por objeto garantizar el acceso a ella cuando ha sido denegada expresa o tácitamente, o cuando la que se ha proporcionado no sea completa o fidedigna. Podrá ser interpuesta incluso si la negativa se sustenta en el carácter secreto, reservado, confidencial o cualquiera otra clasificación de la información. El carácter reservado de la información deberá ser declarado con anterioridad a la petición, por autoridad competente y de acuerdo con la ley”* (el énfasis es propio).

El artículo 17 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, prescribe: *“De la Información Reservada.- No procede el derecho a acceder a la información pública, exclusivamente en los siguientes casos: a) Los documentos calificados de manera motivada como reservados por el Consejo de Seguridad Nacional, por razones de defensa nacional, de conformidad con el artículo 81, inciso tercero, de la Constitución Política de la República y que son: 1) Los planes y órdenes de defensa nacional, militar, movilización, de operaciones especiales y de base s e instalaciones militares ante posibles amenazas contra el Estado; 2) Información en el ámbito de la inteligencia, específicamente los planes, operaciones e informes de inteligencia y contra inteligencia militar, siempre que existiera conmoción nacional; 3) La información sobre la ubicación del material bélico cuando ésta no entrañe peligro para la población; y, 4) Los fondos de uso reservado exclusivamente destinados para fines de la defensa nacional; y, b) Las informaciones expresamente establecidas como reservadas en leyes vigentes”* (el énfasis es propio).

En este sentido, el Art. 18 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, determina: *“Protección de la Información Reservada.- La información clasificada previamente como reservada, permanecerá con tal carácter hasta un período de quince años desde su clasificación. La información reservada será desclasificada cuando se extingan las causas que dieron lugar a su clasificación. Se ampliará el período de reserva sobre cierta documentación siempre y cuando permanezcan y se justifiquen las causas que dieron origen a su clasificación”*.

Que el Código Orgánico Integral Penal en el artículo 180, dispone: *“Difusión de información de circulación restringida, [...] Es información de circulación restringida: 1. La información que está protegida expresamente con una cláusula de reserva previamente prevista en la ley. 2. La información producida por la Fiscalía en el marco de una investigación previa. 3. La información acerca de las niñas, niños y adolescentes que viole sus derechos según lo previsto en el Código Orgánico de la Niñez y Adolescencia.*

Con lo que se concluye y se sustenta que la categoría de información reservada requiere de un basamento de índole legal y clasificada por entidad competente, y puede ser nombrada como “Información Reservada”.

IV. De la información Confidencial:

La Constitución de la República del Ecuador señala en el numeral 19 del artículo 66 que *“Se reconoce y garantizará a las personas 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 6 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, dispone: *“Información Confidencial.- Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República. El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes. No podrá invocarse reserva, cuando se trate de investigaciones que realicen las autoridades, públicas competentes, sobre violaciones a derechos de las personas que se encuentren establecidos en la Constitución Política de la República, en las declaraciones, pactos, convenios, instrumentos internacionales y el ordenamiento jurídico interno. Se excepciona el procedimiento establecido en las indagaciones previas”*.

El tercer párrafo del artículo 10 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, dispone: *“Custodia de la Información (...) El tiempo de conservación de los documentos públicos, lo determinará la Ley del Sistema de Archivo Nacional y las disposiciones que regulen la conservación de la información pública confidencial”* (el énfasis es propio).

El artículo 21 de la Ley de Estadística, dispone: *“Los datos individuales que se obtengan para efecto de estadística y censos son de carácter reservado; en consecuencia, no podrán darse a*

conocer informaciones individuales de ninguna especie, ni podrán ser utilizados para otros fines como de tributación o conscripción, investigaciones judiciales y, en general, para cualquier objeto distinto del propiamente estadístico o censal". Esta norma legal data desde el año 1976 con el término "reservado" que se contrapone al mismo término utilizado en la Ley Orgánica de Transparencia y Acceso a la Información Pública emitida por el año 2004, por lo que se aplicará la norma jerárquica superior, por lo que, el término reservado en la Ley de Estadística hace referencia a la "información confidencial" en la LOTAIP (el énfasis es propio).

El artículo 6 de la Ley del Sistema Nacional de Registro de Datos Públicos, establece: "Accesibilidad y confidencialidad.- Son **confidenciales los datos de carácter personal**, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales. El acceso a estos datos sólo será posible con autorización expresa del titular de la información, por mandato de la ley o por orden judicial. También son confidenciales los datos cuya reserva haya sido declarada por la autoridad competente, los que estén amparados bajo sigilo bancario o bursátil, y los que pudieren afectar la seguridad interna o externa del Estado. La autoridad o funcionario que por la naturaleza de sus funciones custodie datos de carácter personal, deberá adoptar las medidas de seguridad necesarias para proteger y garantizar la reserva de la información que reposa en sus archivos".

Con lo que se concluye y se sustenta que esta categoría de información puede ser nombrada como "Información Confidencial".

V. De otro tipo de información:

El artículo 3 del Acuerdo Ministerial No. 025-2019, publicado en la Edición Especial del Registro Oficial No. 228 de 10 de enero de 2020, señala: "Recomendar a las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, utilicen como guía las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la información".

Conforme la serie NTE INEN-ISO/IEC 27002, el numeral 7.2.1 Directrices de clasificación señala como "control" que "La información se debería clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización".

[...] Las clasificaciones y los controles de protección asociados para la información deberían considerar las necesidades del negocio respecto a compartir o restringir la información, al igual que los impactos del negocio asociados con tales necesidades.

[...] Es conveniente considerar la cantidad de categorías de clasificación y los beneficios a obtener con su utilización. Los esquemas demasiado complejos pueden volverse engorrosos y de uso costoso o no ser prácticos. Se debería tener cuidado al interpretar las etiquetas de clasificación en los documentos de otras organizaciones, las cuales pueden tener diferentes definiciones para etiquetas iguales o similares.

[...] El nivel de protección se puede evaluar analizando la confidencialidad, la integridad y la disponibilidad como también otros requisitos para la información en consideración.

Con frecuencia, la información deja de ser sensible o importante después de un periodo de tiempo dado, por ejemplo, cuando la información se hace pública. Se deberían considerar estos aspectos puesto que la super clasificación puede originar la implementación de controles innecesarios que llevan a un costo adicional".

Conforme lo señala el libro DAMA DMBOK (Guía de Fundamentos para la Gestión de Datos – primera edición – Edición impresa 2010), en el numeral 7.2.8 Confidencialidad de información clasificada [...] “Un esquema de clasificación típico puede incluir los siguientes niveles de clasificación de cinco confidencialidades: Para Audiencias Generales: Información disponible para cualquier persona, incluido el público en general. El público general es la clasificación por defecto asumido. Sólo para uso interno: Información limitado a empleados o miembros, pero con un riesgo mínimo si se comparten. Sólo para uso interno se puede mostrar o discutida, pero no copian fuera de la organización. Confidencial: La información que no debe ser compartida fuera de la organización. La información confidencial del cliente no puede ser compartida con otros clientes. Confidencial Restringido: Información limitada a individuos que realizan ciertas funciones con la “necesidad de conocer”. La confidencial restringida podría exigir a individuales a calificar mediante la liquidación. Registrado Confidencial: La información de manera confidencial que cualquiera que acceda a la información debe firmar un acuerdo legal para acceder a los datos y asumir la responsabilidad de su carácter secreto.

Clasificar los documentos e informes basados en el más alto nivel de confidencialidad de cualquier información que se encuentra en el documento. Etiqueta de cada página o pantalla con la clasificación en el encabezado o pie de página. Los productos de información clasificada “para todos los públicos” no necesitan etiquetas. Asumir cualquier producto sin etiqueta de ser para todos los públicos. Los autores del documento y diseñadores de productos de información son responsables de evaluar, clasificar correctamente y etiquetar el nivel apropiado de confidencialidad para cada documento.

Además, clasifique las bases de datos, tablas relacionales, columnas y puntos de vista. Clasificación de la información confidencial es una importante característica de metadatos, guiando cómo se otorgan los usuarios privilegios de acceso. Los administradores de datos son responsables de evaluar y determinar el nivel apropiado de confidencialidad para los datos.”

Tomando en consideración que la información que se procesa al interior del INEC representa por ejemplo: contraseñas, actas de reuniones, firmas, planes estratégicos, indicadores, configuraciones de seguridad, publicaciones internas, código fuente, estructura de base de datos, cuentas de empleados en bancos, entre otros, pueden corresponder a Información confidencial y en algunos casos a información que solamente puede divulgarse al interior del INEC; por lo que en concordancia a la ISO/IEC 27002 y al DAMA DMBOK, **se concluye y se sustenta que la categoría de “Información Confidencial” puede contener información distinta a la personal y que se incentiva la categoría a ser nombrada como “Información Interna”**.

VI. Conclusión del Análisis:

Con lo descrito, se concluye que la información en el INEC debe ser clasificada, por jerarquía de mayor a menor en:

- **Información Reservada:**
Información estipulada como tal en la normativa legal y por autoridad competente.
Confidencialidad: Extrema
Integridad: Extrema
Disponibilidad: Alta
Riesgo: Extremo

Nota: Información no disponible en el INEC.

- **Información Confidencial:**

Información estipulada como tal en la normativa legal y otro tipo de información que solamente ciertos servidores del INEC, están autorizados a acceder como parte de su gestión. La divulgación de este tipo de información, a quienes no son sus titulares, requerirá la autorización expresa de la Dirección Ejecutiva o Subdirección General.

Confidencialidad: Alta

Integridad: Alta

Disponibilidad: Alta

Riesgo: Alto

- **Información Interna:**

Información que es de interés de todo el personal del INEC y que aún no ha sido publicada. La divulgación a terceros de este tipo de información requerirá la autorización de la Coordinación o Dirección que originó tal información.

Confidencialidad: Media

Integridad: Alta

Disponibilidad: Media

Riesgo: Medio

- **Información Publicada:**

Información que se encuentra disponible en los medios públicos, incluso en el portal institucional.

Confidencialidad: Baja

Integridad: Alta

Disponibilidad: Baja

Riesgo: Bajo

Cabe indicar que cualquier dato o metadato que forme parte de la información será tratado con el nivel de protección que amerita cada categoría.