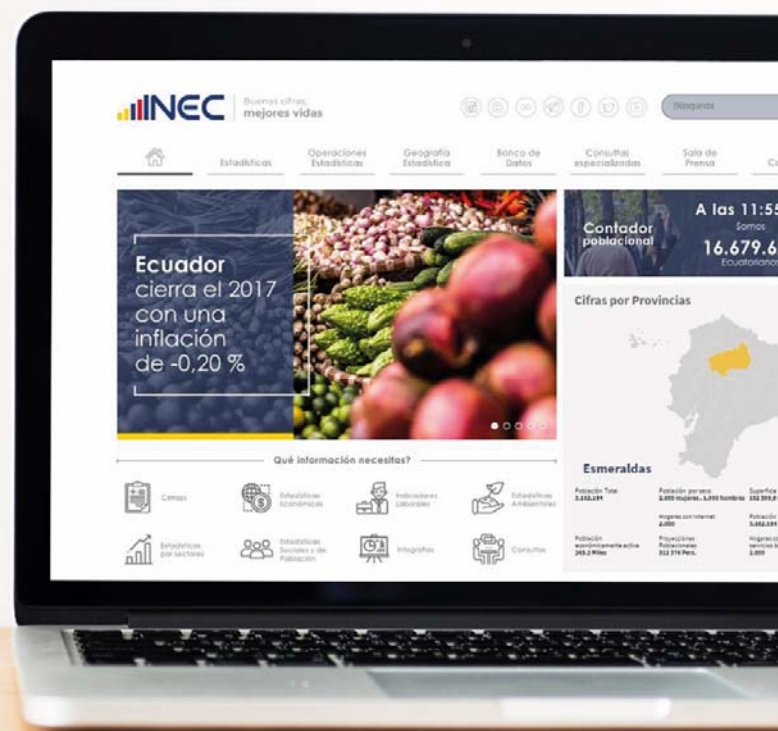


POLÍTICA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

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	
Mat. Víctor Bucheli	Subdirector General	
Mgs. David Muñoz	Coordinador General Técnico de Planificación Normativas de Calidad Estadística, Encargado y Presidente Comité de Seguridad de la Información	

Nombre	Cargo	Firma
Mgs. Jenny Delgado Enríquez	Oficial de Seguridad de la Información	
Abg. María Eugenia Morales	Directora de Asesoría Jurídica	
Mgs. Diana Soriano	Directora de Comunicación Social	
Sra. Yolanda Rosero	Directora de Planificación y Gestión Estratégica Subrogante	
Ing. Paulina Suárez	Directora de Tecnologías de la Información y Comunicación	
Sra. Diana Molina	Coordinadora General Administrativa Financiera	
Sra. María Fernanda Cifuentes	Directora Administrativa	
Sra. Silvana Guambuete	Directora Financiera, Encargada	
Abg. María José Arrobo	Directora de Administración de Recursos Humanos	
Srta. Mónica Alexandra Torres	Directora de Planificación Estadística del SEN, Subrogante	
Srta. Ivonne Benítez	Directora de Normativas Estandarización y Calidad Estadística Encargada	
Sr. David Sánchez	Coordinador General Técnico de Producción Estadística	
Ing. David Caín	Director de Registros Administrativos, Encargado	

Nombre	Cargo	Firma
Ing. Christian Garcés	Director de Infraestructura Estadística y Muestreo	
Srta. Viviana Ruiz	Directora de Cartografía Estadística y Operaciones de Campo	
Sra. María Soledad Carrera	Directora de Estadísticas Socio-Demográficas Encargada	
Econ. Darío Vélez	Director de Estadísticas Económicas	
Econ. David Salazar	Director de Estadísticas Agropecuarias y Ambientales	
Sra. María Isabel García	Coordinadora General Técnica de Innovación en Métricas y Análisis de la Información Encargada	
Sra. Natalia Garzón	Directora de Estudios y Análisis de la Información Subrogante	
Ing. Fernando Goyes	Coordinador Zonal 3 - Centro, Encargado	
Mgs. Joffre León	Coordinador Zonal 8 INEC (E)	
Lcdo. José Ayala	Coordinador Zonal 6 - Sur (Enc)	

CADA HECHO DE TU VIDA *Cuenta*



@ecuadorencifras



@InecEcuador



t.me/ecuadorencifras



INEC/Ecuador



INECEcuador



INEC Ecuador

