RESOLUCIÓN Nro. CNIG-ST-2020-0025

Nelly Piedad Jácome Villalva
SECRETARIA TÉCNICA
CONSEJO NACIONAL PARA LA IGUALDAD DE GÉNERO

CONSIDERANDO:

Que la Constitución de la República del Ecuador en el artículo 18, números 1 y 2, prescribe: *"Todas las personas, en forma individual o colectiva, tienen derecho a: 1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior. 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 artículo 82 de la Constitución de la República del Ecuador, establece: *"El derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, clara, públicas y aplicadas por la autoridades competentes"*;

Que el artículo 156 de la Constitución dispone: *"Los Consejos Nacionales para la Igualdad son órganos responsables de asegurar la plena vigencia y el ejercicio de los derechos consagrados en la Constitución y en los instrumentos internacionales de derechos humanos. Los consejos ejercerán atribuciones en la formulación, transversalización, observancia, seguimiento y evaluación de las políticas públicas relacionadas con las temáticas de género, étnicas, generacionales, interculturales, de discapacidades y movilidad humana, de acuerdo con la ley. Para el cumplimiento de sus fines se coordinarán con las entidades rectoras y ejecutoras y con los organismos especializados en la protección de derechos en todos los niveles de gobierno";*

Que el artículo 226 de la Constitución de la República del Ecuador, señala que: *"Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos 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, establece que: *"La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, partícipación, planificación y transparencia y evaluación"*;

Que la Ley Orgánica de los Consejos Nacionales para la Igualdad, en el artículo 4 establece, que: *"(…) son organismos de derecho público, con personería jurídica; forman parte de la Función Ejecutiva, con competencias a nivel nacional y con autonomía administrativa, técnica, operativa y financiera; y no requerirán estructuras desconcentradas ni entidades adscritas para el ejercicio de sus atribuciones y funciones";*

Que el artículo 10 de la Ley Orgánica de los Consejos Nacionales para la Igualdad, señala que: *"La gestión de los Consejos Nacionales para la Igualdad previstos en la presente Ley, se ejerce a través de la respectiva Secretaría Técnica"*;

Que el artículo 12 de la Ley Orgánica de los Consejos Nacionales para la Igualdad establece que: *"Las o los Secretarios Técnicos tendrán entre otras atribuciones y funciones las siguientes: (…) 5. Dirigir la gestión administrativa, financiera y técnica de los Consejos Nacionales para la Igualdad (…)";*

Que el artículo 1 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, señala: *"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 la Ley Orgánica de Transparencia y Acceso a la Información Pública, en el artículo 5 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"*;

Que en la Edición Especial Nro. 228, de 10 de enero de 2020, fue publicado en el Registro Oficial el Acuerdo Ministerial Nro. 025-2019 que contiene en su Anexo el Esquema Gubernamental de Seguridad de la Información (EGSI versión 2.0), el cual es de implementación obligatoria en las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva (APCID);

Que según Decreto Ejecutivo Nro. 434, de 14 de junio de 2018 el Lcdo. Lenin Moreno Garcés Presidente Constitucional de la República, expide la reforma al Decreto 319, de 20 de febrero del 2018, en los siguientes términos: *"Artículo 1.- Sustituir el artículo 1 por el siguiente: "Designar a las y los siguientes funcionarias y funcionarios en su calidad de titulares de las Carteras de Estado en representación de la Función Ejecutiva ante los Consejos Nacionales para la Igualdad: (...) 4. De Género: Ministra/o de Justicia, Derechos Humanos y Cultos."*;

Que mediante Decreto Ejecutivo Nro. 560, de 14 de noviembre del 2018, el Lcdo. Lenin Moreno Garcés Presidente Constitucional de la República dispone: *"Artículo 1. Transfórmese el Ministerio de Justicia, Derechos Humanos y Cultos en la Secretaría de Derechos Humanos, como entidad de derecho público, con personalidad jurídica, dotada de autonomía administrativa y financiera. Artículo 2. La Secretaría de Derechos Humanos, tendrá a su cargo las siguientes atribuciones (…) En consecuencia, todas las atribuciones constantes en leyes y demás normativa vigente relacionada con estas competencias serán asumidas por la Secretaría de Derechos Humanos"*;

Que mediante Decreto Ejecutivo Nro. 818, de 03 de julio de 2019, el Licenciado Lenin Moreno Garcés, Presidente Constitucional de la República, en el artículo 4 designa a la Mgs. Cecilia del Consuelo Chacón Castillo como Secretaria de Derechos Humanos;

Que mediante Resolución Nro. CNIG-CNIG-2020-0001, de 02 de enero de 2020, la Mgs. Cecilia del Consuelo Chacón Castillo, en su calidad de Presidenta del Pleno del Consejo Nacional para la Igualdad de Género, resolvió: *"(…) Artículo 2.- Designar a la Dra. Nelly Jácome Villalva, como Secretaria Técnica del Consejo Nacional para la Igualdad de Género, a partir del 02 de enero del 2020, por ser el primer día hábil del mes."*;

Que mediante Resolución Nro. CNIG-ST-2019-0001-RI, de 16 de agosto de 2019, publicada en el Registro Oficial Edición Especial Nro. 41, de 23 de agosto de 2019, se publicó el Estatuto Orgánico de Gestión Organizacional por Procesos del Consejo Nacional para la Igualdad de Género – CNIG; en donde se establecen las atribuciones y responsabilidades de la Secretaria/o Técnica/o, estableciendo en el literal f): *"(…) Dirigir la gestión administrativa, financiera y técnica del Consejo Nacional para la Igualdad de Género";*

Que mediante Acta Nro. 04, de 30 de septiembre 2020, el Comité de Seguridad de la Información, resolvió: *"1. Aprobar la Política institucional de Seguridad de la información del CNIG. 2. Aprobar el perfil del Proyecto para la implementación del EGSI en el CNIG; y, 3. Aprobar el Acta No. 4 correspondiente al 30 de septiembre de 2020"*;

Que mediante memorando Nro. CNIG-PGE-2020-0142-M, de 21 de octubre de 2020, la Ing. Rocío Balarezo Bustamante, Responsable de la Unidad de Planificación y Gestión Estratégica, en su calidad de Presidenta del Comité de Seguridad de la Información, comunica a la Dra. Nelly Jácome Villalva que: "… *la "Política de Seguridad de la Información del CNIG", que fue aprobada por el Comité de Seguridad de la Información, en sesión celebrada el 30 de septiembre de 2020; y, de conformidad a lo establecido en el Instructivo Interno para la Elaboración, Revisión, Aprobación y Difusión de las Resoluciones Administrativas, solicito a usted se sirva autorizar la normativa interna, para el efecto adjunto: Política de Seguridad de la Información del CNIG Acta N0. 4 del Comité de Seguridad de la Información, del 30 de septiembre de 2020";*

Que mediante nota inserta en el memorando CNIG-PGE-2020-0142-M, de 21 de octubre de 2020, la Secretaria Técnica del Consejo Nacional para la Igualdad de Género, dispuso: "*UPGE: autorizado*";

Que mediante memorando Nro. CNIG-PGE-2020-0148-M, de 27 de octubre de 2020, la Ing. Rocio Balarezo Bustamante Responsable de la Unidad de Planificación y Gestión Estratégica, comunica a la Dra. Lorena Caizaluisa que: "*Por medio del presente, me permito informar a usted que la máxima autoridad autorizó la normativa: "Política de Seguridad de la Información del CNIG", según sumilla inserta en Memorando Nro. CNIG-PGE-2020-0142-M, la citada Política fue aprobada previamente por el Comité de Seguridad de la Información, en sesión celebrada el 30 de septiembre de 2020; en este contexto solicito a usted se sirva gestionar la aprobación de nueva normativa interna, para el efecto adjunto: Formulario para solicitud de elaboración de nueva normativa Acta N0. 4 del Comité de Seguridad de la Información, del 30 de septiembre de 2020. El proyecto borrador de norma interna Memorando Nro. CNIG-PGE-2020-0142-M, aprobado por la máxima autoridad.";*

Que es necesario se emitan las Políticas de Seguridad de la Información en consideración del tipo de documentación que manejan los y las servidoras del Consejo Nacional para la Igualdad de Género;

En ejercicio de las atribuciones constitucionales, legales y reglamentarias:

RESUELVE:

EXPEDIR LA POLITICA DE SEGURIDAD DE LA INFORMACION CONSEJO NACIONAL PARA LA IGUALDAD DE GÉNERO

Capítulo I
GENERALIDADES

Artículo 1. Objeto.- Proporcionar las directrices para la Gestión de Seguridad de la Información para proteger y salvaguardar la información generada por las unidades técnicas, administrativas, operativas y de asesoría del Consejo Nacional para la Igualdad de Género y los recursos tecnológicos utilizados para su creación, procesamiento y administración, frente a amenazas internas o externas, intencionales o no, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Artículo 2. Ámbito de aplicación.- El presente instrumento, regirá para todos los/las servidores/as, funcionarios/as, trabajadores/as, practicantes o cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género, inclusive para proveedores externos vinculados a la Institución a través de contratos, convenios o acuerdos; y, con apego a la definición de roles y perfiles relacionados con el Esquema Gubernamental de Seguridad de la información (EGSI).

Artículo 3. Conceptos y Definiciones.- Para efectos del cumplimiento de la Política de Seguridad de la Información, se entenderá por:

a) **ACTIVO DE INFORMACIÓN:** Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de la Institución y, en consecuencia, debe ser protegido;
b) **ACUERDO DE CONFIDENCIALIDAD:** Es un documento en el que, los/las servidores/as, funcionarios/as, trabajadores/as, practicantes, cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género que en el marco del servicio o actividad realizada hayan tenido acceso a la información institucional, manifiestan su voluntad de mantener la confidencialidad de la información de la institución, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan;
c) **ADMINISTRACIÓN DE RIESGOS:** Comprende el proceso de control y minimización, o la completa eliminación, de los riesgos de seguridad que podrían afectar a la información de la Institución;

d) **ANÁLISIS DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN:** Es un proceso Sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información;
e) **BYOD - Brirsg Your Own Device:** Son herramientas basadas en tecnologías de gestión de movilidad que permiten la protección de estos dispositivos, incorporan mecanismos de autenticación accediendo a las aplicaciones y datos en cualquier dispositivo;
f) **CUSTODIO DEL ACTIVO DE LA INFORMACIÓN:** Es la unidad organizacional o proceso, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados;
g) **DISPOSITIVO MÓVIL:** se puede definir como un aparato de pequeño tamaño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, que ha sido diseñado específicamente para una función, pero que puede llevar a cabo otras funciones más generales;
h) **DOMINIO:** Es el conjunto de computadoras conectadas en una red informática que confían a uno de los equipos de dicha red, la administración de los usuarios y los privilegios que cada uno de los usuarios/as tiene en dicha red;
i) **ESCRITORIO LIMPIO:** Es la protección de los papeles y dispositivos removibles de información, almacenados y manipulados en estaciones de trabajo (escritorio, oficina, etc.), de accesos no autorizados, pérdida y/o daño de la información durante y fuera de las horas normales de trabajo;
j) **EVALUACIÓN DE RIESGOS:** Comprende las acciones realizadas para identificar y analizar las amenazas y/o vulnerabilidades relativas a la información y a los medios de procesamiento de la misma, así como la probabilidad de ocurrencia y el potencial impacto a las operaciones de la Institución;
k) **INCIDENTE DE SEGURIDAD INFORMÁTICA**: Es un intento de acceso, uso, divulgación, modificación o destrucción no autorizados de Información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o, cualquier otro acto que implique una violación a la Política de Seguridad de la Información del Consejo Nacional para la Igualdad de Género;
l) **INCIDENTE DE SEGURIDAD:** Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo);
m) **INFORMACIÓN:** Se refiere a toda representación de conocimiento en forma de datos vinculados entre sí. Pudiendo ser texto, numérica, gráfica, cArtículoográfica, narrativa o audiovisual, almacenada en cualquier medio, ya sea magnético, en papel, en medios electrónicos computadoras, audiovisual u otras;
n) **INFORMACIÓN SENSIBLE:** Es aquella a la cual la ley tiene prohibido divulgar, ya que perjudica la seguridad nacional, o la intimidad personal; por ejemplo, ciertos datos personales y bancarios, contraseñas de correos electrónicos. Estos son datos personales que solo pueden ser revelados con autorización del titular;
o) **INSTITUCIÓN:** Se refiere al Consejo Nacional para la Igualdad de Género CNIG;

p) **MEDIOS MAGNÉTICOS:** Son dispositivos que utiliza materiales magnéticos para archivar información digital, tales como los discos duros o los CD que almacenan grandes volúmenes de datos en un espacio físico pequeño;
q) **MEDIOS ÓPTICOS:** Los discos ópticos son un producto de almacenamiento de datos que guarda el contenido en formato digital; estos discos se pueden escribir y leer mediante un láser que generalmente se encuentra en su computadora;
r) **PANTALLA LIMPIA:** Es la protección de las computadoras, dispositivos móviles, u otros dispositivos, mediante un bloqueo de pantalla o desconexión cuando no están en uso;
s) **PERFIL:** Es un entorno personalizado específicamente para un usuario/a o grupo de usuarios/as. Contiene configuración de los programas de acuerdo a las características por área de trabajo y responsabilidad;
t) **PLATAFORMA:** Es un sistema que sirve como base para hacer funcionar determinados módulos de hardware o de software con los que es compatible. Dicho sistema está definido por un estándar alrededor del cual se determina una arquitectura de hardware y una plataforma de software (incluyendo entornos de aplicaciones);
u) **PROPIETARIO/A DE LA INFORMACIÓN:** Es la persona responsable de la integridad, confidencialidad v disponibilidad de una cierta información; y las unidades que producen o generan la información, quienes clasifican la información de acuerdo con el grado de sensibilidad y criticidad de la misma;
v) **RESGUARDO:** Es proteger la información del computador, hacer una copia de seguridad o copia de respaldo de datos de tal forma que estas copias adicionales puedan restaurar un sistema después de una perdida de información;
w) **RIESGO:** Se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Los factores que lo componen son la amenaza y la vulnerabilidad;
x) **SEGMENTACIÓN:** Es dividir la red en varias subredes para mantener una mejor administración de recursos y proporcionar seguridad de forma dinámica;
y) **SEGURIDAD DE LA INFORMACIÓN - SI**: Es la preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad (accountability), no repudio y fiabilidad, para lo cual se debe considerar que las características mencionadas a continuación se cumplan:

1. Autenticidad: Asegura la validez de la información en tiempo, forma y distribución. Así mismo, garantiza el origen de la información al validar el emisor de ésta, para evitar suplantación de identidades;
2. Auditabilidad: Asegura que todos los eventos de un sistema deben quedar registrados, permitiendo su control posterior, ya sea en forma automática o manual;
3. Confiabilidad: La información debe ser adecuada para sustentar la toma de decisiones y la ejecución de las actividades propias de la Institución;
4. Confidencialidad: La información es accesible únicamente a quien esté autorizado;

5. Disponibilidad: Los usuarios autorizados tienen acceso a la información y a los recursos relacionados, toda vez que lo requieran;
6. Integridad: La información debe permanecer correcta (Integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros. Salvaguarda la exactitud y la totalidad de la información y los métodos para su creación, recuperación y procesamiento;
7. Legalidad: Garantizar el cumplimiento de las leyes, acuerdos, reglamentos, disposiciones o cualquier otra norma que integre el ordenamiento jurídico;
8. No repudio: Invitar que una entidad que haya interactuado con alguna información alegue ante terceras que no lo ha hecho; y,
9. Protección a la duplicación: Asegura que una transacción sea realizada por única vez, a menos que se especifique lo contrario.

z) **SISTEMA DE INFORMACIÓN:** Se refiere a un conjunto de recursos organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información, que cumplen con determinadas características propias de la Institución, así como con procedimientos que pueden ser automatizados o manuales.

aa) **SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN:** Es un conjunto de políticas de administración de la información, que requiere del diseño, implementación y mantenimiento de un conjunto de procesos y procedimientos que permitan la gestión eficiente de la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de ésta, minimizando los riesgos. Un Sistema de Gestión de Seguridad de la información debe ser eficiente a través del tiempo, adaptándose a los cambios de la Institución, así como a los de su entorno;

bb) **SOFTWARE:** Son los programas informáticos que hacen posible la realización de tareas específicas dentro de un computador;

cc) **TECNOLOGÍAS DE LA INFORMACIÓN:** Se refiere a equipos de cómputo, aplicativos con desarrollo propio o adquiridos, medios de almacenamiento y comunicaciones, que en conjunto son operados por la Institución o por un tercero, con el objetivo de procesar, almacenar y/o transmitir información para llevar a cabo una función propia de la Institución;

dd) **TERCEROS:** Todas las personas, jurídicas o naturales, como proveedores, contratistas que provean servicios o productos a la Institución;

ee) **USUARIO/A:** Es cualquier persona que acceda a los servicios de la Institución, o que utiliza un sistema informático, y ello implica su adhesión plena e incondicional a estas Políticas, por lo tanto, es responsabilidad del/a Usuario/a leerlas previamente, de tal manera que esté consciente de que se sujeta a ellas y a las modificaciones que pudieran sufrir; y,

ff) **VULNERABILIDADES:** Son las debilidades, vacíos de seguridad inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la Institución (amenazas), las cuales se constituyen en fuentes de riesgo.

CAPITULO II
LINEAMIENTOS GENERALES

Artículo 4. Lineamientos Generales de las Políticas.- La Seguridad de la Información, es un factor clave para el correcto desarrollo institucional, en este sentido, la Institución ha establecido los lineamientos generales para la aplicación de las Políticas de Seguridad de la Información, que serán de cumplimiento obligatorio para los/las servidores/as, funcionarios/as, trabajadores/as, practicantes o cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género, proveedores externos vinculados a la Institución a través de contratos, convenios o acuerdos, y otras partes interesadas.

Así mismo, se considera que la Gestión de la Seguridad de la información, es uno de los pilares en los que se fundamenta las actividades de la Institución, por ello, se consideran los siguientes lineamientos:

a) Cumplir con todas las leyes, reglamentos, disposiciones y mandatos; así como las obligaciones contractuales;
b) Realizar actividades de formación y concienciación en materia de los procesos de Seguridad de la Información para todos los/las servidores/as, funcionarios/as, trabajadores/as, practicantes o cualquier persona que preste servicios en el Consejo Nacional para la Igualdad de Género;
c) Determinar que la información generada o almacenada en diferentes medios, es de propiedad del Consejo y debe ser utilizada exclusivamente para las tareas propias de la función desarrollada en la Institución;
d) Establecer que para el manejo de la información institucional debe tener relación laboral con la Institución, o contar con la autorización escrita, del/a funcionario/a del nivel jerárquico superior competente;
e) Monitorear cambios significativos de los riesgos que afecten a los recursos de información frente a las amenazas más importantes;
f) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información;
g) Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios;
h) Designar a los custodios y responsables de la información de cada una de las unidades administrativas donde se genera la misma;
i) Velar por la aplicación de la normativa relacionada a las normas técnicas ecuatorianas INEC ISO/IEC 27000 conforme al ámbito de cada Institución;
j) Establecer los objetivos de control correspondientes para mitigar los riesgos detectados; y,
k) Establecer la responsabilidad, y sanciones a los/las servidores/as, funcionarios/as, trabajadores/as, practicantes o cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género, en los casos que correspondan y que tengan relación con:

1. Reportar las violaciones a la seguridad;
2. Preservar la confidencialidad, integridad y disponibilidad de la información en cumplimiento de esta política; y,
3. Cumplir las políticas y procedimientos inherentes al Sistema de Gestión de la Seguridad de la Información.

Artículo 5. Políticas de Seguridad de la Información.- A efectos de salvaguardar la información que se genera en los medios tecnológicos institucionales, esta Institución, podrá crear otras políticas vinculadas al cumplimiento del EGSI acorde a las necesidades institucionales, las mismas que serán de estricto cumplimiento de los/las servidores/as, funcionarios/as, trabajadores/as, practicantes o cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género.

Capítulo III
GESTIONES INTERNAS DEL CONSEJO Y USUARIOS/AS EXTERNOS/AS

Artículo 6. Gestión de Organización de la Seguridad de Información.

a) **Máxima autoridad o su delegado.-** Dispone la difusión e implementación del Esquema Gubernamental de Seguridad de la Información, así como las Políticas de Seguridad de la información del Consejo;
b) **Designación del Comité de Seguridad de la Información.-** La Máxima Autoridad o su delegado será el/a encargado/a de designar a los/as integrantes del Comité de Seguridad de la Información;
c) **Oficial de Seguridad de la Información.-** El Comité de Seguridad de la información, designará de entre sus integrantes al Oficial de Seguridad de la Información, es el responsable de revisar el texto de la Política de Seguridad de la información, la estructuración, seguimiento y mejora del Sistema de Gestión de Seguridad de la Institución, para lo cual deberá cumplir al menos lo siguiente:

1. Definir las estrategias de capacitación en coordinación con la unidad de Administración de Talento Humano en materia de seguridad de la información y coordinar las acciones, impulsando la implementación y cumplimiento de la presente política;
2. Controlar la aplicación de la política de protección de datos y privacidad de la información personal e implementar medidas técnicas y organizacionales apropiadas para gestionar de manera responsable la información personal de acuerdo con la legislación vigente y a lo establecido en el Acuerdo Nro. 166 del Esquema Gubernamental de Seguridad de la Información - EGSI, de 19 de septiembre del 2013, referente a los roles y responsabilidades que se definen en el numeral 2.3;
3. Implementar de manera conjunta con los órganos administrativos del Consejo, mecanismos de carácter organizacional y tecnológico para autorización al acceso a la información, así como para el intercambio de datos personales o ciudadanos en custodia de la Institución. Primará el principio de que los datos personales

pertenecen a los ciudadanos y no a las instituciones en concordancia con la normativa legal vigente;

4. Implementar medidas y mecanismos de seguridad física, lógica y procedimentales para la protección de la información digital de la Institución; y,
5. Ejecutar en coordinación con el Responsable de Tecnologías de la Información, revisiones independientes de la gestión de seguridad en las áreas que manejan información confidencial de la Institución en intervalos planificados o cuando ocurran cambios, identifican las oportunidades de mejora y la necesidad de cambios con enfoque de seguridad, incluyendo la política y los objetivos de control.

   El/la Oficial de Seguridad de la información (OSI) es el responsable directo del mantenimiento de esta política;

d) Responsable de Tecnología de la Información.- El responsable de Tecnologías de la Información, se encarga de establecer, mantener y dar a conocer las políticas y procedimientos de los servicios de tecnología, incluida esta política de seguridad de la información y todos sus capítulos; el uso de los servicios tecnológicos en toda la Institución conjuntamente con la Unidad de Talento Humano, de acuerdo con las mejores prácticas y lineamientos institucionales y normativa vigente, para ello será el responsable de:

1. Mantener la custodia de la información que reposa en los diferentes sistemas, bases de datos y aplicativos de la Institución;
2. Informar de los eventos que están en contra de la seguridad de la información e infraestructura tecnológica de la Institución;
3. Controlar la existencia de documentación física y/o electrónica actualizada relacionada con los procedimientos de comunicaciones, operaciones y sistemas;
4. Procesar la obtención de copias de resguardo de información; así como la prueba periódica de su restauración;
5. Implementar y verificar los controles de seguridad definidos;
6. Gestionar los incidentes de seguridad de la información de acuerdo con los procedimientos;
7. Proporcionar las medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la Institución;
8. Garantizar las condiciones tecnológicas óptimas para la implementación de las políticas de seguridad de información institucional;
9. Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio del Consejo;
10. Resolver de común acuerdo con las áreas y los propietarios de la información los conflictos que se presenten por la propiedad de la información al interior de la Institución, esto incluye los posibles medios de acceso a la información, los datos derivados del procesamiento de la información a través de cualquier aplicación o sistema, los datos de entrada a las aplicaciones y los datos que son pArtículoe integral del apoyo de la solicitud;

11. Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo;
12. Implementar los mecanismos de control necesarios y pertinentes paro verificar el cumplimiento de la presente política;
13. Definir procedimientos para el control de cambios a los procesos operativos, los sistemas e instalaciones y verificar su cumplimiento, de manera que no afecte la seguridad de la información;
14. Establecer criterios de seguridad para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas antes de su aprobación definitiva;
15. Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento;

16. Controlar los mecanismos de distribución y difusión de información dentro y fuera de la Institución;
17. Definir y documentar controles para la detección y prevención de accesos no autorizados, protección contra software malicioso, garantiza la seguridad de los datos y servicios conectados a las redes de la Institución; y,
18. Desarrollar procedimientos adecuados de concienciación de usuarios en materia de seguridad, controles de acceso a los sistemas;

e) Responsabilidades de los Propietarios de la Información.- Los/las servidores/as, funcionarios/as, trabajadores/as, practicantes o cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género, que manejan, generan, procesan, reciben y almacenan en cualquier medio la información institucional, son responsables de:

1. Velar, valorar y clasificar la información que está bajo su administración y /o generación, siguiendo los lineamientos establecidos por la Constitución de la República del Ecuador, Ley Orgánica de Transparencia y Acceso a la Información Pública, el Esquema de Seguridad de la información y la Dirección Administrativa Financiera referente a la Gestión Documental y Archivo;
2. Autorizar, restringir y delimitar a los demás usuarios de la Institución el acceso a la información de acuerdo a sus roles y responsabilidades y a los diferentes servidores/as, funcionarios/as, trabajadores/as, practicantes o cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género que por sus actividades requieran consultar, crear o modificar pArtículoe o la totalidad de la información, así como la solicitud y aceptación de acuerdos de confidencialidad;
3. Determinar los tiempos de retención de la información conjuntamente entre la Unidad de Gestión Documental y Archivo y las áreas que se encarguen de su protección y almacenamiento, de acuerdo con las normas vigentes y las políticas de la Institución, así como de los entes externos y las normas o leyes vigentes; y,
4. Determinar y evaluar de forma periódica los riesgos asociados a la información, así como los controles implementados para el acceso y gestión de la

administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de la misma;

f) Responsable de Administración de Talento Humano.- El/a Responsable de la Unidad de Administración de Talento Humano cumplirá la función de notificar a todo el personal que se vincula a la Institución acerca de las obligaciones respecto del cumplimiento de las Políticas de Seguridad de la información, de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de Seguridad de la Información y demás normativa interna, procedimientos y prácticas que se generan, para ello será el responsable de:

1. Difundir al personal, los cambios en las políticas de seguridad de la información que se presenten y de la suscripción del Acuerdo de Confidencialidad al personal que se vincula a la Institución y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el/a Oficial de Seguridad de la información; y,.

g) Responsable de Gestión Documental y Archivo.- Es responsable de clasificar la información de acuerdo con el grado de sensibilidad y criticidad; de documentar, mantener actualizada, custodiada, y preservar la misma, aplicando las medidas de seguridad que establecen los instructivos institucionales y la Norma Técnica de Gestión Documental y Archivo; otorgar los permisos de acceso a la información de acuerdo con sus funciones y competencias.

Artículo 7. Responsabilidades de los/las servidores/as, funcionarios/as, trabajadores/as, practicantes, cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género y Usuarios de la Información.-En el manejo y uso de la información, los/las servidores/as, funcionarios/as, trabajadores/as, practicantes o cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género y/o terceras personas que generan o acceden a la información de la Institución, tienen las siguientes responsabilidades:

a) Manejar la información de la Institución y rendir cuentas por el uso y protección de la misma, mientras esté bajo su conocimiento y custodia, la que puede ser física o electrónica o almacenada en cualquier medio;
b) Proteger la información a la cual accedan o procesen, para evitar su pérdida, alteración destrucción o uso indebido;
c) No divulgar la información cuyo uso no esté autorizado, por las autoridades competentes;
d) Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma;
e) Informar a sus superiores, en el caso de terceros a cualquier persona que tenga relación con la institución, sobre la violación de estas políticas;
f) Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición, de la destrucción o alteración y de la divulgación no autorizada;

g) Reportar a la autoridad competente, los incidentes de seguridad, eventos sospechosos y mal uso de los recursos que identifique;
h) Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos designados para el cumplimiento de sus funciones. No está permitida la conexión de equipos de cómputo y de comunicaciones ajenas a la Institución, a la red Institucional ni el uso de dispositivos de acceso externo a internet o de difusión de señales de red que no hayan sido previamente autorizadas por Tecnologías de Información y Comunicación;
i) Utilizar el software autorizado adquirido legalmente por la Institución. No está permitido la instalación ni uso de software diferente al institucional sin el consentimiento de sus superiores y visto bueno de Tecnologías de Información y Comunicación;
j) Aceptar y reconocer que en cualquier momento y sin previo aviso, Tecnologías de Información y Comunicación puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web y redes sociales propiedad del Consejo, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la Institución. Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por petición de la Máxima Autoridad, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales;
k) Proteger y resguardar su información personal que no esté relacionada con sus funciones en la Institución.;
l) La Institución no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito al utilizar la infraestructura tecnológica facilitada por la Institución; y,
m) Si un usuario debiera cambiar de equipo, ya sea por reemplazo del mismo o por traslado a otra unidad, el usuario deberá solicitar apoyo tecnológico a Tecnologías de la información.

Artículo 8. Gestión de los Activos Fijos.- A través de las unidades de la Dirección Administrativa Financiera, son responsables de la gestión y manejo de activos que tienen valor para la Institución, en colaboración con otras unidades y serán responsables de:

a) Inventariar activos primarios en formatos físicos y/o electrónicos conforme lo establece el Esquema de Seguridad de la Información y el Reglamento General Sustitutivo para la Administración, Utilización, Manejo y Control de los Bienes e Inventarios del Sector Público;
b) Inventariar los activos de Hardware, conforme lo establece el Esquema Gubernamental de la Información, donde consten equipos móviles, fijos, periféricos de salida, periféricos de entrada, dispositivos, sistemas ente otros vinculados a las acciones que ejecuta la Institución y que permitan dar continuidad al negocio; y,
c) Inventariar los activos de Software, Redes y demás aplicativos informáticos de la Institución.

Los/las servidores/as, funcionarios/as, trabajadores/as, practicantes o cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género, son responsables del manejo y uso de los activos de la Institución que utiliza para sus actividades diarias.

El uso aceptable de los activos de la Institución se enmarca en la utilización adecuada de los mismos y el cumplimiento de las normativas y políticas establecidas por la Institución.

Artículo 9. Gestión de Seguridad de Talento Humano- Mediante sus unidades responsables ejecutan las siguientes acciones vinculadas al cumplimiento del Esquema Gubernamental de la información EGSI.

La gestión de Administración de Talento Humano, verifica la información entregada por los/as candidatos/as previo a su contratación y entrega de manera formal las funciones y responsabilidades de los/las servidores/as, funcionarios/as, trabajadores/as, practicantes o cualquier persona, que haya sido contratada. Los/las servidores/as, funcionarios/as, trabajadores/as, practicantes o cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género, deberán firmar un acuerdo de confidencialidad y de no divulgación, para acceder a la información confidencial.

La gestión de Administración de Talento Humano deberá brindar una inducción a los nuevos/as funcionarios/as y servidores/as que se integran a la Institución, donde expliquen las funciones, responsabilidades respecto a la seguridad de la información, acceso a la información, uso de contraseñas con sistemas de información confidencial.

Los órganos administrativos del CNIG, se encargan de explicar y definir las funciones y responsabilidades respecto a la seguridad de la información. Previa la terminación de un contrato laboral se debe realizar la transferencia de la documentación e información de la que fue responsable el/la servidor/a, funcionario/a, trabajador/a, practicante o cualquier persona que tuvo relación con el Consejo Nacional para la Igualdad de Género a la persona que designe el jefe/a inmediato/a; como requisito previo a la salida, para garantizar la continuidad de las operaciones importantes dentro de la Institución.

Artículo 10. Gestión Administrativa.- Los órganos administrativos responsables, deberán encargarse de velar por el acceso y seguridad física de las áreas restringidas, así como de los equipos tecnológicos y personal; el acceso deberá ser controlado y restringido para el personal ajeno a estas áreas o usuarios/as externos/as, para lo cual se puede implementar normas, controles y/o registros de acceso.

Se debe definir un área de recepción, con personal y otros medios que permitan controlar el acceso físico, supervisión de la permanencia de los visitantes en las áreas restringidas, debiendo registrar la hora, fecha de ingreso y salida, así como si ingresa con equipos o dispositivos tecnológicos, los cuales deben ser debidamente identificados y registrados.

Deben establecerse directrices restrictivas en las áreas de procesamiento de información como: prohibición de ingerir alimentos, fumar, utilizar equipos de grabación, cámaras,

equipos de video y audio, dispositivos móviles entre otros dispositivos que ponen en riesgo la conservación de la información, más aún si no se encuentran autorizados.

Establece un sistema de suministro de energía sin interrupción (UPS) o al menos permitir el cierre/apagado ordenado de los servicios y equipos que soportan las operaciones de los servicios informáticos de la Institución.

Debe disponer de documentación, diseños/planos y distribución de conexiones de: datos alámbricos/inalámbricas (locales y remotos), voz, eléctricas polarizadas, etc.

Se deberá mantener barreras físicas y de procedimientos que impidan el acceso a las áreas restringidas, pudiendo ingresar solamente el personal autorizado a ellas respetando el debido proceso de identificación.

Artículo 11. Gestión de Comunicaciones y Operaciones.- Establece las normas que regulan esta Gestión, con el propósito de proteger la Información almacenada en los computadores dentro de la infraestructura tecnológica de la Institución y minimizar los riesgos ante las amenazas que puedan surgir, para ello Tecnologías de la Información y Comunicación debe ejecutar lo siguiente:

a) Documentar los contactos de soporte y analizar los reportes de servicio, reportes de incidentes;
b) Monitorear los niveles de desempeño de los servicios; realizar proyecciones de necesidad institucional respecto de capacidad operativa y tecnológica para asegurar el desempeño de los servicios de la Institución;
c) Revisar y verificar los registros y pruebas de auditoria de terceros, con respecto a eventos de seguridad, problemas de operación, fallas relacionadas con el servicio prestado;
d) Emitir normas reglamentarias de uso de software autorizados por la Institución, que para el efecto se encargará a la unidad responsable de seguridad de información;
e) Debe instalar y actualizar de forma periódica el software antivirus y contra código malicioso, además debe, implementar soluciones que proporcionen valor agregado a las conexiones y servicios de red como; firewalls, antivirus y demás mecanismos, se encarga a la unidad responsable del área tecnológica la ejecución de dichas tareas;
f) El/la Oficial de Seguridad de la Información, el responsable de Tecnologías de la Información y los/as propietarios/as de la información, deben determinar los procedimientos, etiquetado para el resguardo y contención de la información; y,
g) Tecnologías de la Información y Comunicación es la responsable de documentar los incidentes y eventos incluyendo la hora, fecha, e información del evento, así como el registro y cuenta del administrador y operador que estuvo involucrado; además es corresponsable de la aplicación de políticas y normas para registrar los accesos, tipos de accesos, protocolos de red, sistemas de protección como antivirus y sistemas de detección de intrusos de conformidad a lo dispuesto en el numeral 6 del Esquema Gubernamental de Seguridad de la Información.

Artículo 12. Gestión de Control de Acceso.- Tecnologías de Información y Comunicación, deberá regular el proceso de administración y control de accesos lógicos a los sistemas de información, con el fin de mitigar los riesgos de accesos y uso indebido de los mismos; para ello, se aplicarán las siguientes medidas:

a) Contribuir en la socialización de la Política de Control de Accesos para usuarios a los sistemas de información acorde al nivel y tipo;
b) Establecer normas y procesos formales para la asignación y cambio de contraseñas;
c) Determinar, diseñar y especificar el manejo de usuarios/as contraseñas y características especiales para la creación y uso de contraseñas como: uso de letras mayúsculas, minúsculas, con caracteres especiales, difíciles de descifrar, que cumplan una complejidad media y alta para evitar contraseñas en blanco;
d) Controlar el cambio periódico de contraseñas e implementar medidas en el caso de que el usuario no está realizando ningún trabajo, el equipo se bloquee y lo desbloquee únicamente si el usuario ingresa nuevamente su clave;
e) Definir mecanismos para asegurar que la información transmitida por los canales de conexión remota, sean usando técnicas como encriptación de datos, redes virtuales privadas y otros que asegure la información;
f) Eliminar o deshabilitar los puertos, servicios que no requiera la Institución. g) Establecer un proceso de monitoreo y registro de los intentos exitosos y fallidos de autenticación del sistema, registros de alarmas cuando se violan las políticas de seguridad del sistema; y,
h) Identificar y documentar los equipos que se encuentran en las redes, así como realizar una evaluación de riesgos para identificar los segmentos de red donde se encuentra los activos críticos para la institución.

Artículo 13. Gestión de Adquisición y Mantenimiento de Sistemas de Información.- La unidad de Tecnologías de la Información y Comunicación es responsable de establecer normas de seguridad y controles durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan, por ello se realizará lo siguiente:

a) Implementar la política de controles y gestión de claves, así como su generación;
b) Emitir y socializar la Política sobre el uso de controles criptográficos;
c) Establecer normas de controles de cifrado (criptográficos) que se adoptan, para la implementación eficaz en toda la Institución; establece la solución a usar para cada proceso; y,
d) Evaluar los requerimientos de seguridad y los contrales requeridos, teniendo en cuenta que éstos deben ser proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que pudiera ocasionar a las actividades realizadas por alguna falla o falta de seguridad.

Artículo 14. Consideraciones de la Seguridad de la información con actores externos (Ciudadanos/as o entidades gubernamentales o de control). Previo a la entrega de información a ciudadanos/as o clientes de entidades gubernamentales o de control, los

órganos administrativos del CNIG responsables de proveer la información solicitada deberán considerar los siguientes criterios:

a) Autorización de la máxima autoridad o su delegado;
b) Tipo de información solicitada;
c) Protección de activos de información;
d) Protección de datos en base a la Constitución, Ley del Sistema Nacional de Registro de Datos Públicos, LOTAIP y demás Leyes nacionales aplicables a los planes, programas y proyectos de la Institución, particularmente datos personales de ciudadanos y/o financieros; y,
e) Entendimiento adecuado de los acuerdos de confidencialidad de la información entre la Institución y el solicitante con el objeto de cumplir los requisitos de la seguridad de la Institución.

Capítulo IV
ADMINISTRACION DE RIESGOS

Artículo 15. Gestión de Incidentes Informáticos.- Se establece los lineamientos generales para la gestión efectiva de incidentes de seguridad que afecten a la Institución y al cumplimiento de su misión y objetivos, con la finalidad de prevenir y responder de forma idónea, para lo cual, Tecnologías de la Información y Comunicación realiza las siguientes acciones:

a) Implementar y ejecutar el procedimiento formal para el reporte de eventos de seguridad informáticos junto al procedimiento de escalada y respuesta al incidente que amenace la seguridad informática;
b) Mantener una bitácora de registro de incidentes y el reporte de vulnerabilidades de la seguridad de la información, el monitoreo de los sistemas, alertas y las vulnerabilidades, se establece y ejecuta un procedimiento para la gestión de incidentes;
c) Identificar y clasificar los diferentes tipos de incidentes de seguridad de la información mediante la mesa de servicios y con la utilización de la matriz de asignación de responsabilidades-matriz RACI;
d) Identificar y analizar las posibles causas de un incidente producido;
e) Planificar e implementar acciones conectivas para evitar la recurrencia del incidente; y,
f) Establecer procesos internos cuando se recolecta y se presenta evidencia con propósitos de acción disciplinaria dentro de la Institución.

El/la servidor/a, funcionario/a, trabajador/a, practicante o cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género, de turno que sea responsable del equipo o sistema afectado debe identificar, registrar el incidente en la bitácora incluyendo datos, fecha y hora, así como el tipo de incidente suscitado y el nivel de severidad del mismo.

En caso de que el/la servidor/a, funcionario/a, trabajador/a, practicante o cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género, de turno no pueda

solucionarlo, el escalamiento debe ser registrado en la bitácora de escalamiento de incidentes, se notificará al jefe inmediato.

Artículo 16. Gestión de Incidentes de la Seguridad de la Información.- En caso de que los incidentes informáticos que produzcan afectación en la Seguridad de lo Información de esta Institución, el/la Oficial de Seguridad de la Información es el contacto para el reporte de los eventos de seguridad de la información. Los/las servidores/as, funcionarios/as, trabajadores/as, practicantes, cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género y usuarios contratados por los proveedores deben reportar todos los eventos de inseguridad de la información lo más pronto posible.

Los/las servidores/as, funcionarios/as, trabajadores/as, practicantes, cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género y usuarios/as contratados/as por los proveedores de la Institución, deben informar los asuntos de las debilidades en la seguridad al Responsable de Tecnologías de la Información, tan pronto como sea posible. Cuando se detecte alguna vulnerabilidad o debilidad en un equipo o sistema se debe:

a) Informar y notificar a su jefe/a inmediato/a y este al Oficial de Seguridad de la Información la debilidad y vulnerabilidad encontrada;
b) El/la Oficial de Seguridad de la Información debe llevar el reporte de vulnerabilidades y debilidades de seguridad de la información, que contendrá la fecha, hora, apellidos, nombres de los/las servidores/as, funcionarios/as, trabajadores/as, practicantes o cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género que detectó la debilidad, descripción de la misma, detalle de posibles incidentes de seguridad que pudieran ocurrir como producto de la vulnerabilidad;
c) El/la Oficial de Seguridad de la información debe emitir un reporte del o los incidentes ocurridos a los/as jefes/as de las unidades donde se produjo el incidente; y,
d) El/la Oficial de Seguridad de la Información en coordinación con el Responsable de Tecnologías de la Información realizarán una evaluación del impacto generado por el o los incidentes de seguridad de la información producidos donde se evidencie el tipo de incidente, el número de incidentes graves, el tiempo medio de resolución de incidentes, costo promedio de incidentes, frecuencia del incidente.

Capítulo V
SANCIONES POR INCUMPLIMIENTO DE LAS POLITICAS DE SEGURIDAD DE LA INFORMACION

Artículo 17. En caso de detectar incumplimiento de esta política, el/la titular del órgano administrativo del CNIG pondrá en conocimiento de el/la Oficial de Seguridad de la Información, la transgresión de la Política de Seguridad establecida en el presente instrumento y demás normativa relacionada, para ello el/la Oficial de Seguridad de la Información levantará un informe que será puesto en conocimiento de la Unidad de Administración de Talento Humano y a la máxima autoridad.

Cuando el/la titular del órgano administrativo del CNIG omita notificar al Oficial de Seguridad de la información, sobre las transgresiones de la Política de Seguridad de la información e instrumentos vinculantes, se pondrá en conocimiento de la máxima autoridad.

La divulgación o uso de la información que ocasionen el incumplimiento del presente instrumento podrá ser sancionado por el delito de difusión de información de circulación restringida o cualquier otro tipificado en el Código Orgánico Integral Penal, y leyes conexas; para lo cual, el Consejo se reserva el derecho de iniciar las acciones administrativas, civiles o penales de las que se crea asistido, incluyendo la reclamación de daños y perjuicios sin límite alguno.

Cualquier uso malicioso, ilegal o fraudulento de la información estará sujeto al procesamiento penal de su responsable, sin perjuicio de las demás acciones legales a las que hubiere lugar, así como de la determinación del régimen disciplinario correspondiente.

Los mencionados informes, servirán de insumo para lo determinado en líneas precedentes.

DISPOSICIONES GENERALES

Primera.- Las políticas elaboradas y emitidas por el Comité de Seguridad de la Información (EGSI), serán de cumplimiento obligatorio para todos/as los/las servidores/as, funcionarios/as, trabajadores/as, practicantes o cualquier persona que tenga relación con el Consejo Nacional para la Igualdad de Género.

Segunda.- El/la Oficial de Seguridad de la Información de ser necesario identificará y definirá nuevas políticas de carácter específico y particular para diferentes procesos que se implementen en el CNIG, con la aprobación de la máxima autoridad y que serán incorporadas en las siguientes actualizaciones de la Política de Seguridad de la Información.

Tercera.- El/la Oficial de Seguridad de la Información conjuntamente con la Unidad de Comunicación Social, y Tecnologías de la Información y Comunicación, serán responsables de elaborar estrategias de difusión y capacitación a todos los/las servidores/as, funcionarios/as, trabajadores/as, practicantes y en general a todo el personal del Consejo Nacional para la Igualdad de Género, sobre el Esquema Gubernamental de la Información (EGSI) y de la Política de Seguridad de la información.

Cuarta.- El/la Oficial de Seguridad de la Información, presentará un informe semestral a la máxima autoridad, respecto de novedades, seguimiento y cumplimiento de las presentes políticas.

Quinta.- Encárguese de la difusión de la presente Resolución a la Dirección de Asesoría Jurídica.

Sexta.- Encárguese a la Unidad de Comunicación Social la publicación de esta Resolución en la Intranet de la Institución.

DISPOSICIÓN FINAL

Esta Resolución rige a partir de la fecha de su suscripción, sin perjuicio de su publicación en el Registro Oficial.

Dada en la ciudad de Quito, Distrito Metropolitano, el 05 de Noviembre de 2020.

NELLY PIEDAD JACOME VILLALVA

Firmado digitalmente por NELLY PIEDAD JACOME VILLALVA
Fecha: 2020.11.05 15:43:14 -05'00'

Dra. Nelly Jácome Villalva
SECRETARIA TÉCNICA
CONSEJO NACIONAL PARA LA IGUALDAD DE GÉNERO

sz/lc