Consejo Nacional para la Igualdad Intergeneracional

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

(Alto Nivel)

Contenido

1. OBJETIVOS.

- ✓ Establecer directrices políticas sobre las cuales se debe direccionar el desarrollo de la seguridad de información del Consejo Nacional para la Igualdad Intergeneracional (CNII), adicionalmente que regule toda la administración de los activos de información.
- ✓ Proteger los recursos de información y tecnología utilizados para su procesamiento, frente a amenazas internas y externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad, mediante la implementación de controles efectivos. Asegurar la comunicación y gestión efectiva ante eventos, debilidades e incidentes de seguridad de la información.
- ✓ 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.

2. ALCANCE.

El EGSI cubrirá todos aquellos aspectos a tener en cuenta en relación a estándares, procedimientos, normas y medidas que empleen tecnología que permitan asegurar la confidencialidad, integridad y disponibilidad de la información, la cual permitirá proteger todos los activos de información que permiten el desempeño normal y exitoso de las funciones, servicios y actividades principales del CNII.

3. NORMATIVA VIGENTE.

El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), a través del Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, publicó en el Registro Oficial, Tercer Suplemento Nº 509 del viernes, 01 de marzo de 2024, el Esquema Gubernamental de Seguridad de la Información (EGSI versión 3), el cual establece:

"Artículo 1.- Expedir el Esquema Gubernamental de Seguridad de la Información – EGSI que se encuentra como Anexo al presente Acuerdo Ministerial, el cual es el mecanismo para implementar el Sistema de Gestión de Seguridad de la Información en el Sector Público.

Artículo 2.- El EGSI es de implementación obligatoria en las entidades, organismos e instituciones del sector público, de conformidad con lo establecido en el artículo 225 de la Constitución de la República del Ecuador y los artículos 7 literal o), y 20 de la Ley Orgánica para la Transformación Digital y Audiovisual; y, además, es de implementación obligatoria para terceros que presten servicios públicos

mediante concesión, u otras figuras legalmente reconocidas, quienes podrán incorporar medidas adicionales de seguridad de la información." (…)

4. MARCO NORMATIVO.

4.1. Documentos Externos

- Constitución de la República del Ecuador
- Ley Orgánica de Transparencia y Acceso a la Información Pública.
- Ley del Sistema Nacional de Archivos.
- Ley Orgánica para la Optimización y Eficiencia de Trámites Administrativos (LOETA).
- Ley Orgánica de Protección de Datos Personales
- Ley Orgánica para la Transformación Digital y Audiovisual.
- Reglamento de la Ley Orgánica de la Contraloría General.
- Decreto Ejecutivo No. 1014 sobre el uso de Software Libre en la Administración Pública.
- Decreto Ejecutivo No. 1384 sobre Interoperabilidad Gubernamental en la Administración Pública.
- Acuerdo Ministerial Nro.MINTEL-MINTEL-2024-0003, publicado en el Registro Oficial, Tercer Suplemento Nº 509 del viernes, 01 de marzo de 2024.
- Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de recursos públicos.
- Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000.

4.2. Documentos Internos

- No aplica.

4.3. Normas Generales

- Las normas de esta política son de aplicación obligatoria para todos los funcionarios del CONSEJO NACIONAL PARA LA IGUALDAD INTERGENERACIONAL (CNII), en tanto guarden conformidad con las disposiciones constitucionales, legales, reglamentarias y resoluciones vigentes al momento de su ejecución.
- El servidor que incumpliere sus obligaciones o contraviniere las disposiciones de esta política, así como las leyes y normativa conexa, incurrirá en responsabilidad administrativa que será sancionada disciplinariamente, sin perjuicio de la acción civil o penal que pudiere originar el mismo hecho.

- La Dirección de Planificación y Gestión Estratégica con su unidad de Tecnologías de la Información en el ámbito de sus competencias, ejecutarán actividades que aseguren el cumplimiento del presente documento, para lo cual podrán acceder a los registros de auditoría de los aplicativos informáticos e información contenida en bases de datos institucionales, así como a la información custodiada por el personal del CNII.
- Todos los funcionarios del CNII aplicarán las normas de seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la institución, tendrán acceso permanente a este documento desde la nube de información institucional y se obligan a cumplirlo.
- Es obligación de las unidades administrativas, funcionarios del CNII, entregar oportunamente la información solicitada en procesos de monitoreo y control del cumplimiento de este documento.

5. GLOSARIO DE TÉRMINOS Y ABREVIATURAS.

TÉRMINO / ABREVIATURA	DEFINICIÓN
Activos de Información	Ficheros y bases de datos, contratos y acuerdos, documentación institucional, manuales de los usuarios, material de formación, aplicaciones, software del sistema.

6. RESPONSABILIDADES.

Elaboración de la política: La persona asignada es responsable de la elaboración de la presente política.
Revisión y Aprobación de la política: El Comité de Seguridad de la Información (Unidad de Planificación y Gestión Estratégica) es responsable de la revisión y aprobación de la presente política.
Cumplimiento de la política: Los funcionarios de la institución son responsables de cumplir con la presente política.
Actualización de la política: El presente documento, deberá ser revisado y actualizado a intervalos de un año o cuando se produzcan cambios significativos en las normativas vigentes, leyes y reglamentos generales de aplicación, actos administrativos normativos y demás regulaciones en las que está soportada.

7. POLITICA DE SEGURIDAD DE INFORMACIÓN.

Implantar y mantener un Sistema de Gestión de Seguridad de la Información y Servicios TI basado en los requisitos de las normas Técnicas Ecuatorianas INEN ISO/IEC 27000 EGSI ISO/IEC 27001, para asegurar la confidencialidad, integridad y disponibilidad de la información que promueven la eficacia de los procesos y la mejora continua de su sistema de gestión.

7.1. Responsabilidades de la Gestión Interna de Tecnología Informática.

La responsabilidad ante la adquisición, instalación, mantenimiento y buen funcionamiento de los equipos de la Institución son las siguientes:

- ✓ Levantará y verificará el inventario de los equipos y programas informáticos que sean instalados, con la finalidad de llevar un control de los mismos.
- ✓ Será responsable de hacer requerimientos de los activos informáticos, según las necesidades que se presenten en cada dirección.
- ✓ Deberá entregar informes de la vida útil de los equipos de informática, con la finalidad de optimizar su uso.
- ✓ Deberá ser parte en todo proceso de adquisición de equipos o software informáticos.
- ✓ Deberá realizar el mantenimiento preventivo y correctivo de todos los equipos informáticos de la Institución.
- ✓ Será el único responsable de instalar los equipos y programas informáticos utilizados en la Institución.
- ✓ Será el encargado de evaluar el área física donde se instalará los nuevos equipos informáticos, confirmando que el área este óptima para la instalación de los mismos.
- ✓ Deberá solicitar a la Dirección Administrativa Financiera la adecuada infraestructura, previamente a la instalación de los equipos informáticos requeridos por las direcciones correspondientes.
- ✓ Instalará todas las aplicaciones de los equipos y programas informáticos utilizados por la Institución.
- ✓ Deberá dar una capacitación al usuario sobre el uso y manejo adecuado de los equipos y programas informáticos instalados.

7.2. Propiedad del equipo.

Los recursos informáticos asignados a los funcionarios, deben usarse adecuadamente, con responsabilidad acorde a los siguientes lineamientos:

- ✓ El CNII, proveerá a su personal del equipo de cómputo, según las actividades a realizar y cuyo desempeño organizacional se considere necesario.

- ✓ El equipo de cómputo asignado se utilizará exclusivamente para las labores propias de la institución. El usuario debe cuidar la integridad, buen uso y limpieza del equipo. Los equipos de cómputo no podrán ser trasladados del lugar designado o fuera del CNII sin previa autorización de la Dirección Administrativa Financiera.
- ✓ Los funcionarios por ningún motivo podrán instalar en los discos duros de las computadoras, programas ajenos a los proporcionados por la institución y ningún material digital que atente contra la moral pública.
- ✓ El usuario no debe instalar componentes a los equipos de cómputo y periféricos sin previa autorización de la GITI, cualquier cambio a la configuración original del equipo deberá ser realizado por la Gestión Interna de Tecnología de Información (GITI).
- ✓ La Gestión Interna de Tecnología de Información (GITI) es la única autorizada a remover o instalar componentes, reparar o gestionar la reparación de equipos de cómputo o periféricos. La pérdida de la garantía del equipo provocada por el usuario se notificará a su jefe inmediato. En caso de comprobarse el uso negligente del equipo de cómputo por parte del usuario deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado.
- ✓ Cuando el usuario se percate de que alguna pieza del equipo en cuestión haya sido removida, cambiada o dañada deberá ser notificada a su jefe inmediato y a la Gestión Interna de Tecnología de Información (GITI).
- ✓ El usuario es responsable de cerrar su sesión de trabajo y dejar el equipo en suspensión, cuando deje de usarlo por tiempo prolongado.
- ✓ No dejar dispositivos de respaldo de información, como USB, Pendrive, CD, DVD, etc., al alcance de cualquier persona.
- ✓ No escribir contraseñas ni otros datos sensibles en papeles o documentos que queden a la vista.
- ✓ Se establecen las cuentas de acceso a los equipos son un elemento intransferible y de carácter individual.
- ✓ Las cuentas de acceso a sistemas gubernamentales e institucionales se realizará previo requerimiento escrito del área de Talento Humano del CNII.
- ✓ Está prohibido tener sustancias o líquidos en su escritorio, los que pueden dañar los equipos, así como la documentación.
- ✓ Desde el momento en que firma el acta de asignación de un equipo, la responsabilidad sobre el estado del equipo, es totalmente del usuario.

7.3. Propiedad de la información.

- ✓ Toda la información recolectada, elaborada, distribuida, procesada y almacenada, junto con los procesos que manipulan dicha información en las instalaciones o en cualquier sistema informático, durante la jornada laboral será propiedad exclusiva del CNII, por lo que el empleado no podrá considerarla de carácter personal.

- ✓ Toda la información perteneciente al CNII, no podrá ser extraída por ningún medio de almacenamiento, ni podrá ser transmitida por ningún medio alámbrico o inalámbrico, para su uso fuera de la institución sin previa autorización por correo electrónico de su jefe inmediato.
- ✓ Los respaldos de información deberán solicitarse a la GITI y se realizarán en los servidores, equipos informáticos o medios de almacenamiento destinados para este fin y estarán ubicados dentro del CNII.

7.4. Uso de correo electrónico institucional.

- ✓ La creación de una cuenta de correo electrónico debe ser solicitada formalmente a la Unidad de Planificación y Gestión Estratégica por parte de la Dirección Administrativa Financiera.
- ✓ El sistema de correo electrónico debe ser usado únicamente para realizar tareas propias de las funciones que se desarrollan en la institución y no debe utilizarse para ningún otro fin.
- ✓ La cuenta de correo que le sea asignada al usuario es personal e intransferible.
- ✓ La definición de la cuenta de correo está a cargo de la GITI.
- ✓ Cada usuario es responsable de la contraseña que utilice para acceder al correo, la cual tiene carácter de privada e intransferible.
- ✓ La contraseña debe tener al menos 6 caracteres alfanuméricos combinando letras mayúsculas, minúsculas, números y caracteres especiales (Pepito1*).
- ✓ Para evitar, alto consumo de ancho de banda y saturación involuntaria, se debe comprimir los archivos para que tengan un tamaño máximo de 10MB que se adjunten al correo.
- ✓ Se debe cerrar la sesión del correo electrónico para evitar que otra persona use su cuenta sin su autorización.
- ✓ Cada usuario es responsable de toda la información enviada desde su correo electrónico.
- ✓ Queda prohibido el uso del correo electrónico e Internet para fines políticos y religiosos dentro y hacia fuera de la Institución.
- ✓ Queda prohibido enviar correos con información no relacionada con las funciones específicas de la institución.
- ✓ No se podrá usar la cuenta de correo electrónico institucional como referencia para crear perfiles en redes sociales, compras online, instituciones bancarias, etc.

7.5. Acceso y uso de la Internet y sus aplicaciones/servicios.

- ✓ Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la institución, y no debe utilizarse para ningún otro fin.
- ✓ Debe limitarse a los funcionarios el acceso a portales, aplicaciones o servicios de la Internet y la Web que pudieren perjudicar los intereses de la institución. Específicamente, se debe bloquear el acceso por medio de dispositivos fijos y/o móviles a aquellos portales, aplicaciones o servicios de la Internet

y la Web sobre pornografía, racismo, violencia, delincuencia o de contenidos ofensivos y contrarios a los intereses, entre otros, y valores de la institución o que impacten negativamente en la productividad y trabajo de la institución (ej., mensajería instantánea-chats, redes sociales, video, otros) y particularmente a los que atenten a la ética y moral.

- ✓ La institución podrá en cualquier momento bloquear o limitar el acceso y uso de la Internet a los funcionarios o a terceros que accedan tanto por medio alámbrico como inalámbrico.

7.6. Dispositivos Externos.

- ✓ Todo equipo de cómputo tendrá acceso al enlace inalámbrico de internet del CNII previa solicitud y autorización de la máxima autoridad
- ✓ La clave para acceso se deberá pedir al encargado de la GITI mediante correo electrónico.
- ✓ En cualquier momento el área de GITI podrá deshabilitar el acceso a los dispositivos móviles sin previo aviso por demandas institucionales.

7.7. Teletrabajo.

El/la servidor/a que se encuentre en teletrabajo, se compromete a respetar la legislación en materia de protección de datos, las políticas de seguridad y privacidad de la información que la institución ha implementado, como también con el cumplimiento de las siguientes normas:

- ✓ El acceso remoto a sistemas de información de la institución únicamente se podrá realizar mediante mecanismos de seguridad establecidos por la institución (claves de acceso).
- ✓ Los/as servidores/as son responsables de la información utilizada y procesada para el desarrollo de sus funciones, por tal razón deberán realizar de copias de respaldo de la información regularmente para asegurar la continuidad de las funciones realizadas.
- ✓ El almacenamiento de la información se deberá realizar en la nube institucional.
- ✓ El mantenimiento y soporte de equipos que son propiedad de la institución, se lo realizará mediante correo electrónico al responsable de soporte del área de GITI.
- ✓ Se dará soporte a usuario mediante herramientas remotas como es any desk o teamviewer y en caso de ser necesario se retirará su equipo para mantenimiento físico.
- ✓ La administración, mantenimiento y soporte de equipos que son propiedad de los funcionarios, es responsabilidad de los mismos, en ningún momento la institución, se hace responsable por estas actividades.
- ✓ Cada funcionario podrá retirar su equipo informático llenando el formulario de "*Retiro de equipos informáticos*" y será responsable de su cuidado.

- ✓ En caso de pérdida, suplantación o robo de equipo informático o cualquier medio de almacenamiento utilizado, se deberá realizar de forma inmediata, el respectivo reporte al administrador de bienes de la institución y se deberá poner la denuncia ante la autoridad competente.

7.8. Usuarios y Contraseñas

Siempre que los funcionarios hagan uso de contraseñas, ya sea, para el acceso a los sistemas de información o a las cuentas de Servicios Informáticos institucionales, deben cumplir las siguientes normas:

- ✓ El nombre de usuario y contraseña de inicio de sesión en su equipo personal, serán entregados por la Gestión Interna de Tecnología de Información (GITI) al usuario.
- ✓ Las contraseñas son de uso personal y por ningún motivo se deberán entregar a otros servidores.
- ✓ Todas las contraseñas del sistema utilizados en el CNII (cuentas de correo, cuentas de servicios web, etc.), se cambiarán con una periodicidad de al menos una vez cada seis meses.
- ✓ Los funcionarios deberán cambiar las contraseñas la primera vez que usen las cuentas asignadas.
- ✓ Las contraseñas estarán compuestas al menos por: una letra mayúscula, una minúscula, número, caracteres especiales y su longitud debe ser de ocho (8) caracteres mínimos.
- ✓ Reportar a la GITI de cualquier sospecha de que una persona esté utilizando una contraseña y una cuenta que no le pertenece.
- ✓ Las contraseñas de los funcionarios que terminen relación con el CNII se desactivarán por parte de la GITI cuando reciba la solicitud respectiva por parte de la Dirección Administrativa Financiera.

7.9. Uso de controles criptográficos.

La unidad de GITI deberá identificar a la(s) persona(s) responsable(s) de implementar la política, así como de su debida administración. Se utilizará controles criptográficos para la protección de la confidencialidad, integridad y disponibilidad de la información en los siguientes casos:

- ✓ Protección de claves de acceso a sistemas de información.
- ✓ Protección de documentos electrónicos.
- ✓ Transmisión de información confidencial fuera de la institución.
- ✓ Se definirá algoritmos de cifrado según el nivel de clasificación de la información. La GITI será la encargada de la gestión de claves criptográficas y tendrá las siguientes responsabilidades:
- ✓ Serán los responsables de la administración de claves criptográficas.
- ✓ Cada clave criptográfica tendrá un ciclo de vida, el cual dependerá de la clasificación de la información.
- ✓ Todas las claves criptográficas deberán estar protegidas contra modificaciones, divulgación y destrucción.

7.10. Desarrollo Seguro.

- ✓ La presente política establece controles para garantizar que la seguridad de la información sea un requisito para el desarrollo de nuevos sistemas o la mejora a los existentes.
- ✓ Previo a que un sistema de información sea desarrollado, mantenido o adquirido, el dueño del proceso deberá especificar los requerimientos o necesidades; por tanto, deberá adjuntar el "Anexo 01 Formato de Requerimientos".
- ✓ La solicitud deberá ser evaluada con respecto a su viabilidad y conveniencia para analizar alternativas de desarrollo y la evaluación de los aspectos de seguridad necesarios en cumplimiento de los objetivos del requerimiento.
- ✓ Todo lineamiento de seguridad debe ser incluido en los requisitos para los sistemas de información nuevos o mantenciones de los sistemas de información existentes.
- ✓ Para mantener la seguridad de los desarrollos, se implementará de ser posible una separación de ambientes para desarrollo, aseguramiento de la calidad y producción.
- ✓ Los desarrolladores deben monitorear de manera continua el proceso de diseño y construcción, a fin de evitar, encontrar y solucionar vulnerabilidades en los sistemas.
- ✓ La Unidad de GITI, debe elaborar y mantener una lista de todos los sistemas de información indicando la criticidad de cada uno.
- ✓ Se deben realizar pruebas periódicas a los sistemas de información de la entidad, para lo cual, se deben tener bien definidos ambientes de pruebas seguros, y en caso de que el desarrollo sea hecho externamente.
- ✓ Todo desarrollo, que haya sido creado interna o externamente, debe contar con un proceso de soporte. En caso de ser creado de manera interna, el (los) desarrollador(es) deben proporcionar un nivel adecuado de soporte y de documentación.
- ✓ El desarrollo de trabajo externo debe seguir los mismos lineamientos definidos en esta Política.

7.11. Equipo de impresión

- ✓ Los recursos de impresión deben ser utilizados con fines de apoyo en las labores diarias pertinentes a cada departamento del CNII, por lo que, no es permitida la impresión de trabajos personales.
- ✓ Las impresoras conectadas como recurso compartido serán preinstaladas en cada equipo dónde sea requerido; en caso de que se pierda conexión o exista la necesidad de reconfiguración se solicitará de manera formal a la GITI mediante el mecanismo de soporte implementado.
- ✓ Los recursos de las impresoras pueden ser manipulados o reemplazados, solamente, por personal de la GITI.
- ✓ Las impresoras a color solo serán utilizadas para imprimir documentos que exclusivamente requieran ser impresos a color, no para hacer pruebas ni borradores.

7.12. Sistema de video-conferencia

- ✓ La grabación de la videoconferencia podrá ser realizada por cualquiera de las Partes, previo acuerdo. Si se acuerda que una de las Partes se encarga de la grabación, la misma se compromete a realizar la grabación, custodia y registro de la videograbación. La grabación estará a disposición de las Partes que lo requieran.
- ✓ Las Partes acordarán las reglas de confidencialidad y seguridad de las videoconferencias en cuanto a la realización y resguardo de la información transmitida.
- ✓ Las Partes se comprometen a coordinar y respetar las pautas de días y horarios de inicio con el objeto de no demorar los actos. El equipamiento deberá estar disponible en cada extremo y conectado con un mínimo de 30 minutos antes del horario de inicio.
- ✓ La videoconferencia puede ser cancelada por motivos de fuerza mayor comunicadas en forma previa o al iniciar la misma, por fallas técnicas que no pudieran ser subsanadas y/o fallas de coordinación entre los participantes. Se elevará un informe a la instancia superior informando los motivos de la cancelación. Las partes se comprometen a subsanar dichos inconvenientes y/o realizar pruebas que no comprometan futuros eventos de la misma índole.
- ✓ Las solicitudes de transmisión en vivo se deben realizar al responsable de la Unidad mínimo ocho días antes de la misma, así se garantiza la realización de pruebas previas a los eventos.
- ✓ Se destinará un equipo de cómputo específico para realizar las transmisiones en vivo, con esto se garantizará la confiabilidad e integridad del evento.

7.13. Escritorios limpios.

- ✓ Se deberá guardar en un lugar seguro cualquier documento, medio magnético u óptico removible que contenga información sensible.
- ✓ Todos los funcionarios de la institución, deben dejar siempre sus equipos bloqueados en caso de no estar en su puesto de trabajo.
- ✓ Todo el personal debe adoptar las medidas de seguridad necesarias para la adecuada custodia de documentos y demás medios de almacenamientos de información institucional.
- ✓ No escribir contraseñas ni otros datos sensibles en papeles o documentos que queden a la vista.
- ✓ Desde el momento en que firma el acta de asignación de un equipo, la responsabilidad sobre el estado del equipo, es totalmente del usuario.
- ✓ El/la servidor/a realizará el apagado por completo del equipo al término de la jornada, excepto aquellos que por su naturaleza y servicio requieran estar encendidos las 24 horas, el apagado incluye a los periféricos (impresoras, escáner).
- ✓ Todos los funcionarios deberán guardar en un lugar seguro los documentos y medios que contengan información relevante de la institución.

7.14. Respaldo de información.

- ✓ La Gestión Interna de Tecnología de Información (GITI) definirá el estándar de respaldos de los servidores y los equipos de hardware de la institución.
- ✓ La Gestión Interna de Tecnología de Información (GITI) deberá generar los planes de respaldo, coordinar, ejecutar y probar en intervalos de tiempo los respaldos de información, llevar registros de los respaldos y de pruebas.
- ✓ La Gestión Interna de Tecnología de Información (GITI) definirá el tiempo y periodicidad de respaldos que se utilizará para cada aplicación.
- ✓ Se debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
- ✓ Para restauración de información se deberá realizar una solicitud a la Unidad responsable conforme la metodología aprobada, y acorde a las necesidades que se requiera.
- ✓ Los documentos y archivos digitales se deberán guardar únicamente en la nube de información del CNII de cada funcionario, los archivos que no se encuentren en esta carpeta no serán respaldados y el área de TI no se responsabilizará de su perdida.
- ✓ Es responsabilidad de todos los funcionarios identificar la información que debe ser respaldada y almacenarla de acuerdo a su nivel de sensibilidad.

7.15. Control de Acceso

- ✓ Los funcionarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información.
- ✓ Se deben establecer procedimientos formales para el registro y eliminación de funcionarios, de modo de garantizar que se otorguen y quiten accesos a los sistemas y servicios de información.
- ✓ Se deben revisar los derechos de acceso otorgados a los funcionarios regularmente a través de procedimientos formales.
- ✓ Para los accesos a sistemas se deben establecer procedimientos de autenticación seguros, de modo de minimizar la oportunidad de accesos no autorizados.
- ✓ Todos los funcionarios deben autenticarse con usuario y contraseña válidos antes de ingresar a los sistemas de información de la institución.

7.16. Gestión de incidentes.

- ✓ Adoptar medidas de seguridad eficientes para proteger sus activos de información crítica.
- ✓ Analizar los eventos de seguridad informática para ver si se trata un incidente de seguridad de información.
- ✓ Ejecutar procedimientos de respuesta a incidentes para contener y mitigar incidentes.

- ✓ Documentar y clasificar los incidentes.
- ✓ Tener una base de conocimiento para prevenir nuevos incidentes.

7.17. Seguridad física.

- ✓ Se deberá dar tratamiento a amenazas tales como acceso no autorizado, robo, pérdida, daño, entre otros (riesgos físicos y ambientales) que puedan afectar los activos de información, medios de procesamientos y comunicaciones, así como las instalaciones donde que se encuentran ubicados.
- ✓ Estas áreas deben contar con protecciones físicas y ambientales acordes con los activos que protegen, incluyendo perímetros de seguridad, controles de acceso físicos, controles especiales en áreas de mayor sensibilidad, seguridad de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales de operación y sistemas de contención, detección y extinción de incendios adecuados, que preserven el medio ambiente.
- ✓ Esta seguridad debe conservarse en los momentos de mantenimiento, cuando la información o los equipos que la contienen salen de la entidad o cuando se eliminan o dan de baja.

7.18. Clasificación de la información.

Los delegados de cada dirección clasificarán la información de acuerdo a los parámetros establecidos a continuación:

Nivel	Descripción
Alta o Confidencial	Cuando el nivel de confidencialidad de la información se incremente.
Media o Reservada	Para niveles medios de confidencialidad.
Baja o Pública	Información con un nivel bajo de confidencialidad y todas las personas pueden ver dicha información.

- ✓ Estos niveles serán divulgados y oficializados a la institución, para asegurar que los niveles de protección son entendidos y se mantienen, la socialización se realizará una vez que se finalizado el levantamiento del inventario con cada unidad organizativa.
- ✓ Se define como Custodios de Información Institucional, al personal de la Institución que usa o resguarda, temporal o permanentemente la información durante su vinculación laboral.

7.19. Software no autorizado por la institución.

- ✓ Está expresamente prohibido descargar, usar, intercambiar y/o instalar software no autorizado, información y/o productos, que de alguna forma atenten contra el régimen legal e institucional de la propiedad intelectual.
- ✓ No descargar, usar, intercambiar y/o instalar archivos que contengan código malicioso o herramientas de hacking.
- ✓ Ningún funcionario podrá adelantar acciones orientadas a dañar, atacar o entorpecer la información que se procesa o almacena en los sistemas de la institución, ya sea a través de medio físico o electrónico alguno.
- ✓ No hacer uso de herramientas que comprometan la disponibilidad, desempeño y confidencialidad de datos transmitidos por la red de la institución.

7.20. Software de antivirus

- ✓ Este software se instalará únicamente en aquellos equipos de cómputo que hayan sido designados como bienes institucionales y a su vez, previamente autorizados.
- ✓ Ningún usuario debe por su propia cuenta y por ninguna razón, deshabilitar las aplicaciones de antivirus instaladas en los equipos de la Institución.
- ✓ Toda instalación o desinstalación de las aplicaciones de antivirus, será llevada a cabo únicamente por personal de la Gestión Interna de Tecnología de Información (GITI).

7.21. Autorizaciones

- ✓ Toda autorización en la instalación de software, hardware, aplicaciones y recursos informáticos en los equipos de propiedad del CNII, necesarios para llevar a cabo las labores administrativas respectivas, deberá constar por memorando y ser solicitada a la dirección correspondiente.
- ✓ La Gestión Interna de Tecnología de Información (GITI) es la única autorizada a realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos del CNII.
- ✓ Las autorizaciones concedidas a los/las servidores/ras para acceder a los recursos de la red de datos; serán estrictamente individuales y no transferibles. Las mismas pueden expirar con el cese de las actividades que la han justificado o por la no solicitud de renovación.

8. SANCIONES.

El incumplimiento de la presente política se seguridad de la información se sujetará a la investigación administrativa y a la imposición de las medidas disciplinarias correspondientes, de acuerdo a lo

previsto en el Reglamento Interno de administración del Talento Humano del Consejo Nacional para la Igualdad Intergeneracional.

Leves. **-** Cuando su afectación no es de forma significativa, se notificará a la Dirección Administrativa Financiera para que se aplique el reglamento interno vigente. Se consideran faltas leves a las acciones u omisiones realizadas ya sea por error, descuido o desconocimiento menor, siempre que no exista la intención de causar daño y que no altere o perjudique gravemente el normal desarrollo o desenvolvimiento del Consejo Nacional para la Igualdad Intergeneracional. Las mismas que tendrán las siguientes sanciones: Amonestación verbal, Amonestación escrita; Sanción pecuniaria administrativa.

Amonestación Verbal. - A más de las faltas establecidas en el Reglamento Interno de administración del Talento Humano del Consejo Nacional para la Igualdad Intergeneracional, se impondrá amonestación verbal en los siguientes casos:

1. No asistir a las capacitaciones sobre seguridad de la información sin justificación.
2. No cumplir los procedimientos establecidos para el uso de contraseñas.
3. Abrir páginas de Internet restringidas y hacer mal uso de la red
4. Uso de software no autorizado.
5. Afectar el espacio laboral por el uso fuerte del volumen de audio en el equipo de cómputo u otros dispositivos electrónicos.

Amonestación Escrita. - A más de las faltas establecidas en el Reglamento Interno de administración del Talento Humano del Consejo Nacional para la Igualdad Intergeneracional, se impondrá amonestación escrita en los siguientes casos:

1. Acceder a páginas web no relacionadas con sus funciones.
2. Retrasar sin causa justificada el reporte de incidentes en los equipos electrónicos.
3. Omitir la actualización de antivirus o parches en los equipos asignados
4. Descargar, usar, intercambiar y/o instalar software no autorizado, información y/o productos, que de alguna forma atenten contra el régimen legal e institucional de la propiedad intelectual.
5. Instalar archivos que contengan código malicioso o herramientas de hacking.
6. Queda prohibido al personal que tiene a su cargo un equipo de cómputo, prestarlo a personas ajenas a la institución sin la debida autorización, pues éste será directamente responsable del mal uso que se otorgué a dicho equipo o de la información que sea sustraída del mismo.
7. Provocar daños intencionales al equipo de cómputo.

Graves. **-** Cuando su afectación es de forma significativa a la institución, se notificará a la dirección Administrativa Financiera para que se aplique el reglamento interno vigente. Son aquellas acciones u omisiones que alteren gravemente el ordenamiento jurídico o institucional, se sancionarán con suspensión temporal sin goce de remuneración o destitución, previo el trámite del sumario administrativo correspondiente, que se sustanciará en aplicación de las garantías del debido proceso,

respetando el derecho a la defensa, de acuerdo al procedimiento establecido en la normativa legal vigente. Las faltas graves darán lugar a la imposición de las siguientes sanciones: Suspensión temporal de funciones sin goce de remuneración; y, Destitución.

Suspensión temporal de funciones sin goce de remuneración. – Se impondrá la sanción de Suspensión temporal de funciones sin goce de remuneración, a más de los casos señalados en el Reglamento Interno de administración del Talento Humano del Consejo Nacional para la Igualdad Intergeneracional, los siguientes:

1. Divulgar sin autorización información institucional confidencial
2. Haber sido sancionado por dos ocasiones por el cometimiento de faltas leves dentro del mismo año calendario.
3. El sustraer información confidencial y restringida, mediante cualquier dispositivo de almacenamiento, temporal, físico magnético, electrónico o de cualquier otra naturaleza; de cualquier departamento sin la autorización correspondiente.

Destitución. - Se impondrá la máxima sanción de destitución, a más de los casos señalados en el Reglamento Interno de administración del Talento Humano del Consejo Nacional para la Igualdad Intergeneracional, las siguientes:

1. Eliminar o modificar deliberadamente la información almacenada en los registros institucionales (nube o el sistema de información que haga sus veces)
2. Haber sido sancionado por dos ocasiones con suspensión temporal de funciones sin goce de remuneración dentro de un mismo año calendario.

9. PROHIBICIONES.

- Queda prohibido al personal que tiene a su cargo un equipo de cómputo, prestarlo a personas ajenas a la institución sin la debida autorización, pues éste será directamente responsable del mal uso que se otorgué a dicho equipo o de la información que sea sustraída del mismo.
- El sustraer información confidencial y restringida, mediante cualquier dispositivo de almacenamiento, temporal, físico magnético, electrónico o de cualquier otra naturaleza; de cualquier departamento sin la autorización correspondiente.
- Abrir páginas de Internet restringidas y hacer mal uso de la red.
- Uso de software no autorizado.
- Provocar daños intencionales al equipo de cómputo, será grave y se hará la reposición del componente o equipo de cómputo según sea el caso.
- Afectar el espacio laboral por el uso fuerte del volumen de audio en el equipo de cómputo u otros dispositivos electrónicos.

10. DIFUSIÓN.

La difusión de la presente política estará a cargo de la Unidad de Planificación y Gestión Estratégica y la Unidad de Comunicación a través de los responsables encargados de la Información.

CONTROL E HISTORIAL DE CAMBIOS

Versión	Descripción del cambio	Fecha de Actualización
1.0	Emisión de Políticas de Seguridad	*12/08/2019*
2.0	Actualización	*13/08/2019*
3.0	Actualización	*18/062021*
4.0	Actualización	*14/03/2024*
5.0	Actualización	*01/08/2025*

FIRMAS DE REVISIÓN Y APROBACIÓN

	Nombre / Cargo	Firma	Fecha
Elaborado por:	Ramiro Delgado Oficial de Seguridad de la Información	Firmado electrónicamente por: RAMIRO EDUARDO DELGADO NAVARRETE Validar únicamente con FirmaEC	01/08/2025
Revisado y Aprobado por:	Arón Sánchez Secretario Técnico	Firmado electrónicamente por: ARON JOEL SANCHEZ ESCALANTE Validar únicamente con FirmaEC	01/08/2025

Declaración de confidencialidad.

Los equipos técnicos metodológicos aquí firmantes se comprometen a tratar de manera estrictamente confidencial todos los documentos y la información aquí evidenciada; así mismo a no ser divulgada a terceros externos al Consejo Nacional para la Igualdad Intergeneracional, sin una autorización por escrito de la Máxima Autoridad y de la Dirección de Planificación y Gestión Estratégica.