POLÍTICA DE USO DE DISPOSITIVOS PROPIOS

1. INTRODUCCION

Esta política regula el uso de equipos y dispositivos de propiedad de las y los servidores/as, funcionario/as, trabajador/as, practicantes o terceras personas que trabajen o brinden servicios en la Institución, para tener acceso a recursos, tales como correos electrónicos y archivos en equipos informáticos, así como datos y aplicaciones personales.

Mediante la presente política se establece el marco referencial con lineamientos generales en la utilización de dispositivos observando la protección de la información.

2. ANTECEDENTES

El Consejo Nacional para la Igualdad de Género gestiona información, la cual debe ser manejada y respaldada de forma segura y oportuna.

El Esquema Gubernamental de Seguridad de la Información EGSI establece un conjunto de directrices prioritarias para Gestión de la Seguridad de la información,

3. JUSTIFICACION

El establecimiento de políticas de uso de dispositivos propios es fundamental para determinar los parámetros de utilización por el personal del Consejo Nacional para la Igualdad de Género y usuarios/as externos/as autorizados para el uso de servicios tecnológicos institucionales.

El EGSI establece: "Las entidades de la Administración Pública Central, Dependiente e institucional que generan, utilizan, procesan, comparten y almacenan información en medio electrónico o escrito, clasificada como pública, confidencial, reservada y no reservada, deberán aplicar el Esquema Gubernamental de Seguridad de la Información para definir los procesos, procedimientos y tecnologías a fin de garantizar la confidencialidad, integridad y disponibilidad de esa información, en los medios y el tiempo que su legitimidad lo requiera".

4. OBJETIVO

Definir lineamientos para el uso de dispositivos propios de los servidores/as, trabajadores/a y terceras personas en el Consejo Nacional para la Igualdad de Género.

5. ALCANCE

Esta política se aplica a todos los dispositivos personales autorizados para conectarse a la red institucional, sea de forma inalámbrica o cableada; y, también para aquellos utilizados durante las jornadas de Teletrabajo autorizado por la Entidad.

Esta política se aplica a todo el personal que trabaja en la Institución, independientemente del tipo de régimen laboral en que presten sus servicios.

La política debe ser revisada y/o actualizada anualmente, o cuando se considere necesario por la Unidad de Tecnologías de Información y Comunicación.

6. RESPONSABILIDADES

La Unidad de Tecnologías de Información y Comunicación proporciona los servicios tecnológicos y los lineamientos para el manejo seguro de la información y se encargará de revisar y gestionar la aprobación de los permisos de accesos especiales a la red e Internet.

Cada usuario/a tiene la responsabilidad de cumplir con esta política.

Las autoridades institucionales son responsables de cumplir y controlar el cumplimiento de esta política por parte de los usuarios/as bajo su responsabilidad.

7. POLITICAS DE USO DE DISPOSITIVOS PROPIOS

Las políticas se aplican para los dispositivos propios que contengan información institucional, dentro o fuera de las instalaciones del Consejo.

La solicitud de uso de dispositivos propios, debe ser presentada ante la Unidad de Tecnologías de la Información y comunicación, adjuntando el respectivo formulario de SOLICITUD DE ACCESOS ESPECIALES A LA RED E INTERNET, con la debida justificación e indicando el tiempo requerido

7.1. Política

Los dispositivos propios deben ser registrados antes de su ingreso a la institución, para el efecto el/a propietario/a del equipo, solicitará su registro en la guardianía al ingreso del mismo.

Para acceder a la red institucional de los dispositivos propios, las y los servidores/as requerirán autorización previa de su Jefe/a inmediato/a; para lo cual es indispensable llenar un formulario especificando las características del dispositivo, la justificación

del requerimiento de acceso a la red institucional y la autorización de su jefe/a inmediato/a.

Los datos que se almacenan transfieren o procesan en los dispositivos propios siguen perteneciendo a la Institución, la cual tiene el derecho de controlar, aunque no sea propietaria del dispositivo.

7.2. Uso de dispositivos propios

7.2.1. Utilización de equipos

La unidad de Tecnologías de Información y Comunicación debe mantener un registro actualizado de los funcionarios, equipos, permisos y fechas en las que se permite su utilización.

7.2.2. Dispositivos contemplados:

a) Laptops
b) Computadores de escritorio
c) Teléfonos inteligentes
d) Tabletas, etc.

7.2.3. Uso aceptable

A los y las servidoras que tienen autorizado el uso de los Dispositivos propios se recomienda que:

a) Los dispositivos deben estar protegidos contra códigos maliciosos y virus.
b) La información sensible de la Institución que se encuentre en los dispositivos, debe estar encriptada o con clave de acceso.
c) Los dispositivos deben estar configurados con usuario, contraseña y bloqueo automático; lo cual es responsabilidad del/a propietario/a
d) Cuando se utiliza un dispositivo fuera de la Institución, el/a propietario/a debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
e) Evitar conectarse a redes inalámbricas desconocidas.
f) Los sistemas operativos y las aplicaciones de los dispositivos deben estar actualizados, lo cual es responsabilidad del/a propietario/a del dispositivo.

7.3. Prohibiciones

a) Permitir el acceso a la información de la Institución a cualquier persona que no sea el propietario/a del dispositivo o pertenezca a la Institución.
b) Compartir o almacenar claves de los sistemas del Consejo.

7.4. Reembolso

El Consejo Nacional para la Igualdad de Género no pagará a las y los servidores propietarios/as de los dispositivos, ningún valor por el uso, por robo o daño de los mismos, aunque estén siendo usados con fines laborales.

7.5. Propiedad intelectual

La información almacenada en los dispositivos propios durante las jornadas de Teletrabajo, son de propiedad intelectual del CNIG, por lo que sus propietarios/as se comprometen a entregar la citada información de manera digital, dividida por carpetas, asunto y fechas de creación, para su adecuado registro en la Dirección o Unidad a la que pertenece.

7.6. Derechos Especiales.

La Institución tiene el derecho de ver, editar y borrar todos los datos relacionados con ella, que se encuentran almacenados, transferidos o procesados en los dispositivos propios de las y los servidores de la institución, ya que la información relacionada con el CNIG, es propiedad intelectual de la Entidad.

La unidad de Tecnologías de Información y Comunicación está autorizada a configurar cualquier dispositivo propio de conformidad con la presente política y está autorizada a controlar el uso de dispositivos a través de herramientas tecnológicas institucionales.

El Consejo Nacional para la Igualdad de Género tiene el derecho de realizar el borrado completo de todos los datos del dispositivo, si considera que es necesario para la protección de la información de la Institución, sin el consentimiento del/a propietario/a del dispositivo.

7.7. Guía de Conducta - Violaciones de Seguridad

Todas las violaciones de seguridad relacionadas con los dispositivos propios deben ser reportadas inmediatamente a la Oficial de Seguridad de la Información.

8. COMPROMISO DE TODO EL PERSONAL DE LA INSTITUCION

En personal de la Institución acepta esta Política de Uso de Dispositivos Propios, como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la Institución.

El personal de la Institución demuestra su compromiso a través de:

a) La aceptación de las Políticas de Uso de Dispositivos Propios contenidas en este documento.
b) El cumplimiento de las politices de Uso de Dispositivos Propios.

9. IDENTIFICACION DE RIESGOS

En cumplimiento al Acuerdo No. 166 del Esquema Gubernamental de Seguridad de la Información - EGSI, en el Artículo 7 "las entidades realizarán una evaluación de riesgos y diseñarán e implementarán el plan de manejo de riesgos, en base a la norma INEN ISO/IEC:27005 "Gestión del Riesgo en la Seguridad de la Información".

Elaborado Por
Rocío Balarezo B.
Responsable de Planificación y GE
1 abril 2020