POLÍTICA DE CONTROL DE ACCESOS A SERVICIOS TECNOLÓGICOS

1. INTRODUCCION

Las políticas de control de accesos a servicios informáticos, definen los niveles de autorización para su acceso, además de explicar el uso apropiado de los mismos y las medidas para optimizar su utilización.

2. ANTECEDENTES

El Consejo Nacional para la Igualdad de Género presta servicios tecnológicos al personal de la Institución, estos son administrados por parte de la Unidad de Tecnologías de Información y Comunicación, misma que se encuentra alineada a las políticas de control, regulación y optimización de los recursos tecnológicos vigentes, lo cual permite la correcta gestión, de acuerdo a las necesidades institucionales.

Se ha tomado el Esquema Gubernamental de Seguridad de la Información como guía de referencia en temas de seguridad informática.

Los principales servicios tecnológicos entregados actualmente son:

a) Internet
b) Correo institucional
c) Aplicativos Gubernamentales
d) Aplicativos provistos por terceros
e) Telefonía IP

3. NORMATIVA

a) Acuerdo Ministerial No. 025-2019, las instituciones tienen un plazo de 12 meses para implementar o actualizar el EGSI versión 2.0
b) Acuerdo Ministerial N°0166, del 25 de septiembre de 2013, se dispone a las entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.
c) Acuerdo Ministerial N° 1606, del 17 de mayo de 2016, en su artículo 12 y 13 se dispone eliminar los "Comités de Gestión de Gestión de Seguridad de la Información"
d) Acuerdo Ministerial No. 025-2019, del 20 de septiembre de 2019, se expide el Esquema Gubernamental de Seguridad de la Información -EGSI- (Versión 2.0)

4. JUSTIFICACION

Las políticas de control de accesos a servicios tecnológicos institucionales permitirán utilizar los recursos de forma efectiva, disminuyendo el riesgo y asegurando la entrega eficiente de los recursos informáticos tanto a los/las servidores/as, funcionarios/as, trabajadores/as, practicantes y cualquier persona que tenga una relación con el Consejo Nacional para la Igualdad de Género.

El Esquema Gubernamental de Seguridad de la Información en el punto 7. CONTROL DE ACCESO, 3.2. Responsable de los activos, establece con (*) los aspectos que se deben considerar como primordiales de cumplimiento para una buena gestión de control de accesos.

5. OBJETIVOS

a) Definir y reglamentar las normas generales de control de acceso a los servicios informáticos, mejorando la seguridad de la información en la Institución.
b) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de estaciones de trabajo.
c) Establecer los niveles de acceso apropiados a la información institucional, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema y usuario/a.

6. ALCANCE

Las políticas de control de accesos aplican a los/las servidores/as, funcionarios/as, trabajadores/as, practicantes y cualquier persona que trabaja en el Consejo Nacional para la Igualdad de Género y utiliza servicios tecnológicos provistos por la misma.

7. DEFINICIONES

a) **Acceso a la información**: El acceso a la información es el derecho que tiene toda persona de buscar, recibir y difundir información en poder del Estado.
b) **Derechos de accesos**: Conjunto de permisos dados a un/a usuario/a, de acuerdo con sus funciones, para acceder a un determinado recurso.
c) **Restringir el acceso**: Delimitar el acceso de los/as funcionarios/as, servidores/as públicos y terceras partes a determinados recursos.
d) **Sanción**: Puede ser definida como una consecuencia por el incumplimiento de una obligación.
e) **Sistema informático**: uno o más computadores, software asociado, periféricos, terminales, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información y/o transferencia de información.
f) **Usuario/a**: persona que utiliza un sistema informático y recibe un servicio, tales como: correo electrónico o red de conectividad proporcionado o administrado por el CNIG.
g) **Documento electrónico**: toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.
h) **Documento público**: aquellos documentos que no son ni reservados ni secretos y cuyo conocimiento no está circunscrito.
i) **Documento electrónico institucional**: Documento electrónico creado, enviado, comunicado o recibido, por los/as usuarios/as del CNIG.
j) **Activos de información**: Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la Institución cualquiera sea el

formato que la contenga y los equipos y sistemas que la soporten. Por ejemplo: dispositivos móviles, tarjetas de accesos, software, equipamiento computacional.

k) **Riesgo**: Es la contingencia de un daño a un activo de información. A su vez, contingencia significa que el daño puede materializarse en cualquier momento o no suceder nunca.
l) **Amenaza**: Causa potencial de un incidente no deseado por el cual puede resultar dañado un sistema.
m) **Gestión del riesgo**: Proceso definido para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un aseguramiento razonable.
n) **Evaluación del riesgo**: Comparar los niveles de riesgo encontrados contra los criterios de riesgo preestablecidos.
o) **Seguridad de la Información**: es el proceso encargado de asegurar que los recursos de un sistema de información sean utilizados de manera adecuada y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización, preservando la Integridad, Confidencialidad y Disponibilidad.
p) **Proceso**: Conjunto de actividades o eventos que se realizan o suceden (alternativa o simultáneamente) con un fin determinado.
q) **Incidente de Seguridad**: Se define incidente como cualquier evento o situación que comprometa de manera importante la disponibilidad, integridad y confidencialidad de la información. En general, es una violación de una política, estándar o procedimiento de seguridad, que no permite prestar un servicio computacional.

   Como ejemplos de incidentes de seguridad podemos enumerar:
   - Acceso no autorizado.
   - Robo de contraseñas.
   - Robo de información.
   - Denegación de servicio.
   - Robo y extravío de un medio de procesamiento de la información.

r) **Confidencialidad**: Es la propiedad de un documento o mensaje, que está autorizado para ser leído o entendido, únicamente, por algunas personas o entidades.
s) **Integridad**: Se entiende por la corrección y completitud de los datos o de la información manejada.
t) **Disponibilidad**: es la certeza de que sólo los/as usuarios/as autorizados/as tienen acceso a la información y a los activos asociados cuando es requerido.
u) **Medios de procesamiento de información**: Los dispositivos internos y/o externos que tengan la capacidad de procesar información, almacenarla y que se encuentren disponibles para ser manipulados por el usuario.
   Como ejemplos de medios de procesamiento de información, podemos enumerar:
      - Servidores de aplicaciones: de correo, de impresión, aplicaciones web.
      - Servidores de Almacenamientos.
      - Computadores personales.

- Discos duros externos.
- Memorias externas
- Teléfonos móviles.
-

v) **Operaciones informáticas**: Todas las actividades que estén relacionadas con un sistema informático y/o procesamiento de la información.
Como ejemplos de operaciones informáticas podemos enumerar:

- Configuración de servidores y estaciones de trabajo.
- Configuración de equipos de comunicación que conectan a los/as usuarios/as a la red.
- Creación y/o retiro de acceso a los medios de procesamiento de información.
- Mantención de base de datos de los sistemas.
- Respaldo de la información de servidores y estaciones de trabajo.

w) **Terceras partes**: Persona u organismo reconocido como independiente y que no forma parte de la institución, se entenderá como terceras partes a:

- Proveedores de servicios y de red.
- Proveedores de productos de software y servicios de información.
- Outsourcing de instalaciones y operaciones.
- Servicios de asesoría de seguridad.
- Auditores externos.

x) **Estación de Trabajo**: En una red de computadores, una estación de trabajo es un computador que facilita a los/as usuarios/as el acceso a los servidores y periféricos de la red.

y) **Programa malicioso**: Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora.

z) **Virus**: Es un programa que, al ejecutarse, se propaga infectando otros softwares ejecutables dentro de la misma computadora.

aa) **Malware**: El término malware es muy utilizado para referirse a una variedad de software hostil, intrusivo o molesto. El término malware incluye virus gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo, crimeware y otros softwares maliciosos e indeseables.

bb) SPAM: Se llama spam al correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo, habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor). La acción de enviar dichos mensajes se denomina spamming.

7.- PRINCIPIOS DE SEGURIDAD

a) **Confidencialidad**: La información solo podrá ser accedida, modificada y/o eliminada por quienes estén autorizados/as para ello.

b) **Disponibilidad**: La información deberá estar accesible siempre que se requiera.

c) **Integridad**: La información deberá preservar su veracidad y fidelidad a la fuente, independientemente del lugar y de la forma de almacenamiento y transmisión.

8. POLITICAS DE CONTROL DE ACCESO A SERVICIOS TECNOLOGICOS

El acceso a la red de la Entidad debe ser otorgado solo a usuarios/as autorizados/as, previa definición, verificación y control de los perfiles y roles, otorgados por el/a jefe/a inmediata en coordinación con la Unidad de Talento Humano, cuya implementación es responsabilidad de TIC´s.

La información generada o almacenada en medios institucionales es de propiedad del Consejo Nacional para la Igualdad de Género y debe ser utilizada exclusivamente para las tareas propias de las funciones desarrolladas en la Institución.

Para acceder a los servicios tecnológicos la persona debe tener relación laboral con la Institución, o contar con la autorización escrita de un/a servidor/a del nivel jerárquico superior.

8.1. GESTION DE ACCESOS

8.1.1. Solicitud de acceso a los servicios tecnológicos

Desde la Unidad de Administración de Talento Humano, se envía una solicitud a la Unidad de Tecnologías de la información y Comunicación para habilitar usuarios/as y claves en los sistemas informáticos utilizados en la Institución, de acuerdo al cargo y funciones asignadas al servidor/a, funcionario/a, trabajador/a, practicante o cualquier persona que ingrese a trabajar en la Institución.

En cuanto al uso de los sistemas institucionales la solicitud debe ser remitida por el/a Jefe/a Inmediato/a informando los perfiles que utilizará.

Dentro de esta solicitud se encuentra especificada la información básica del/a usuario/a.

8.1.2. Creación de usuarios/as de servicios tecnológicos

Nombre de usuario/a: El nombre de usuario/a de servicios tecnológicos está generado de la siguiente forma:

Primera letra del primer nombre, seguido del primer apellido y luego @igualdadgenero.gob.ec

En caso de existir homónimos en los nombres, el usuario se creará con el segundo nombre del/a usuario/a solicitante o en su defecto se analizará la estructura para evitar usuarios/as repetidos.

8.1.3. Asignación de Permisos

Los permisos concedidos son asignados de manera personal e intransferible. La Unidad de Tecnologías de Información y Comunicación asigna los servicios tecnológicos básicos de uso general para todos los/las servidores/as, funcionarios/as, trabajadores/as, practicantes y cualquier persona del Consejo.

Para el caso de requerir servicios tecnológicos especiales, se debe proceder a solicitar a la el Jefe/a inmediato/a, realice el requerimiento a la Unidad de Tecnologías de la Información.

8.1.4. Perfiles de Servicios Tecnológicos

a) Acceso Administrador: Este perfil permite la creación, modificación o eliminación de usuarios.
b) Acceso estándar: Este perfil permite acceder únicamente a los permisos asignados a su usuario y hacer uso de las funcionalidades básicas que ofrece el servicio tecnológico.

8.1.5. Asignación de perfiles a los/as usuarios/as de la Institución

Se asignarán los permisos de acuerdo a los siguientes perfiles:

a) Perfil básico, este perfil permite acceder a las aplicaciones básicas
b) Perfil avanzado, este perfil permite acceder a otro tipo de aplicaciones de conformidad a las autorizaciones otorgadas por el/a jefe/a inmediato/a

Todo usuario creado debe tener incluido el número de cédula y nombre en el sistema, aplicación, etc. En el caso de utilizar usuarios genéricos se debe justificar e ingresar la identificación y el nombre del usuario/a responsable.

8.2. RESPONSABILIDADES DEL/A USUARIO/A

Todos/as los/as usuarios/as del Consejo Nacional para la Igualdad de Género que ingresan a la Institución deben utilizar los servicios tecnológicos provistos por la Institución.

Al momento de ingresar a los sistemas, aplicaciones institucionales, cada usuario/a está aceptando la responsabilidad y confidencialidad del uso y manejo de los servicios e información institucional.

Los/las servidores/as, funcionarios/as, trabajadores/as, practicantes y cualquier persona de la Institución son responsables de los usuarios, contraseñas y servicios tecnológicos asignados.

Si un servidor/a, funcionario/a, trabajador/a, practicante y cualquier persona de la Institución debiera cambiar de equipo, ya sea por reemplazo del mismo o por traslado a otra unidad, la persona deberá solicitar apoyo tecnológico a TIC´s.

8.3. CONTROL DE ACCESO A LA RED

Las conexiones no seguras a los servicios de red pueden afectar a toda la Institución, por lo tanto, se debe controlar el acceso a los servicios de red tanto internos como externos, para garantizar que los/as usuarios/as que tengan acceso a las redes y a sus servicios no comprometan la seguridad de los mismos.

Las reglas de acceso a la red a través de los puertos estarán basadas en la premisa: "todo está restringido, a menos que este expresamente permitido".

8.3.1. Utilización de los servicios de red

La Unidad de Tecnologías de la Información y Comunicación, deben desarrollar procedimientos para la activación y desactivación de permisos de acceso a las redes y servicios, los cuales comprenderán principalmente:

a) Controlar el acceso a los servicios de red tanto internos como externos.
b) Identificar las redes y servicios de red a los cuales se permite el acceso.
c) Autorización de acceso entre redes.
d) Establecer controles de administración para proteger el acceso y servicios de red.

8.3.2. Autenticación de usuarios para conexiones externas

La unidad de Tecnologías de la Información y Comunicación contempla como servicios de conexiones externas SSL (Capa de conexión segura), VPN (Redes privadas virtuales) y primarios para aquellas personas del Consejo que requieran conexión remota a la red de datos institucional.

8.3.3. Identificación de equipos en la Red

La unidad de Tecnologías de la Información y Comunicación, identificará y controlará los equipos conectados a su red, mediante el uso de controladores de dominio, estandarización de nombres de equipos o dispositivos, asignación de IP y portales cautivos en el caso de conexiones inalámbricas.

8.3.4. Protección de los puertos de configuración y diagnóstico remoto

Los puertos que permita realizar mantenimiento y soporte remoto a los equipos de red, servidores y equipos de usuario final, estarán restringidos a los administradores de red.

Para el caso del diagnóstico remoto, los usuarios finales deben permitir tomar el control remoto de sus equipos por parte de Tecnologías de la Información y Comunicación, teniendo en cuenta, no mantener archivos con información sensible a la vista y no desatender el equipo mientras que se tenga el control del equipo por un tercero.

8.3.5. Separación de redes

La unidad de Tecnologías de la información y Comunicación utilizará dispositivos de seguridad perimetral, para controlar el acceso de una red a otra y proteger la información más crítica o vulnerable.

8.3.6. Control de conexión de las redes

a) La capacidad de descarga de cada usuario final debe ser limitada y controlada.
b) La seguridad para las conexiones WiFi será WPA2 o superior.
c) Dentro de la red de datos institucional se restringirá el acceso a:
    - Mensajería Instantánea y redes sociales.
    - La telefonía a través de internet.
    - Correo electrónico comercial no autorizado.
    - Descarga de archivos de sitio peer to peer o repositorios no autorizados.
    - Conexiones a sitios de streaming no autorizado.
    - Acceso a sitios de pornografía.
    - Violencia contra niños, niñas y adolescentes.

- Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de la misma.

8.3.7. Control de enrutamiento de red

El acceso a redes desde y hacia afuera de la Institución cumplirá con los lineamientos del Control de acceso a la red y adicionalmente se utilizarán métodos de autenticación de protocolo de enrizamiento, translación de direcciones IP y listas de control de acceso.

8.3.8. Uso de equipos de cómputo y dispositivos de almacenamiento móviles

El uso de equipos de cómputo (laptops) institucionales y dispositivos de almacenamiento móviles, deberán contemplar las siguientes directrices:

- Uso de usuario y contraseña para acceso al mismo.
- Cifrado de la información.
- Uso de software antivirus provisto por la Unidad de Tecnología.
- Uso de software licenciado.
- Realización de copias de seguridad periódicas.
- Uso de mecanismos de seguridad que protejan la información en caso de pérdida o hurto de los dispositivos.
- Permanecer siempre cerca del dispositivo
- No dejar desatendidos los equipos
- No llamar la atención, acerca de portar equipos móviles
- No identificar el dispositivo con distintivos de la Institución
- No colocar datos de contacto técnico en el dispositivo
- Mantener apagado el Bluetooth o cualquier otra tecnología inalámbrica que exista.

8.4. CONTROL DE ACCESO AL SISTEMA OPERATIVO

8.4.1. Registro de inicio seguro

El acceso a los sistemas operativos estará protegido, mediante un inicio seguro de sesión, que contemplará las siguientes condiciones:

a) No mostrar información de sistema, hasta que el proceso de inicio se haya completado.
b) No suministrar mensajes de ayuda, durante el proceso de autenticación.
c) Validar los datos de acceso, una vez que se han diligenciado todos los datos de entrada.
d) Limitar el número de intentos fallidos de conexión auditando los intentos no exitosos
e) No mostrar las contraseñas digitadas.
f) Las contraseñas deben almacenarse en los sistemas en forma encriptada.
g) No transmitir la contraseña en texto claro.

8.4.2. Gestión de contraseñas

a) La generación de contraseña del usuario debe cumplir una complejidad media y alta que consiste en la utilización de letras mayúsculas, minúsculas, con caracteres especiales.
b) La asignación y cambio de contraseñas se deberá controlar a través de un proceso formal de gestión de contraseñas, a cargo de la unidad de TIC´S.
c) La contraseña que se establece como valor inicial es la cédula del/a usuario/a y esta deberá ser cambiada la primera vez que ingrese al servicio. Cada usuario/a deberá cambiar su clave cada 60 días; los sistemas deberán enviar una notificación de cambio para realizar este proceso.
d) Las contraseñas no deben estar escritas y expuestas a que otras personas las vean.
e) Aplicar una política y procedimientos para controlar el cambio de contraseña del usuario de la Unidad de tecnología, en rangos de tiempo y complejidad.
f) Forzar el cambio de contraseña en el primer registro de acceso o inicio de sesión.
g) Generar un procedimiento formal para la administración y custodia de las contraseñas de acceso de administración e información crítica de la Institución
h) Documentar el control de acceso para los/as usuarios/as temporales.
i) Almacenar y transmitir las contraseñas en formatos protegidos (encriptados o codificados.
j) La asignación de contraseñas se deberá controlar a través de un proceso formal de gestión a cargo de la Unidad TIC´s. Las recomendaciones son:

- No escribirlas en papeles de fácil acceso, ni en archivos sin cifrar.
- No habilitar la opción —recordar clave en este equipo“, que ofrecen los programas
- No enviarla por correo electrónico
- Nunca guardar las contraseñas, en ningún tipo de papel, agenda, etc.
- Las contraseñas se deben mantener confidenciales en todo momento.
- No compartir las contraseñas, con otros/as usuarios/as.
- Cambiar la contraseña si piensa que alguien más la conoce y si ha tratado de dar mal uso de ella.
- Selecciona contraseñas que no sean fáciles de adivinar.
- Nunca grabe su contraseña en una tecla de función o en un comando de caracteres pre- definido.
- Cambiar las contraseñas regularmente.
- No utilizar la opción de almacenar contraseñas en Internet.
- No utilizar contraseña con números telefónicos, nombre de familia etc.
- No utilizar contraseña con variables (soporte1, soporte2, soporte3 etc.)

8.4.3. Uso de usuarios del Sistema

- Se establecerá una política a nivel del controlador de dominio, que no permita la instalación de software y cambios de configuración del sistema. Ningún usuario final, deberá tener privilegios de usuario administrador.
- Después de diez (10) minutos de inactividad del sistema, se considerará tiempo muerto y se bloqueará la sesión, sin cerrar las sesiones de aplicación o de red (ítem 7.20. Tiempo de inactividad de la sesión - EGSI).

- Los/as usuarios/as procederán a bloquear sus sesiones, cuando deban abandonar temporalmente su puesto de trabajo.
- Las estaciones de trabajo deberán quedar apagadas al finalizar la jornada laboral o cuando una ausencia temporal supere dos (2) horas.

8.5. CONTROL DE ACCESO A LAS APLICACIONES E INFORMACION

El control de acceso a la información, se realizará a través de roles que administren los privilegios de los usuarios de cada sistema, aplicativo o servicio, mismos que deben constar en un registro incluido en carpetas compartidas con acceso solo a personal de tecnología autorizado.

El control de acceso a información física o digital, se realizará teniendo en cuenta los niveles de clasificación y el manejo de intercambio de información determinado por las autoridades.

La Unidad de Tecnologías de Información y Comunicación, identificará según los niveles de clasificación de información, cuales sistemas considera sensibles y que deberían gestionarse desde ambientes tecnológicos aislados e independientes. Al aislar estos sistemas se debe prever el intercambio seguro de información, con otras fuentes de datos, ya que no se permite duplicar información en otros sistemas, siguiendo las directrices de fuentes únicas de datos.

A las personas que se desvinculan de la Institución, se desactivará su acceso, una vez que la Unidad de Tecnologías de Información y Comunicación, reciba el listado respectivo por parte de la Unidad de Administración de Talento Humano.

8.6. MONITOREO DE SERVICIOS INFORMATICOS INSTITUCIONALES

La Unidad de Tecnologías de Información y Comunicación monitoreará los servicios tecnológicos entregados con el fin de evitar anomalías que interfieran en la alta disponibilidad de los mismos.

8.7. DEPURACION DE LOS ACCESOS EXISTENTES

- La Unidad de Tecnologías de Información y Comunicación realizará una depuración de los accesos otorgados a los/las servidores/as, funcionarios/as, trabajadores/as, practicantes y cualquier persona que tenga una relación con el Consejo Nacional para la Igualdad de Género.
- Se deberá realizar las depuraciones respectivas de los accesos de los usuarios, determinando un período máximo de 60 días; en casos de presentar cambios estructurales, esta gestión deberá hacerse inmediatamente que se ejecute el cambio organizacional.
- Considerando la optimización del espacio de almacenamiento y la memoria limitada, tanto en los servidores de datos de la Institución como en las computadoras asignadas a los usuarios/as, es indispensable que las/os usuarios realicen una revisión continua de sus archivos y depuren la información no relevante.

8.8. CASOS ESPECIALES

En ciertas ocasiones o casos especiales, esta política no se podrá aplicar en su totalidad, estos casos deberán ser analizados por la unidad de Tecnologías de la Información y Comunicación, la que evaluará la pertinencia y los riesgos asociados y aceptará o negará la excepción.

Los casos especiales son los que no se encuentren contemplados en esta política y deberán ser informados de manera escrita al Oficial de Seguridad de la Información para su registro y evaluación.

Elaborado Por:
Rocío Balarezo B.
Versión 1
31 de marzo de 2020