POLÍTICA DE CONTROL DE ACCESOS

DIRECCIÓN DE INFORMÁTICA Y ESTADÍSTICA

DEPARTAMENTO DE ORGANIZACIÓN Y MÉTODOS
DIRECCIÓN DE GESTIÓN Y CONTROL INTERNO

FECHA DE EMISIÓN	Mayo 2024
CÓDIGO	POL-DIE-01-2024
VERSIÓN	04

DIRECCIÓN DE INFORMÁTICA Y ESTADÍSTICA
POLÍTICA DE CONTROL DE ACCESOS
VERSIÓN 04: POL-DIE-01-2024

Elaborado por:	
Ing. Otto Fernando Hernández Barillas Profesional de Organización y Métodos	Ing. Otto Fernando Hernández Barillas Profesional de Organización y Métodos Dirección de Gestión y Control Interno Sede del RENAP Guatemala, Guat...

Revisado por:	
Lic. Ricardo Bernabé Bercián Ramírez Jefe de Organización y Métodos	Lic. Ricardo Bernabé Bercián Ramírez Jefe de Organización y Métodos Dirección de Gestión y Control Interno Sede del RENAP, Guatemala, Guatemala
Licda. Mónica Reneé Recinos Casanova Director de Gestión y Control Interno	Licda. Mónica Reneé Recinos Casanova Director de Gestión y Control Interno Dirección de Gestión y Control Interno Sede del RENAP, Guatemala, Guatemala

Validado por:	
Ing. Edwin Alexander Román Camó Jefe de Seguridad Informática	MGSI. Edwin Alexander Román Camó Jefe de Seguridad Informática Dirección de Informática y Estadística Sede del RENAP Guatemala, Guatemala
Lic. Juan Pablo Illescas De la Cruz Subdirector de Servicios Críticos	Lic. Juan Pablo Illescas de la Cruz Subdirector de Servicios Críticos Dirección de Informática y Estadística Sede del RENAP Guatemala, Guatemala
Ing. José Daniel Girón Miranda Director de Informática y Estadística	Ing. José Daniel Girón Miranda Director de Informática y Estadística Dirección de Informática y Estadística Sede del RENAP Guatemala, Guatemala

Aprobado por:	
Dr. Rodolfo Estuardo Arriaga Herrera Director Ejecutivo	Dr. Rodolfo Estuardo Arriaga Herrera Director Ejecutivo Registro Nacional de las Personas -RENAP- Guatemala, Guatemala

REGISTRO NACIONAL DE LAS PERSONAS -RENAP-
GUATEMALA, C.A.

ACUERDO DE DIRECCIÓN EJECUTIVA NÚMERO DE-334-2024
EL DIRECTOR EJECUTIVO DEL REGISTRO NACIONAL DE LAS PERSONAS -RENAP-

CONSIDERANDO:

Que de conformidad con la literal a) del artículo 134 de la Constitución Política de la República de Guatemala, las entidades autónomas actúan por delegación del Estado, y tienen como una de las obligaciones el coordinar su política, con la política general del Estado y, en su caso, con la especial del Ramo a que correspondan; y de conformidad con lo regulado en los artículos 1 y 8 del Decreto número 90-2005 del Congreso de la República de Guatemala, Ley del Registro Nacional de las Personas, se crea el Registro Nacional de las Personas, como una entidad autónoma, de derecho público, con personalidad jurídica, patrimonio propio y plena capacidad para adquirir derechos y contraer obligaciones; son órganos del Registro: a) Directorio; b) Director Ejecutivo; c) Consejo Consultivo; d) Oficinas Ejecutoras; e) Direcciones Administrativas.

CONSIDERANDO:

Que de conformidad con los artículos 19, 20 literales a) y m) y 42 del Decreto número 90-2005 del Congreso de la República de Guatemala, Ley del Registro Nacional de las Personas, el Director Ejecutivo es el superior jerárquico administrativo, quien ejerce la representación legal y es el encargado de dirigir y velar por el funcionamiento normal e idóneo de la entidad; son funciones del Director Ejecutivo, cumplir y velar porque se cumplan los objetivos de la Institución, así como las leyes y reglamentos; y todas aquellas que sean necesarias para que la Institución alcance plenamente sus objetivos; asimismo, la Dirección de Informática y Estadística es el ente encargado de dirigir las actividades relacionadas con el almacenamiento y procesamiento de los datos que se originen en el Registro Central de las Personas, en relación a su estado civil, capacidad civil y demás datos de identificación. Formula los planes y programas de la institución en la materia de su competencia, informa sobre el cumplimiento de las metas institucionales programadas y elabora las estadísticas pertinentes.

CONSIDERANDO:

Que de conformidad con lo establecido en los artículos 52, 55 y 88 del Acuerdo de Directorio número 22-2023 del Registro Nacional de las Personas, Reglamento de Organización y Funciones del Registro Nacional de las Personas, la Subdirección de Servicios Críticos es la dependencia encargada de planificar, organizar, dirigir y controlar las actividades relacionadas con la seguridad informática, infraestructura tecnológica y soporte técnico hacia toda la Institución, orientadas a fortalecer los procesos informáticos, tomando como base los objetivos y políticas institucionales; el Departamento de Seguridad Informática es la dependencia encargada de realizar actividades que permitan establecer controles de seguridad informática, por medio de la evaluación, análisis, diseño, implementación y monitoreo de los accesos a los sistemas de información, con el fin de garantizar la disponibilidad y confidencialidad de la información. Asimismo, el Director Ejecutivo aprobará los

Manuales de Normas y Procedimientos y cualquier otro documento técnico administrativo de las dependencias del RENAP.

CONSIDERANDO:

Que la Dirección de Gestión y Control Interno del Registro Nacional de las Personas, solicitó la aprobación de la **"POLÍTICA DE CONTROL DE ACCESOS"**, Versión 04, de la Subdirección de Servicios Críticos, de la Dirección de Informática y Estadística del RENAP, para proveer un documento técnico administrativo de apoyo y orientación que brinde a los usuarios los lineamientos de administración y uso de los accesos proporcionados por la Dirección de Informática y Estadística para asegurar el cumplimiento de los requisitos normativos que estén orientados hacia la seguridad de la información.

POR TANTO:

Con base en lo considerado, normas legales citadas y lo que para el efecto establecen los artículos 134, 153 y 154 de la Constitución Política de la República de Guatemala; 1, 8, 19, 20 literales a) y m), 42, 43 y 46 del Decreto número 90-2005 del Congreso de la República de Guatemala, Ley del Registro Nacional de las Personas; 52, 55, 86, 88 y 90 del Acuerdo de Directorio Número 22-2023, Reglamento de Organización y Funciones del Registro Nacional de las Personas -RENAP-.

ACUERDA:

Artículo 1. APROBAR bajo la estricta responsabilidad de la Dirección de Informática y Estadística, el contenido formulado por la Subdirección de Servicios Críticos de dicha Dirección, dentro del documento denominado **"POLÍTICA DE CONTROL DE ACCESOS"**, Versión 04, de la Subdirección de Servicios Críticos de la Dirección de Informática y Estadística del Registro Nacional de las Personas.

Artículo 2. Se derogan todas las disposiciones anteriores que regulen la materia o que se opongan a la presente Política.

Artículo 3. Se instruye a las Direcciones involucradas, para que una vez se encuentre notificado el presente Acuerdo, se realicen las diligencias necesarias a efecto de hacer posible la ejecución del mismo.

Artículo 4. Notifíquese a todas las Oficinas Ejecutoras, Direcciones Administrativas y Dependencias de Apoyo del Director Ejecutivo del RENAP, por medio de la Secretaría General de la Institución.

Artículo 5. El presente Acuerdo entra en vigencia inmediatamente.

Dado en la ciudad de Guatemala, el veinticinco de junio de dos mil veinticuatro.

DOCTOR RODOLFO ESTUARDO ARRIAGA HERRERA
DIRECTOR EJECUTIVO

Contenido

Elaborado por:	Revisado por:	Revisado por:	Validado por:	Validado por:	Validado por:	Aprobado por:
Departamento de Organización y Métodos	Jefe de Organización y Métodos	Director de Gestión y Control Interno	Jefe de Seguridad Informática	Subdirector de Servicios Críticos	Director de Informática y Estadística	Director Ejecutivo

1. Objetivo

Proveer un documento técnico administrativo que sirva de apoyo y orientación, que brinde a los usuarios los lineamientos de administración y uso de los accesos proporcionados por la Dirección de Informática y Estadística para asegurar el cumplimiento de los requisitos normativos que estén orientados hacia la seguridad de la información.

2. Campo de aplicación

La presente Política es de observancia y aplicación obligatoria para los trabajadores del Registro Nacional de las Personas; asimismo, para quienes presten servicios técnicos o profesionales a la Institución y usuarios externos que tengan acceso a la información ingresada, procesada, almacenada y proporcionada por el RENAP.

3. Base legal

- Constitución Política de la República de Guatemala.
- Decreto número 33-98 del Congreso de la República de Guatemala, Ley de Derecho de Autor y Derechos Conexos.
- Decreto número 89-2002 del Congreso de la República de Guatemala, Ley de Probidad y Responsabilidades de Funcionarios y Empleados Públicos.
- Decreto número 90-2005 del Congreso de la República de Guatemala, Ley del Registro Nacional de las Personas.
- Acuerdo de Directorio número 56-2022 del Registro Nacional de las Personas, Reglamento Interior de Trabajo del Registro Nacional de las Personas -RENAP-.
- Acuerdo de Directorio número 22-2023 del Registro Nacional de las Personas, Reglamento de Organización y Funciones del Registro Nacional de las Personas.

4. Monitoreo y seguimiento

Para garantizar la vigencia y efectividad de esta Política, el Jefe de Seguridad Informática, el Subdirector de Servicios Críticos y el Director de Informática y Estadística deberán solicitar la actualización oportuna para realizar la inclusión de ajustes y modificaciones que se consideren pertinentes.

5. Política de control de accesos

Política de control de accesos

La información es el activo más importante de la Institución, el acceso a los sistemas de información y la red del RENAP están restringidos, salvo que bajo los lineamientos regulados de registro y de derecho de acceso sean autorizados por la dependencia correspondiente, siendo la Dirección de Informática y Estadística la encargada de administrar el control de accesos de los sistemas bajo responsabilidad de la misma.

Elaborado por:	Revisado por:	Revisado por:	Validado por:	Validado por:	Validado por:	Aprobado por:
Departamento de Organización y Métodos	Jefe de Organización y Métodos	Director de Gestión y Control Interno	Jefe de Seguridad Informática	Subdirector de Servicios Críticos	Director de Informática y Estadística	Director Ejecutivo

6. Acceso a redes y servicios de red

6.1. Los accesos serán gestionados bajo el principio de cuentas únicas, personales e intransferibles.

6.2. El acceso a las redes y servicios de la red institucional deberá ser solicitada por medio de la "Boleta Única Todos los Servicios", debidamente autorizada por el jefe inmediato y máxima autoridad de la dependencia a donde pertenezca.

6.3. La solicitud de acceso al Sistema de Registro Civil -SIRECI-, deberá contar con autorización del Registrador Central de las Personas o la persona a quien delegue.

6.4. El Departamento de Desarrollo de Sistemas deberá mantener un listado actualizado de todos los sistemas de información con los que opera la Institución, este deberá incluir a los responsables de la administración de estos.

6.5. El jefe inmediato del trabajador o quien preste servicios técnicos o profesionales a la Institución, deberá notificar por la vía oficial al Departamento de Seguridad Informática de cualquier cambio en las funciones para que pueda reflejarse en sus privilegios de acceso.

6.6. El Departamento de Seguridad Informática será responsable de realizar periódicamente pruebas de intrusión y vulnerabilidades (al menos una vez al año) y del seguimiento de los resultados obtenidos.

6.7. El Departamento de Seguridad Informática será el responsable de resguardar todas las "Boletas Únicas Todos los Servicios" originales.

7. Registro de usuarios

7.1. Para el registro de usuarios, todo trabajador y quien preste servicios técnicos o profesionales a la Institución, deberá completar la "Boleta Única Todos los Servicios", con la autorización del jefe inmediato y máxima autoridad de la dependencia donde pertenezca.

7.2. El Departamento de Seguridad Informática es el único autorizado para crear usuarios y contraseñas en la red del RENAP.

7.3. El Departamento de Seguridad Informática otorgará al usuario el acceso a la red y servicios, toda vez haya sido aprobado en la "Boleta Única Todos los Servicios".

7.4. El Departamento de Seguridad Informática creará la cuenta del usuario y contraseña (inicial) al personal autorizado para el acceso a la red y servicios de la Institución, la contraseña deberá ser modificada por el usuario inmediatamente después de haber sido utilizada por primera vez para ingresar a la red.

7.5. El Departamento de Seguridad Informática será responsable de realizar la depuración periódica de cuentas inactivas. Para el efecto, se inactivan todas aquellas cuentas que permanezcan sin ser utilizadas durante cinco (5) días hábiles consecutivos en el Active Directory[1].

7.6. Para la creación de usuario deberá utilizarse los trece (13) dígitos, correspondientes al Código Único de Identificación -CUI-.

7.7. El Departamento de Seguridad Informática mensualmente notificará por medio de oficio a la Subdirección de Recursos Humanos, un informe con los usuarios que fueron deshabilitados por inactividad para su respectivo seguimiento.

7.8. Todo requerimiento de acceso provisional a la red y servicios de la Institución deberá establecer fecha de caducidad del acceso.

7.9. Auditoría Interna podrá solicitar permisos a sus trabajadores para revisión de bitácoras de los sistemas que posean estos registros, por medio de oficio.

8. Asignación de equipo

8.1. Cada solicitud de asignación o cambio de equipo a un usuario nuevo deberá ser solicitada a la Dirección de Informática y Estadística a través de la "Boleta Única Todos los Servicios", adjuntando la "Tarjeta de Responsabilidad" proporcionada por la Dirección de Presupuesto u "Hoja de Asignación de Bienes" entregada por la Dirección Administrativa (deberá de estar marcado o resaltado el equipo a asignar). En el caso de quienes presten servicios técnicos o profesionales a la Institución, deberán presentar los documentos de la persona responsable del equipo.

8.2. Los trabajadores del RENAP podrán tener asignado un usuario a un equipo de cómputo. Se podrá asignar el usuario a equipos de cómputo adicionales, en los casos siguientes:

- Cubrir turnos (rotación de personal de fin de semana u horario no hábil).
- Cubrir permisos previstos (vacaciones o licencias).
- Cubrir horario de almuerzo (en oficinas donde solo se cuenta con dos personas).
- Cubrir emergencias (accidentes, fallecimiento, enfermedad, entre otros).

Para los casos anteriores se deberán acatar las directrices siguientes:

a) Si el equipo no está en la tarjeta de responsabilidad del trabajador, se deberá entregar junto a la "Boleta Única Todos los Servicios", la "Tarjeta de Responsabilidad" del trabajador a quien cubrirá (con el equipo marcado o resaltado).
b) El tiempo contemplado para realizar la cobertura temporal deberá ser menor a un mes.

[1] Para efectos del documento técnico administrativo, se referirá a la implementación de servicio de directorio en una red distribuida de computadores.

c) El personal ajeno a la Dirección de Informática y Estadística, que por sus funciones requiera administrar un sistema informático que se encuentre alojado en otro equipo que no sea el asignado, deberá requerir el acceso mediante oficio firmado por la máxima autoridad de la dependencia, dirigido a la Dirección de Informática y Estadística, adjuntando la "Boleta Única Todos los Servicios".

9. Derecho de acceso

9.1. Toda solicitud de acceso a los sistemas informáticos del RENAP deberá realizarse por medio de oficio dirigido al departamento correspondiente de la Dirección de Informática y Estadística, quienes resguardarán los documentos originales, analizarán y darán resolución por la vía oficial en el plazo establecido por la Dirección de Informática y Estadística, atendiendo lo siguiente:

a) El acceso a los códigos fuente de sistemas informáticos de producción, deberá ser solicitado al Departamento de Seguridad Informática.
b) El acceso a los códigos fuente de sistemas informáticos de desarrollo, deberá ser solicitado al Departamento de Desarrollo de Sistemas.
c) El acceso a los servidores, deberá ser solicitado al Departamento de Infraestructura Informática.

Toda resolución deberá contar con el visto bueno del Director de Informática y Estadística y del Subdirector de Servicios Críticos y/o del Subdirector de Sistemas y Estadística según corresponda.

9.2. La Subdirección de Recursos Humanos deberá dar de baja el acceso de las cuentas de los trabajadores y en conjunto con la Dirección de Informática y Estadística realizarán el procedimiento respectivo para la baja definitiva del usuario, cuando corresponda.

9.3. El Departamento de Soporte Técnico será el único autorizado para instalar los programas y aplicaciones previamente autorizadas en los equipos de los trabajadores del RENAP.

9.4. El Departamento de Seguridad Informática limitará el tiempo de conexión a los sistemas y aplicaciones del RENAP al horario hábil de la Oficina del RENAP.

Con al menos veinticuatro (24) horas de anticipación el Registro Central de las Personas podrá solicitar a la Dirección de Informática y Estadística extender el tiempo de conexión a los sistemas y aplicaciones del RENAP en las Oficinas del RENAP, por medio de oficio con visto bueno de la máxima autoridad del Registro Central de las Personas.

9.5. El trabajador de la Dirección de Informática y Estadística que tenga a su cargo la administración de servidores tendrá acceso a los equipos correspondientes por medio de la "Boleta de acceso políticas de Firewall"

9.6. Todo intento de acceso no autorizado a la información contenida en los sistemas, bases de datos, servidores, computadoras y cualquier otro dispositivo de cómputo del RENAP, así como el abuso sobre los permisos y privilegios que le fueron otorgados será considerado como una intrusión y se dará de baja a los usuarios y se informará a la máxima autoridad de la dependencia para las acciones correspondientes.

10. Uso de contraseña

10.1. Toda contraseña o clave de acceso es considerada como información confidencial.

10.2. La contraseña deberá cumplir con los requisitos mínimos de seguridad siguientes:

- Ocho (8) caracteres.
- Incluir mayúsculas y minúsculas.
- Incluir números y caracteres especiales.

10.3. El cambio de contraseña deberá realizarse cada sesenta (60) días o cuando el usuario considere necesario.

10.4. Todo reinicio de contraseña a causa de bloqueo del equipo de cómputo se tendrá que solicitar por medio de la boleta "Reinicio de Contraseña", adjuntando copia del Documento Personal de Identificación -DPI-.

Los trabajadores que laboran fuera de la Sede del RENAP que no puedan realizar la gestión de manera personal ante la Dirección de Informática y Estadística, la dependencia a la que pertenecen podrá solicitar el reinicio de contraseña por medio de oficio, adjuntando una fotocopia de la boleta "Reinicio de Contraseña" debidamente completada por el trabajador interesado. Posteriormente, la dependencia solicitante tendrá la obligación de presentar ante la Dirección de Informática y Estadística la boleta en original en un plazo no mayor de 30 días calendario, caso contrario serán deshabilitados los accesos.

11. Uso de software de aplicación y software de sistemas

11.1. Todo software instalado y utilizado en los equipos de cómputo, propiedad del Registro Nacional de las Personas -RENAP- o aquellos utilizados en nombre de ella, debe cumplir con los principios institucionales, los acuerdos nacionales e internacionales y la legislación nacional vigente sobre derechos de autor y en todo caso está sujeto al respeto de los derechos o voluntad expresada por el autor en documentos físicos o digitales de licenciamiento.

11.2. Los equipos de cómputo serán verificados semestralmente por parte del Departamento de Soporte Técnico, quienes podrá retirar o inhabilitar todos los programas utilitarios que no cumplan con los derechos de autor.

12. Registro de eventos

12.1. Todo servidor y equipo de comunicación tendrá sincronizado el tiempo con exactitud y precisión, para asegurar el registro de eventos.

13. Usuarios de base de datos

13.1. Únicamente los trabajadores y quienes presten servicios técnicos o profesionales a la Institución, podrán solicitar un usuario en la base de datos del RENAP.

13.2. Toda solicitud de acceso a la base de datos del RENAP deberá efectuarse a través de la "Boleta de Gestión de Usuario de Base de Datos", con visto bueno de la máxima autoridad de la dependencia solicitante y deberá ser entregada a la Dirección de Informática y Estadística, para su análisis y verificación.

13.3. El Departamento de Seguridad Informática verificará las solicitudes realizadas a través de la "Boleta de Gestión de Usuario de Base de Datos" y la "Boleta de Permisos y Creación de Objetos en Base de Datos", previo a autorización.

13.4. El Departamento de Base de Datos será responsable de la creación, modificación o baja de usuarios u objetos de la base de datos del RENAP.

13.5. El Departamento de Base de Datos deberá mantener un registro actualizado de las modificaciones de usuarios u objetos realizadas, así como de la documentación de respaldo correspondiente.

13.6. Ante la terminación de la relación laboral o recisión de contrato administrativo, el jefe inmediato del trabajador o el responsable de quien preste servicios técnicos o profesionales a la Institución, deberá verificar y asegurar la entrega completa de la información utilizada por estos.

14. Carpetas compartidas en red local

14.1. Toda solicitud de creación o acceso a carpetas compartidas en red local deberá especificar los usuarios que tendrán acceso a la misma y el tipo de información que compartirá, debiendo realizarse por medio de oficio dirigido a la Dirección de Informática y Estadística, con visto bueno de la máxima autoridad de la dependencia solicitante.

14.2. El Departamento de Soporte Técnico es el responsable de crear las carpetas compartidas de conformidad con lo solicitado y debidamente autorizado.

14.3. El solicitante será responsable de la información que contenga la carpeta compartida y el uso que se le dé a la misma.

14.4. Las carpetas compartidas son para uso exclusivo de información de la Institución, la Dirección de Informática y Estadística no se responsabiliza por la integridad de la información contenida en ellas.

Control de cambios

Versión	Fecha	No. de folios	Unidades involucradas	Descripción
04	2024	13	Dirección de Informática y Estadística	Política de Control de Accesos.
03	2022	13	Dirección de Informática y Estadística	Política de Control de Accesos aprobada mediante el Acuerdo de Dirección Ejecutiva número DE-640-2022.
02	2019	14	Dirección de Informática y Estadística	Política de Control de Accesos aprobada mediante el Acuerdo de Dirección Ejecutiva número DE-102-2019.
01	2016	20	Dirección de Informática y Estadística	Política de Control de Accesos aprobada mediante el Acuerdo de Dirección Ejecutiva número DE-147-2016.

Elaborado por:	Revisado por:	Revisado por:	Validado por:	Validado por:	Validado por:	Aprobado por:
Departamento de Organización y Métodos	Jefe de Organización y Métodos	Director de Gestión y Control Interno	Jefe de Seguridad Informática	Subdirector de Servicios Críticos	Director de Informática y Estadística	Director Ejecutivo