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

ACUERDO DE DIRECCIÓN EJECUTIVA NÚMERO DE-640-2022
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 que 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 47 y 82 del Acuerdo de Directorio número 80-2016 del Registro Nacional de las Personas, Reglamento de Organización y Funciones del Registro Nacional de las Personas, el Departamento 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; 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 03, 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 lineamientos de administración y uso de los accesos proporcionados por la Dirección de Informática y Estadística y 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 del Decreto número 90-2005 del Congreso de la República de Guatemala, Ley del Registro Nacional de las Personas; 47, 82 y 84 del Acuerdo de Directorio Número 80-2016, 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 03, 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. Notifíquense 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 dos de noviembre de dos mil veintidós.

REGISTRO NACIONAL DE LAS PERSONAS
RENAP
DIRECTOR EJECUTIVO

DOCTOR RODOLFO ESTUARDO ARRIAGA HERRERA
DIRECTOR EJECUTIVO

SECRETARÍA GENERAL

CÉDULA DE NOTIFICACIÓN

En el municipio de Guatemala, departamento de Guatemala, el cuatro de noviembre de dos mil veintidós, siendo las catorce horas con cincuenta y un minuto (s), constituido en: Calzada Roosevelt trece guión cuarenta y seis zona siete. Sede del **RENAP. Ciudad de Guatemala. NOTIFICO A: DIRECCIÓN DE GESTIÓN Y CONTROL INTERNO.** El contenido del Acuerdo emitido por: Dirección Ejecutiva del Registro Nacional de las Personas número DE guión seiscientos cuarenta guión dos mil veintidós **(DE-640-2022),** de fecha dos de noviembre de dos mil veintidós, por medio de cédula entregada a: Evelyn Morales, haciéndole entrega de las copias de ley que consta de **UN** folio (s) y quien de enterado (a) Sí firma.

1

Lic. Carlos Edgar Rodríguez Monroy
Técnico Jurídico de Secretaría General
Secretaría General
Sede del RENAP Guatemala, Guatemala

Registro Nacional de las Personas
RENAP
RECIBIDO
04 NOV 2022
DIRECCIÓN DE GESTIÓN Y CONTROL INTERNO
HORA: 14:51
FIRMA:

RENAP
Registro Nacional de las Personas

DIRECCIÓN DE INFORMÁTICA Y ESTADÍSTICA

POLÍTICA DE CONTROL DE ACCESOS

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

RENAP
Registro Nacional de las Personas
Lic. Rudy Noé Manrriegos Lemus
Director de Gestión y Control Interno
Dirección de Gestión y Control Interno
Sede del RENAP, Guatemala, Guatemala

RENAP
Registro Nacional de las Personas
Ing. José Daniel Girón Miranda
Director de Informática y Estadística
Dirección de Informática y Estadística
Sede del RENAP, Guatemala, Guatemala

RENAP
Registro Nacional de las Personas
Lic. Juan Pablo Ulescas de la Cruz
Subdirector de Servicios Críticos
Dirección de Informática y Estadística
Sede del RENAP, Guatemala, Guatemala

Lic. Ricardo Bernabé Bercián Ramírez
Jefe de Organización y Métodos
Dirección de Gestión y Control Interno
Sede del RENAP, Guatemala, Guatemala

FECHA DE EMISIÓN:	Octubre 2022
CÓDIGO:	POL-09-01-2022
VERSIÓN:	03

DEPARTAMENTO DE ORGANIZACIÓN Y MÉTODOS
DIRECCIÓN DE GESTIÓN Y CONTROL INTERNO

Contenido

1. Objetivo de la política

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

3. Base legal

- 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 74-2013 del Registro Nacional de las Personas, el cual establece la clasificación y denominaciones: Sede, Oficinas y Oficinas Auxiliares del RENAP.
- Acuerdo de Directorio número 80-2016, Reglamento de Organización y Funciones del Registro Nacional de las Personas.
- Reglamento Interior de Trabajo del Registro Nacional de las Personas -RENAP- vigente, aprobado por medio de Acuerdo de Directorio 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 y prohibidos, salvo que bajo los lineamientos 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.

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 pertenece.

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. La solicitud de acceso al Sistema de Consulta de Documento Personal de Identificación -DPI-, deberá contar con autorización del Director de Procesos o la persona a quien delegue.

6.5. El Departamento de Seguridad Informática deberá documentar los diferentes niveles de acceso, con la finalidad de identificar el alcance de cada uno de ellos en la aplicación; a través de una base de datos específica para el efecto.

6.6. El Departamento de Desarrollo de Sistemas deberá mantener un inventario actualizado de todos los sistemas de información con los que opera la Institución y los usuarios que tengan acceso a los mismos, este deberá incluir al responsable de la administración de cada sistema y los usuarios autorizados para su ingreso.

6.7. El jefe inmediato del trabajador o quien preste servicios técnicos o profesionales, 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.

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

6.9. El Departamento de Seguridad Informática será 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 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 de datos del RENAP.

7.3. El Departamento de Seguridad Informática designará al personal que deberá verificar los datos de quien solicita acceso a la red y servicios a través del nombramiento, contrato, toma de posesión o documento generado por la Subdirección de Recursos Humanos.

7.4. El Departamento de Seguridad Informática deberá verificar que el nivel de acceso solicitado por el usuario corresponda al nivel de acceso autorizado para su puesto, según el alcance que tenga en la aplicación.

7.5. El Departamento de Seguridad Informática, otorgará al usuario el acceso a la red y servicios, toda vez haya sido aprobado.

7.6. 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.

7.7. 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].

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

7.9. Todas las solicitudes de creación de usuario (aceptada o denegada), estarán registradas y serán cotejadas con los registros de la Subdirección de Recursos Humanos.

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

7.10. 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.

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

7.12. Los perfiles del personal que labora en la Auditoría Interna deberán incluir permisos para la revisión de bitácoras de los administradores.

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).

Nota: en el caso de quienes presten servicios técnicos o profesionales, los documentos deberán ser de la persona responsable del equipo.

8.2. Los trabajadores del RENAP podrán tener consignado un usuario y un equipo de cómputo. Para casos especiales se podrá consignar un segundo equipo, tomando en cuenta lo siguiente:

a) El usuario podrá tener asignado un equipo que no está consignado en su tarjeta de responsabilidad, cuando requiera cualquiera de lo siguiente:
   - Cubrir turnos (rotación de personal de fin de semana, horario no hábil).
   - Cubrir permisos previstos (vacaciones, licencias).
   - Cubrir horario de almuerzo (en oficinas donde solo se cuenta con dos personas).
   - Cubrir emergencias (accidentes, fallecimiento, enfermedad, entre otros).

b) Se deberá entregar junto a la "Boleta Única Todos los Servicios", la "Tarjeta de Responsabilidad" de la persona a quien se cubrirá (con el equipo marcado o resaltado), a la Dirección de Informática y Estadística.

c) El tiempo contemplado para los casos del punto anterior, en el que el usuario que realizará la cobertura temporal no contará con el equipo consignado en su "Tarjeta de Responsabilidad", deberá ser menor a un mes.

d) El personal de la Dirección de Informática y Estadística que tenga a su cargo la administración de servidores tendrá acceso a los equipos correspondientes para dicho efecto.

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

9. Derecho de acceso

9.1. El Departamento de Seguridad Informática en conjunto con el Departamento de Gestión de Recursos Humanos verificarán periódicamente la vigencia de los derechos de acceso de los usuarios.

9.2. 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 de la solicitud por la vía oficial en el plazo establecido por la Dirección de Informática y Estadística, según lo siguiente:

a) Solicitudes de acceso a los códigos fuente de sistemas informáticos de producción, solicitarlo al Departamento de Seguridad Informática;
b) Solicitudes de acceso a los códigos fuente de sistemas informáticos de desarrollo, solicitarlo al Departamento de Desarrollo de Sistemas; y,
c) Solicitudes de acceso a los servidores, solicitarlo al Departamento de Infraestructura Informática.

Nota: toda resolución deberá contar con el visto bueno de la máxima autoridad de la Dirección de Informática y Estadística y de la máxima autoridad de la Subdirección correspondiente.

9.3. 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.

9.4. 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.

9.5. El Departamento de Seguridad Informática deberá monitorear e identificar los equipos conectados a la red institucional.

9.6. 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.

9.7. Toda solicitud de extensión de horario de conexión a los sistemas y aplicaciones del RENAP deberá ser solicitada por medio de oficio con visto bueno de la máxima autoridad del Registro Central de las Personas, al Departamento de Seguridad Informática de la Dirección de Informática y Estadística, con al menos veinticuatro (24) horas de anticipación.

9.8. 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 tomarán las acciones disciplinarias y legales correspondientes.

10. Uso de contraseña

10.1. Toda contraseña o clave de acceso son consideradas 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; y,
- Sin espacios en blanco.

10.3. El cambio de contraseña deberá realizarse cada sesenta (60) días (se solicitará automáticamente) o cuando el usuario o el Departamento de Seguridad Informática considere que existe peligro de divulgación.

10.4. La contraseña predeterminada por la Dirección de Informática y Estadística deberá ser cambiada inmediatamente después de la instalación de software y/o hardware.

10.5. Todo reinicio de contraseña a causa de bloqueo del equipo de cómputo deberá solicitarlo por medio de la boleta "Reinicio de Contraseña", adjuntando copia del Documento Personal de Identificación -DPI- y ser dirigido a la Dirección de Informática y Estadística o mediante correo dirigido a soporte@renap.gob.gt.

Nota: En los casos que el usuario no pueda realizar la gestión por la vía indicada, el reinicio deberá ser solicitado por medio del Departamento de Atención y Servicio al Usuario o el Departamento de Registro Civil de las Personas del Registro Central de las Personas.

10.6. El usuario es el único responsable del uso de la contraseña, cualquier incidente o evento causado por el mal uso de la contraseña deberá ser sancionado conforme al Reglamento Interior de Trabajo del Registro Nacional de las Personas -RENAP- vigente, aprobado por medio de Acuerdo de Directorio del Registro Nacional de las Personas.

11. Registro de inicio seguro

11.1. El sistema no deberá mostrar mensajes de ayuda durante el procedimiento de registro de inicio.

11.2. El sistema validará la información de registro de inicio únicamente al terminar todos los datos de entrada, si se presenta una condición de error, el sistema no deberá indicar qué parte de los datos es correcta o incorrecta.

11.3. El sistema limitará la cantidad de intentos permitidos de registro de inicio, a un máximo de cinco (5) intentos previos a bloquear el acceso.

11.4. No se deberá mostrar la contraseña que se introduce.

12. Uso de software de aplicación y software de sistemas

12.1. 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.

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

13. Registro de eventos

13.1. Se deberá mantener registro de las actividades críticas de los sistemas, equipos y redes, con el fin de agilizar el monitoreo.

13.2. El registro de eventos deberá estar protegido contra vulnerabilidades informáticas, deberá identificar puntos de falla en los sistemas y proporcionar información para el monitoreo de seguridad.

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

14. Usuarios de base de datos

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

14.2. Toda solicitud de acceso a la base de datos del RENAP deberá ser 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.

14.3. 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.

14.4. 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.

14.5. El Departamento de Seguridad Informática deberá documentar y registrar los diferentes niveles de acceso de los usuarios de la base de datos.

14.6. El Departamento de Seguridad Informática utilizará para el registro de usuarios, la "Boleta de Gestión de Usuario de Base de Datos".

14.7. El Departamento de Base de Datos deberá enviar mensualmente al Departamento de Seguridad Informática, un informe de las modificaciones de usuarios u objetos realizados, adjuntando la documentación de respaldo correspondiente.

14.8. El jefe inmediato del usuario deberá verificar y asegurar la entrega completa del usuario e información correspondiente, utilizados por el trabajador al momento de retirarse de la Institución.

15. Carpetas compartidas locales

15.1. Toda solicitud de acceso a las carpetas compartidas deberá realizarse mediante oficio dirigido a la Dirección de Informática y Estadística, con visto bueno de la máxima autoridad de la dependencia solicitante.

15.2. El Departamento de Soporte Técnico será responsable de crear en las carpetas compartidas lo solicitado, debidamente autorizadas.

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

15.4. 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
03	2022	13	Dirección de Informática y Estadística	Política de Control de Accesos
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.