2016

Controles Generales de los Recursos Informáticos

DTI-CNT-2016-0001

CENTRO NACIONAL DE REGISTROS – DIRECCION DE TECNOLOGÍA DE LA INFORMACIÓN

SAN SALVADOR, 05 MAYO DE 2016

HISTÓRICO DEL DOCUMENTO

FECHA	AUTOR	VERSION	REFERENCIA DE CAMBIO	FIRMAS
29/04/2005	Lic. Carlos Enrique Serpas Flores Director Adjunto de Tecnología de la Información, Supervisor de Seguridad en Tecnologías de la Información y Coordinador de Soporte Informático	1.0	No existe documento previo	
05/05/2016	Lic. Nelson Chacón Supervisor de Seguridad en Tecnología de la Información	2.0	Revisión, modificación y reestructura del documento	

REVISIÓN

NOMBRE	CARGO	FIRMAS
Lic. Luis Enrique Interiano	Gerente de Infraestructura Informática	
Ing. Miguel Alvarenga	Gerente de Soporte Técnico	
Ing. Nelson Tesorero	Gerente de Sistemas Geográficos y Catastrales	
Lic. Guillermo Díaz	Gerente de Sistemas Registrales	
Ing. Paúl Ramírez	Coordinador de Base de Datos	

APROBACIÓN

FECHA	NOMBRE	CARGO	FIRMAS
26/05/2016	Ing. Fernando Edward Calderón	Director de la DTI	

DISTRIBUCIÓN

COPIA	NOMBRE	UBICACION
Para ejecución y Distribución	Lic. Rogelio Canales	Dirección Ejecutiva
Informativa	Licda. María Silvia Guillen	Subdirección Ejecutiva
Informativa	Todo el personal de la DTI	DTI

Contenido

GLOSARIO

No.	TERMINO	CONCEPTO
1	**CLAVE DE ACCESO**	Se refiere al nombre único por medio del cual se identifica a cada individuo que hace uso de los recursos dentro de una red informática y/o accede a los diferentes Sistemas Informáticos.
2	**CUENTAS DE USUARIO**	Se refiere al nombre único por medio del cual se identifica a cada individuo que hace uso de los recursos dentro de una red informática y/o accede a los diferentes Sistemas Informáticos.
3	**CUENTAS DE USUARIO ESPECIALES O COMPARTIDAS**	Son aquellas en las que se han asignado privilegios de modificación y/o eliminación de información, y que en algunos casos comparten la responsabilidad con otros usuarios de igual condición en la administración de información.
4	**REPOSITORIO HISTÓRICO**	Se refiere a un espacio de almacenamiento destinado para guardar la información histórica que se encuentra saturando las Bases de Datos.
5	**SPAMMING**	Es el abuso de cualquier tipo de sistema de mensajes electrónicos y por extensión, cualquier forma de abuso en otros medios como Spam en mensajería instantánea, en foros, en blogs, en buscadores, en mensajes, etc.

MARCO LEGAL

El presente documento tiene como objetivo primordial el normar el uso de los Recursos Informáticos del Centro Nacional de Registros (CNR), basándose en el Reglamento de las Normas Técnicas de Control Interno Especificas del CNR, metodologías, normativas y procedimientos vigentes en el CNR.

CAPÍTULO I

NORMATIVA PARA LA UTILIZACIÓN DE RECURSOS Y SERVICIOS INFORMÁTICOS

Art 1. OBJETO

Normar el uso de los recursos y servicios informáticos que proporciona el CNR a los usuarios para garantizar su correcta utilización y optimizar su aprovechamiento.

Art 2. SUJETOS DE LA NORMATIVA

2.1. Usuario interno, independientemente de la modalidad de contratación, que tengan acceso a recursos y servicios tecnológicos prestados por la institución en sus equipos asignados.

2.2. Usuario externo, según aplique, con acceso autorizado por medio de convenios interinstitucionales a los recursos y servicios tecnológicos del CNR.

Art 3. USO DEL EQUIPO

El CNR provee a los usuarios el equipo computacional, accesorios e insumos que soportan los procesos de los servicios prestados por la institución y que sean adecuados para el buen desempeño de sus labores, por tanto:

3.1. El CNR hará entrega del equipo computacional en buen funcionamiento e instalará software básico.

3.2. Todo el SW especializado requerido para realizar las funciones propias de cada puesto de trabajo, deberá ser solicitadas a la DTI.

3.3. Es responsabilidad del usuario proteger y mantener en buen estado el equipo computacional asignado.

3.4. Se debe utilizar el equipo computacional asignado, exclusivamente para propósitos relacionados con la actividad y funciones desempeñadas en la organización.

3.5. El usuario debe reportar a la mayor brevedad, a la Unidad de Atención al Cliente Interno de la Dirección de Tecnología de la Información (DTI) o al Soporte Informático Local, cualquier tipo de daño en el equipo computacional.

Se prohíbe por parte del usuario del equipo:

3.6. Instalar, desinstalar o modificar la configuración de hardware y software del equipo asignado sin autorización de la DTI.

3.7. Instalar programas, juegos, música o videos, no relacionados con las funciones asignadas.

3.8. Utilizar equipo computacional de otros usuarios sin la debida autorización del responsable de dicho equipo o en su defecto el jefe inmediato.

3.9. Retirar cualquier recurso informático, partes de los mismos o sus accesorios de las instalaciones del CNR, sin la autorización del Jefe de la Unidad a la que está asignado.

3.10. Compartir carpetas de archivos sin la debida autorización del jefe de la unidad.

3.11. Conectar a la red interna del CNR o utilizar equipos computacionales que no pertenezcan a la institución, sin la autorización del Supervisor de Seguridad en Tecnología de la Información.

3.12. Utilizar accesorios de almacenamiento masivo (CD/DVD, memorias USB, discos removibles, cámaras, teléfonos móviles, entre otros) sin la autorización del Supervisor de Seguridad en Tecnología de la Información.

3.13. Conectar a los toma corrientes de UPS, dispositivos eléctricos no autorizados por la DTI y que por su alto consumo de energía, deben estar conectados al flujo eléctrico normal.

Art 4. CONTROL DE COMPUTADORAS PORTÁTILES

Para el personal que tiene asignado computadoras portátiles, se debe cumplir con las siguientes regulaciones específicas:

4.1. Cada Dirección, Gerencia y/o Unidad Staff, tendrá autoridad para definir, justificar y asignar equipos portátiles al personal bajo su cargo.

4.2. Se definen 2 tipos de asignación:

4.2.1. Permanente: Cuando el equipo portátil es utilizado por una sola persona, por tiempo indefinido.

4.2.2. Uso Común: Cuando el equipo portátil puede ser utilizado por varias personas temporalmente, según demanda.

4.3. Para los dos tipos de asignación, deberá haber una persona responsable del equipo portátil.

4.4. El usuario deberá contar con una autorización firmada y sellada por el Jefe inmediato para la salida de computadoras portátiles de las instalaciones del CNR, en la que se deberá especificar y justificar la razón de la salida.

4.5. El usuario será responsable del buen uso y cuido para que el equipo portátil no sea expuesto a condiciones que afecten su operación.

4.6. En caso de pérdida o extravío de una computadora portátil, el usuario será responsable por la reposición del equipo o por el pago del valor determinado por la Unidad Financiera Institucional cuando la pérdida ocurra por culpa, dolo o negligencia de su parte.

Art 5. ACCESO A LA INFORMACIÓN

El usuario tendrá acceso a la información necesaria para la realización de sus tareas a través de cualquiera de los servicios tecnológicos del CNR, por tanto:

5.1. Los accesos a las aplicaciones informáticas y los roles inherentes a cada tipo de acceso, deben ser autorizados por los titulares de las unidades propietarias de la aplicación.

5.2. Para garantizar la disponibilidad, confidencialidad y auditoría de los accesos a las aplicaciones informáticas, la DTI asignará cuentas de usuario y sus respectivas claves de acceso a los usuarios autorizados, que le permitan autenticarse en las distintas plataformas tecnológicas de la institución.

5.3. Las cuentas de usuario y sus respectivas claves de acceso son personales, por lo tanto, su uso adecuado es responsabilidad directa del usuario autorizado, así como las consecuencias que se deriven de actividades fraudulentas efectuadas con dichas cuentas de usuario.

5.4. La creación de cuentas de usuario de especiales o compartidas, debe ser aprobada y justificada por la máxima autoridad del área propietaria de la información.

Art 6. USO DE SOFTWARE

Respecto al uso del software:

6.1. Está prohibido el uso de software no autorizado por la institución, incluyendo el Software Libre, sino está dentro de las funciones de su puesto de trabajo y sin el visto bueno del Supervisor de Seguridad en Tecnología de la Información.

6.2. Está prohibido sacar copias no autorizadas del software licenciado por el CNR y su utilización para fines diferentes a los organizacionales.

6.3. Ningún empleado del CNR podrá copiar software desarrollado internamente o información generada en la institución, para fines particulares.

6.4. Se prohíbe a los usuarios desinstalar o deshabilitar el software antivirus, así como cualquier otro software que garantice la seguridad de los recursos tecnológicos.

6.5. La DTI auditará sin previo aviso, el buen uso del equipo computacional y el software instalado en el mismo.

Art 7. RESPONSABLIDADES DEL USUARIO

7.1. Todo usuario es responsable de cumplir con las Políticas y Normas que aplican al uso de los recursos y servicios que le han sido habilitados.

7.2. Cada usuario debe firmar los Términos de Uso de los Recursos Informáticos del CNR (Ver anexo N° 1).

Art 8. RESPONSABILIDADES DE LA UNIDAD SOLICITANTE

8.1. El titular de la unidad solicitante es el responsable de pedir y autorizar los recursos y servicios informáticos a la DTI asignados al personal bajo su responsabilidad.

8.2. El titular de la unidad solicitante tiene la obligación de pedir y autorizar la revocación de los recursos y servicios informáticos a la DTI del personal bajo su cargo.

CAPÍTULO II

NORMATIVA DE SEGURIDAD PARA CLAVES DE ACCESO A LOS SERVICIOS INFORMÁTICOS DEL CNR

Art 9. OBJETO

Definir los lineamientos de seguridad para la creación y mantenimiento de claves de acceso a los servicios informáticos del CNR.

Art 10. SUJETOS DE LA NORMATIVA

RESPONSABLES DE LA APLICACIÓN:

a) Administradores de servidores.
b) Administradores de bases de datos.
c) Administradores de aplicaciones.
d) Administradores de red.
e) Administradores del Correo Electrónico Institucional.

RESPONSABLES DEL CUMPLIMIENTO:

f) Todos los usuarios que hacen uso de los distintos servicios informáticos del CNR

Art 11. CREACIÓN DE CLAVES DE ACCESO

Para la creación de palabras claves (Password) se deben aplicar las siguientes especificaciones técnicas:

a) 8 caracteres como mínimo.
b) Alguna Combinación de:

- Letras Mayúsculas: A- Z
- Letras minúsculas: a - z
- Números: 0- 9
- Símbolos especiales cuando la plataforma tecnológica así lo permita.

Art 12. MANTENIMIENTO DE CLAVES DE ACCESO

Todas las aplicaciones del CNR deben permitir lo siguiente:

a) Cambio de clave al inicio de la primera sesión
b) Cambio de clave a discreción del usuario cuando sospeche que su clave ha sido comprometida.
c) Recuperación de la contraseña en caso de pérdida u olvido, siendo el correo electrónico institucional el medio de recuperación por defecto.
d) Orientar al usuario el nivel de fortaleza de la contraseña.
e) Parametrizar el vencimiento de la contraseña.
f) Parametrizar el re-uso de contraseñas
g) Parametrizar el número de intentos fallidos y bloquear la sesión al llegar al límite.
h) No guardar ninguna contraseña en la base de datos de la aplicación en texto claro.

Si por alguna razón la tecnología de desarrollo de la aplicación no permite alguna de estas características, debe ser documentado en el manual técnico de la aplicación. Estos lineamientos deben ser aplicados al momento de realizar compras de software de terceros para uso interno del CNR.

Los empleados pueden solicitar el uso de gestores de contraseñas, de tipo bóveda de claves, que hayan sido examinados por el personal técnico del CNR, y aprobados para su uso por la DTI.

CAPÍTULO III

NORMATIVA DE USO DEL SERVICIO DE INTERNET PROVISTO POR EL CNR

Art 13. OBJETO

Regular el uso eficiente, confiable y seguro de Internet por parte de los diferentes usuarios que utilizan dicho servicio en el CNR.

Art 14. SUJETOS DE LA NORMATIVA

Todos los usuarios internos o externos que tengan acceso al servicio de Internet provisto por el CNR.

Art 15. DEL USO DE INTERNET

15.1. El CNR proporcionará acceso a Internet con la finalidad de facilitar la búsqueda de información requerida para el desempeño de sus labores dentro de la institución.

15.2. El tipo de acceso a internet que se habilite a los usuarios será autorizado por los titulares de la unidad solicitante de acuerdo a las funciones que realiza el usuario.

15.3. Los usuarios solo deben utilizar el servicio de Internet para funciones propias del cargo que desempeñan, utilizando única y exclusivamente el software y hardware autorizado por la DTI.

15.4. El usuario debe Informar inmediatamente cualquier actividad irregular en el servicio de Internet a la Unidad de Atención al Usuario Interno de la DTI.

Art 16. PROHIBICIONES

Las prohibiciones en el uso del servicio de internet son:

16.1. Jugar o realizar apuestas usando la red de telecomunicaciones institucional del CNR.

16.2. Utilizar otros mecanismos de acceso a Internet, que no sean los canales autorizados por la DTI.

16.3. Hacer cambios de configuración en los equipos informáticos para acceder a Internet que no sean realizados por personal autorizado por la DTI.

16.4. Violar o intentar violar los sistemas de seguridad de los equipos informáticos propiedad del CNR.

Art 17. DE LA ADMINISTRACIÓN Y MONITOREO

17.1. La Unidad de Atención al Cliente Interno de la DTI, es la encargada de tramitar la creación o mantenimiento de cuentas para los diferentes servicios al usuario, incluyendo el servicio de acceso a Internet, luego de recibir el formulario de solicitud de servicios F0226 debidamente completado, firmado por el usuario final y junto con las autorizaciones correspondientes.

La DTI, a través de la Gerencia de Infraestructura Informática, es responsable de:

17.2. Administrar y mantener en funcionamiento la infraestructura tecnológica requerida para la prestación del servicio de Internet.

17.3. Implementar mecanismos necesarios para mantener la seguridad en el servicio de Internet.

17.4. Monitorear aleatoriamente el servicio de Internet con el fin de controlar posibles abusos en la utilización del servicio.

17.5. La DTI puede asignar el tiempo de navegación de manera prioritaria, de tal forma que si el tráfico del uso de Internet se viera saturado o demasiado congestionado en un momento determinado, la DTI podrá desconectar el servicio, notificando previamente al usuario, o mediante la asignación de horarios de uso o por medio de la restricción de accesos, lo cual le será notificado al usuario involucrado.

CAPÍTULO IV
NORMATIVA DE USO DEL CORREO ELECTRÓNICO INSTITUCIONAL DEL CNR

Art 18. OBJETO

Regular el uso eficiente, confiable y seguro del correo electrónico institucional por parte de los diferentes usuarios del CNR.

Art 19. SUJETOS DE LA NORMATIVA

Todas las personas internas o externas que tengan cuenta de correo electrónico del CNR.

Art 20. DEL USO DEL CORREO ELECTRÓNICO

20.1. El CNR proporcionará una cuenta de correo electrónico institucional con la finalidad de facilitar la comunicación entre los empleados y funcionarios, cuando esto sea necesario para el desempeño de sus labores dentro de la institución, debiendo ser solicitadas a través del formato F0226 a la jefatura inmediata y autorizadas por el Director respectivo.

20.2. Es responsabilidad del titular solicitante definir el perfil de usuario para cada uno de los tipos de cuentas de correo electrónico.

20.3. Los usuarios deben utilizar el correo electrónico del CNR única y exclusivamente para funciones propias del cargo que desempeñan.

20.4. La cuenta de correo electrónico es de uso personal e intransferible, por lo tanto no debe proporcionarse la clave de acceso a terceros por ningún motivo.

20.5. Informar inmediatamente cualquier actividad irregular en el uso del correo electrónico institucional a la Unidad de Atención al Cliente Interno de la DTI.

20.6. Cumplir con la Normativa de Seguridad para Claves de Acceso a los Servicios Informáticos del CNR.

Art 21. PROHIBICIONES

21.1. Utilizar los contenidos con fines o efectos contrarios a la ley, la moral, las buenas costumbres o al orden público.

21.2. Divulgar información de la institución sin contar con la debida autorización.

21.3. Los usuarios no deben modificar su configuración en el correo electrónico, con fines de hacerse pasar por otra persona, usar la cuenta de otro usuario, falsificar mensajes en nombre de otro usuario.

Art 22. DE LA ADMINISTRACIÓN Y MONITOREO

22.1. La Unidad de Atención al Cliente Interno de la DTI, es la responsable de tramitar la creación o mantenimiento de cuentas para los diferentes servicios al usuario, incluyendo el servicio de correo electrónico institucional, luego de recibir el formulario de solicitud de servicios según formato F0226 debidamente completado, firmado por el usuario final y junto con las autorizaciones correspondientes.

La Gerencia de Infraestructura Informática es la responsable de:

22.2. Establecer los mecanismos de control a nivel de correos entrantes y salientes, mediante la utilización de tecnologías informáticas apropiadas para evitar mensajes infectados de virus.

22.3. Administrar y mantener en funcionamiento la infraestructura tecnológica requerida para la prestación del servicio de correo electrónico institucional.

22.4. Implementar mecanismos necesarios para mantener la seguridad en el servicio de correo electrónico institucional.

22.5. Monitorear periódicamente el servicio de correo electrónico con el fin de controlar posibles abusos en la utilización del servicio.

22.6. La DTI podrá inhabilitar aquellas cuentas que sin justificación alguna presenten inactividad durante un período de 30 días calendario.

CAPÍTULO V

NORMATIVA PARA EL PROCEDIMIENTO PARA LA ADQUISICIÓN DE TECNOLOGÍA INFORMÁTICA

Art 23. PROCEDIMIENTO

23.1 Todo requerimiento de adquisición de tecnología informática debe ser validado por La Dirección de Tecnología de la Información (DTI), mediante una solicitud de especificaciones técnicas enviada por la Unidad solicitante a la DTI del equipo o software informático.

23.2 La DTI elaborará las especificaciones técnicas de acuerdo a la tecnología existente y ofertada por los proveedores.

23.3 La DTI apoyará en la evaluación de las ofertas presentadas por los proveedores en cumplimiento de las especificaciones técnicas solicitadas.

CAPÍTULO VI
SANCIONES

El incumplimiento de las obligaciones y la violación de las prohibiciones establecidas en el presente Marco Normativo, hará incurrir al usuario infractor en las sanciones dispuestas en el Reglamento Interno de Trabajo del CNR, las cuales serán impuestas conforme al procedimiento establecido en la Cláusula No. 41 del Contrato Colectivo de Trabajo.

La aplicación de tales sanciones se efectuará sin perjuicio de la responsabilidad penal que pueda corresponder al usuario infractor, o de la civil que pueda caberle para la satisfacción y pago de los daños y/o costos, que sus actos u omisiones hayan causado al CNR o a terceros, por cualquier concepto.

CAPÍTULO VII
DIVULGACIÓN

La DTI será responsable que los Controles Generales de los Recursos Informáticos del CNR, sean hechas del conocimiento de los usuarios.

Se garantizará de ello utilizando los medios y recursos que estime convenientes, entre ellos, el de su puesta a disposición en la Intranet, todo sin perjuicio de cuidar que cada usuario exprese por escrito su conocimiento y aceptación de los Términos de Uso (Ver anexo N°1)

CAPÍTULO VIII
VIGENCIA

El presente Marco Normativo de Controles Generales de los Recursos Informáticos del CNR, entra en vigencia el día siguiente al de su publicación en la Intranet institucional.

ANEXO 1
TÉRMINOS DE USO DE LOS RECURSOS INFORMÁTICOS

1. AVISO LEGAL Y SU ACEPTACIÓN

El presente aviso legal (en adelante "Aviso Legal") expresado en el presente documento de Términos de Uso (TDU) regula la utilización de los recursos y servicios informáticos que el Centro Nacional de Registros (en lo sucesivo, "CNR") a través de la Dirección de Tecnología de la Información (DTI), proporciona al usuario (en adelante denominado El Usuario) para la realización de sus labores dentro de la institución.

El Usuario expresa su adhesión plena y sin reservas a todas y cada una de las condiciones expresadas en los presentes TDU y también a aquellas contenidas en la Política de Tecnologías de Información y Telecomunicaciones aprobada por Consejo Directivo del CNR y los Controles Generales y Controles de Aplicación a los Sistemas Informáticos requeridos por la Normativa Técnica de Control Interno específicas del CNR. Estos documentos y cualquier otro que sea aplicable se mantendrán en sus versiones digitales vigentes en la red interna (Intranet) de la institución. En consecuencia, el Usuario debe estar consciente de los compromisos adquiridos a través de la firma de este acuerdo de uso, en cada una de las ocasiones en que se proponga utilizar los recursos y servicios habilitados.

2. RECURSOS Y SERVICIOS

El CNR proporciona los recursos tecnológicos de información y comunicaciones, necesarios para el buen desempeño de las labores diarias, a considerar: Equipo y dispositivos periféricos, bases de datos, aplicaciones de soporte, antivirus, automatización de oficinas, servicios de valor agregado, servicios de telecomunicaciones y otros que de acuerdo a las distintas funciones que el cargo desempeñado exige.

3. RESPONSABILIDADES, OBLIGACIONES Y RESTRICIONES EN EL USO

El Usuario se compromete a cumplir lo dispuesto en las Políticas, Normativas y Procedimientos vigentes, relacionados con el uso de los recursos, servicios de tecnología de información y telecomunicaciones, aprobados por la Dirección de Tecnología de la Información (DTI) y la Alta Dirección del CNR y a respetar los derechos legales sobre los activos de la institución a los cuales se le haya permitido acceso.

Además se compromete a mantener la confidencialidad de la información institucional, durante el tiempo que ocupe un cargo dentro de la organización, e inclusive después de finalizada su relación laboral, independientemente de los motivos de su retiro.

4. SANCIONES

Las medidas disciplinarias por incumplimiento o faltas en el uso adecuado de los recursos, servicios tecnológicos de información y telecomunicaciones, y/o su regulación sobre su gravedad y reincidencia, serán establecidas y aplicadas de acuerdo al Reglamento Interno de Trabajo.

5. DURACIÓN Y TERMINACIÓN

La utilización de los recursos y la prestación de los servicios objeto del presente documento durará mientras el usuario labore en la institución. El Usuario acuerda a que el CNR, a su plena discreción, pueda cancelar sin previo aviso los servicios puestos a su disposición, o los mecanismos para el uso de los mismos, retirar y eliminar cualquier contenido dentro del servicio por cualquier razón, incluyendo, sin limitación, la falta de uso o si el CNR considera que el usuario ha violado o actuado inconsistentemente con el texto o el espíritu de estos TDU o demás políticas y normativas aplicables.

6. ACTUALIZACIÓN

Estos TDU podrán ser actualizados por el CNR sin previa notificación. El Usuario puede revisar las versiones vigentes de las Políticas, Normativas, Procedimientos, incluyendo los TDU en cualquier momento en: http://intranet.cnr.gob.sv/normativas

7. LEGISLACIÓN APLICABLE.

El Usuario, al hacer uso de los recursos y servicios puestos a su disposición por el CNR acepta en forma expresa e irrevocable el hecho que estos TDU así como la relación del Usuario con el CNR será regida por, e interpretada de acuerdo con, las leyes de la República de El Salvador. En caso de controversia, el Usuario y el CNR se someten expresamente a la jurisdicción de los Tribunales de la Ciudad de San Salvador, El Salvador. Renunciando tanto el Usuario como EL CNR, a cualquier otro fuero que pudiera corresponderles por razón de su domicilio presente o futuro.

Como usuario he leído y estoy de acuerdo a cumplir con las disposiciones contenidas en estos términos de uso aplicables a la infraestructura tecnológica del CNR. Entendiendo que una violación de estos términos de uso puede causar una acción disciplinaria, incluso terminación de contrato laboral, así como la responsabilidad civil y criminal a la que haya lugar.

Firma del Usuario:_____ Fecha: _____

Nombre Completo:_____ No Carnet:_____

2016

Controles Específicos de los Recursos Informáticos

DTI-CNT-2016-0002

CENTRO NACIONAL DE REGISTROS – DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN

SAN SALVADOR, 05 MAYO DE 2016

HISTÓRICO DEL DOCUMENTO

FECHA	AUTOR	VERSION	REFERENCIA DE CAMBIO	FIRMAS
29/04/2005	Lic. Carlos Enrique Serpas Flores Director Adjunto de Tecnología de la Información, Supervisor de Seguridad en Tecnologías de la Información y Coordinador de Soporte Informático	1.0	No existe documento previo	
05/05/2016	Lic. Nelson Chacón Supervisor de Seguridad en Tecnología de la Información	2.0	Revisión, modificación y reestructura del documento	

REVISIÓN

NOMBRE	CARGO	FIRMAS
Lic. Luis Enrique Interiano	Gerente de Infraestructura Informática	
Ing. Miguel Alvarenga	Gerente de Soporte Técnico	
Ing. Nelson Tesorero	Gerente de Sistemas Geográficos y Catastrales	
Lic. Guillermo Díaz	Gerente de Sistemas Registrales	
Ing. Paúl Ramírez	Coordinador de Base de Datos	

APROBACIÓN

FECHA	NOMBRE	CARGO	FIRMAS
26/05/2016	Ing. Fernando Edward Calderón	Director de la DTI	

DISTRIBUCIÓN

COPIA	NOMBRE	UBICACION
Para ejecución y Distribución	Lic. Rogelio Canales	Dirección Ejecutiva
Informativa	Licda. María Silvia Guillen	Subdirección Ejecutiva
Informativa	Todo el personal de la DTI	DTI

Contenido

GLOSARIO

No.	TERMINO	CONCEPTO
1	**ACTIVE DIRECTORY**	Es una implementación de los protocolos de nombres y directorios estándar de Internet. Utiliza un motor de bases de datos para procesar las transacciones y es compatible con diversos estándares de interfaces de programación de aplicaciones. Directorio donde se crean las cuentas de usuarios de red de acuerdo a las unidades organizativas donde correspondan.
2	**CONTROLES CRIPTOGRAFICOS**	Utilizados para encriptar, codificar o asignar una clave secreta. Basados en la confidencialidad de un archivo, poniendo una barrera para aquellos usuarios no autorizados.
3	**JOBS**	Trabajos de respaldo de datos programados
4	**SISSOR**	Sistema de Solicitud de Requerimientos
5	**ENDURECIMIENTO**	Término utilizado en TI, del Inglés Hardening, lo cual significa eliminar de un equipo informático los accesos no autorizados, aplicaciones no utilizadas, configuración y cierre de puertos de comunicación en un aplicativo. Así como aplicar una política de clave segura.

MARCO LEGAL

El presente documento tiene como objetivo primordial el normar el uso de los Recursos Informáticos del Centro Nacional de Registros (CNR), basándose en la norma internacional ISO 27002, adoptada por la Dirección de Tecnología de la Información (DTI).

Se aclara que toda solicitud se remita a través de los canales autorizados por la DTI.

CAPÍTULO I
NORMATIVA DE RESPALDO DE INFORMACIÓN

Art 1. OBJETO

Regular la gestión de los respaldos, recuperación y verificación de datos, alineados a las políticas definidas para tal fin, contenidas en el ANEXO V del Plan de Contingencia para la Continuidad de Servicios Informáticos del CNR con Código DTI-PC-SI-01 y el fiel cumplimiento del Manual de Respaldos, Verificación y Recuperación.

Art 2. SUJETOS DE LA NORMATIVA

Técnicos en Resguardo de Datos, Soportes Informáticos, Coordinador de Administración de Servidores, Administradores de Servidores de Aplicaciones, Gerentes de Sistemas y Administradores de Bases de Datos.

Art 3. RESPALDO DE DATOS

Siendo la información de los Registros de Propiedad Raíz e Hipotecas, Comercio, Propiedad Intelectual, Garantías Mobiliarias y del Instituto Geográfico y del Catastro Nacional de carácter público, el CNR tiene la obligación de garantizar la disponibilidad, integridad y confiabilidad de la información antes mencionada.

Debido a su importancia a escala nacional, se debe asegurar que la información tenga resguardos apropiados que garanticen la integridad de los datos en caso de siniestros o daños a la misma.

Por lo anterior, se debe proveer, gestionar y controlar los recursos necesarios para cumplir con esta responsabilidad institucional. Se deberá garantizar la realización de los respaldos periódicos de la información crítica de carácter organizacional en todas sus formas, incluyendo bases de datos, imágenes, mapas catastrales y aplicaciones relacionadas.

La información a ser respaldada se ha clasificado por su tipo de la siguiente manera: Base de Datos y su estructura, Imágenes de Documentos, Mapas Cartográficos y Archivos de Información (Documentos, Hojas Electrónicas, Presentaciones, etc.).

Para el caso del respaldo de archivos de información, incluyendo imágenes de Documentos y Mapas Cartográficos, los Directores de las sustantivas o en su defecto las personas que ellos designen, serán quienes informen a la DTI de cuales carpetas se les debe hacer dicho respaldo, determinándose en esa misma solicitud la periodicidad y tipo del respaldo.

Art 4. TIPOS DE RESPALDO

Se realizan los siguientes tipos de respaldo:

4.1. TOTAL (FULL): Todos los archivos seleccionados.

4.2. INCREMENTAL: Archivos modificados en un rango de tiempo determinado o creados a partir del último respaldo full.

Art 5. VERIFICACIÓN DE LAS COPIAS

Es responsabilidad del Técnico en Resguardo de Datos revisar diariamente la finalización correcta de los respaldos programados. En caso de falla en la realización del respaldo, deberá informar y tomar las medidas correctivas correspondientes, así como documentar el registro de dicha falla.

Art 6. RECUPERACIÓN DE DATOS

6.1. En caso de daños o pérdidas de archivos, el cliente interno deberá solicitar la recuperación del archivo dañado haciendo la solicitud correspondiente por medio de un requerimiento debidamente autorizado por el Titular de la Unidad Administrativa.

6.2. Cuando el daño o pérdida de datos se relacione con registros de una Base de Datos, será el DBA el responsable de solicitar la recuperación haciendo la solicitud correspondiente por medio de un requerimiento debidamente autorizado por el Titular de la Unidad Administrativa. El Técnico en Resguardo de Datos realizará el proceso de recuperación.

Art 7. MANTENIMIENTO AL HARDWARE

Se deben realizar revisiones preventivas y limpieza del equipo utilizado en los respaldos de acuerdo a un plan de mantenimiento anual, coordinando con cada Soporte Informático para su realización.

Art 8. ALMACENAMIENTO Y CONTROL DE LA MEDIA

8.1. Se debe mantener dentro del equipo, solamente la media de respaldos que se va a utilizar en la realización de respaldo.

8.2. Es responsabilidad del Soporte Informático o el Técnico en Resguardo de Datos, etiquetar la media de la copia de seguridad y documentar toda la información necesaria para la administración efectiva de los respaldos.

8.3. Para el almacenamiento de la media fuera de las oficinas del CNR, el Técnico en Resguardo de Datos, deberá seguir el procedimiento contenido en el ANEXO VI (DTI-PRO-009) del Plan de Contingencia para la Continuidad de Servicios Informáticos del CNR con Código DTI-PC-SI-01.

8.4. El tiempo de retención de todas las medias será acordado con los Titulares de las Unidades Administrativas.

CAPÍTULO II

NORMATIVA PARA EL CONTROL DE ACCESO AL CENTRO DE CÓMPUTO DE LA DTI Y A LOS CUARTOS DE SERVIDORES DE LAS OFICINAS DEPARTAMENTALES

Art 9. OBJETO

Definir los lineamientos de seguridad para el acceso al Centro de Cómputo de la DTI y a los cuartos de servidores de las Oficinas Departamentales del Centro Nacional de Registros (CNR).

Art 10. SUJETOS DE LA NORMATIVA

Todas las personas internas o externas que por razones laborales deben tener acceso al Centro de Cómputo de la DTI y a los cuartos de servidores de las Oficinas Departamentales.

Para los cuartos de servidores de las oficinas departamentales y para el centro de cómputo principal de la DTI, será el personal de Soporte Informático y la Unidad de Operaciones Informáticas respectivamente, quienes deberán mantener actualizado el registro y control del acceso al Centro de Cómputo de la DTI y a los cuartos de servidores de las Oficinas Departamentales.

Art 11. CONTROL DE ACCESO AL CENTRO DE CÓMPUTO DE LA DTI Y A LOS CUARTOS DE SERVIDORES DE LAS OFICINAS DEPARTAMENTALES

11.1. El Centro de Cómputo de la DTI y los cuartos de servidores de las Oficinas Departamentales deben cumplir las condiciones mínimas de protección contra amenazas tales como: Problemas de alimentación eléctrica y enfriamiento, errores humanos o actividades maliciosas e Incendios.

11.2. Para contrarrestar estas amenazas, debe existir el monitoreo regular por medio de capacidades integradas en los dispositivos de alimentación, enfriamiento y extinción de incendios.

11.3. El acceso al Centro de Cómputo de la DTI y a los cuartos de servidores de las Oficinas Departamentales es únicamente para personal de la DTI y personal autorizado por ésta, ya que se consideran áreas seguras y su acceso es restringido, dicho acceso debe ser cancelado inmediatamente a aquellas personas que dejen de tener una relación contractual con el CNR.

11.4. Se consideran "visitantes" a todas aquellas personas internas o externas a la institución cuyos servicios sean requeridos para realizar cualquier tipo de trabajo dentro del Centro de Cómputo de la DTI o en los cuartos de servidores de las Oficinas Departamentales y que no cuenten con autorización previa para ingresar a los mismos.

11.5. Se debe comunicar con anticipación a los Soportes Informáticos o al personal de la Unidad de Operaciones Informáticas cuando personal ajeno a la institución necesite ingresar al Centro de Cómputo de la DTI o a los cuartos de servidores de las Oficinas Departamentales, salvo en caso de emergencias.

11.6. Debe registrarse en el formato de control de acceso correspondiente, todo el personal autorizado que por motivos de trabajo requiera ingresar al Centro de Cómputo de la DTI o a los cuartos de servidores de las Oficinas Departamentales.

11.7. Los visitantes al Centro de Cómputo de la DTI o a los cuartos de servidores de las Oficinas Departamentales sólo tendrán acceso para propósitos específicos. Las visitas deben ser supervisadas por el personal interno autorizado por la DTI, mientras dure su estadía y debe quedar evidencia en un registro que incluya la fecha, nombre, hora de entrada y salida, así como el propósito de la visita.

11.8. Si los visitantes necesitan utilizar dispositivos móviles dentro del Centro de Cómputo de la DTI o de los cuartos de servidores de las Oficinas Departamentales, se debe justificar su uso y debe ser verificado previamente por los Soportes Informáticos o el personal de la Unidad de Operaciones Informáticas, quienes son los responsables de garantizar la ausencia de amenazas y el correcto uso de los mismos.

11.9. En ausencia de personal responsable del Centro de Cómputo de la DTI o los cuartos de servidores de las Oficinas Departamentales, estos lugares deben permanecer cerrados con llave.

CAPÍTULO III
NORMATIVA DE ADMINISTRACIÓN DE CARPETAS PARA EL ALMACENAMIENTO DE ARCHIVOS INSTITUCIONALES DE LOS USUARIOS INFORMÁTICOS DEL CNR

Art 12. OBJETO

Facilitar el almacenamiento y resguardo de los archivos de carácter institucional generados por los usuarios internos de los servicios informáticos del Centro Nacional de Registros (CNR).

Art 13. SUJETOS DE LA NORMATIVA

13.1. El personal de la Unidad de Administración de Servidores son los responsables de crear y administrar los usuarios, los recursos compartidos, servicios y permisos requeridos por las unidades solicitantes.

13.2. Usuarios de red y Responsables de Unidades que utilicen archivos digitales de carácter institucional.

Art 14. SUMINISTRO DEL SERVICIO

Considerando que todos los datos relacionados con el trabajo institucional contenidos en cualquier computadora propiedad del CNR, deberán ser almacenados en un servidor de archivos. La DTI habilitará y pondrá a disposición de los usuarios internos el servicio de almacenamiento y resguardo de archivos de carácter institucional.

Art 15. ADMINISTRACIÓN DE CARPETAS DE USUARIO

15.1 CREACIÓN

El personal de la Unidad de Administración de Servidores a solicitud de las Direcciones y/o Jefaturas del CNR, mediante un requerimiento, procederá a:

15.1.1 Crear la carpeta del usuario y asignarlo a la Unidad Organizacional correspondiente.

15.1.2 Asignar a la carpeta los permisos solicitados según lo establecido en el numeral 164.

15.2 ELIMINACIÓN DE CARPETAS DE USUARIOS

15.2.1 En caso de existir la necesidad de eliminar una carpeta perteneciente a un usuario, el Titular de la Unidad Administrativa correspondiente, deberá revisar y reasignar a otros empleados los archivos institucionales relevantes contenidos en la carpeta a eliminar.

15.2.2 El Titular de la Unidad Administrativa debe solicitar mediante un requerimiento la eliminación de la carpeta del usuario.

15.3 PERMISOS

15.3.1 El personal de la Unidad de Administración de Servidores asignará a la carpeta del usuario los permisos de acuerdo a lo solicitado por el Titular de la Unidad Administrativa correspondiente.

15.3.2 Los accesos a carpeta que no pertenezcan al usuario deberán ser aprobados por el titular o dueño de la información.

15.3.3 La modificación y eliminación de permisos o roles asignados a los usuarios y/o carpetas, solo podrán realizarse previamente con el requerimiento remitido por los Titulares de las Unidades Administrativas correspondientes.

Art 16. RESPALDO DE CARPETAS

16.1. Se incluirán, en los procedimientos de respaldo de información, las carpetas del usuario y de las unidades administrativas.

16.2. El personal de la Unidad de Administración de Servidores, deberá comunicar mediante un requerimiento al Técnico de Resguardo de Datos las adiciones, modificaciones o eliminaciones de carpetas para que sean tomadas en cuenta en los respectivos respaldos, otorgándole al mismo tiempo los permisos necesarios para la realización de dicha tarea.

16.3. La información contenida en las computadoras personales no será respaldada de forma automática; es responsabilidad del usuario trasladar la información de carácter institucional a la carpeta correspondiente del servidor asignado.

Art 17. MONITOREO DEL SERVICIO DE ADMINISTRACION DE CARPETAS

El personal de la Unidad de Administración de Servidores es el responsable de monitorear de manera periódica el servicio de administración de carpetas, a fin de prevenir la saturación de la capacidad y tipos de archivos almacenados, así como modificaciones no autorizadas de permisos asignados a usuarios en determinadas carpetas.

CAPÍTULO IV
NORMATIVA DE SEGURIDAD PARA LA ADMINISTRACIÓN DE SERVIDORES

Art 18. OBJETO

Normar la administración de servidores institucionales del CNR.

Art 19. SUJETOS DE LA NORMATIVA.

El personal de la Unidad de Administración de Servidores, Administradores de Servidores de Aplicación, Administradores de Bases de Datos, Administradores de Respaldo de Datos, Administradores de Redes y Soportes Informáticos Departamentales, son los responsables de la administración de todos los servidores de la Institución.

Art 20. CONFIGURACIÓN DE SERVIDORES.

20.1. El personal de la Unidad de Administración de Servidores es el responsable de que los servidores a su cargo cumplan con el protocolo de endurecimiento autorizado de servidores.

20.2. Todos los servidores deberán estar asignados al segmento de red autorizado.

20.3. Las contraseñas de administración de servidores deberán cumplir con el Art.11. CREACIÓN DE CLAVES DE ACCESO de los Controles Generales de los Recursos Informáticos, los cuales deberán ser resguardados según el artículo 32.3 RESGUARDO DE CUENTAS DE ADMINISTRADOR DE SERVIDOR del presente documento.

Art 21. ADMINISTRACIÓN DE SERVICIOS

El personal de la Unidad de Administración de Servidores, los Administradores de Servidores de Aplicación, los Administradores de Bases de Datos, Administradores de Respaldo de Datos y Administradores de red, son los responsables que los sistemas y servicios proporcionados a través de los servidores bajo su responsabilidad estén disponibles para los usuarios.

Art 22. CONTROL DE CUENTAS DE USUARIOS DE SERVIDORES

El titular de la Unidad Administrativa a la que pertenece el usuario, mediante un requerimiento, podrá efectuar las siguientes funciones relacionadas con la administración de usuarios.

22.1. CREACIÓN.
Crear la cuenta del usuario con los permisos y roles especificados en el requerimiento.

22.2. MODIFICACIÓN.
Los Administradores de Servidores podrán hacer cambios a la cuenta de usuario o a sus roles, de acuerdo a la solicitud efectuada mediante el requerimiento respectivo.

22.3. ELIMINACIÓN.
El Departamento de Recursos Humanos y/o el titular de la Unidad Administrativa mediante un requerimiento, solicita la eliminación de la cuenta/s a la Unidad de Atención al Cliente, de los usuarios retirados de la institución.

Art 23. ATENCIÓN DE FALLAS EN SERVIDORES

23.1. El personal de la Unidad de Administración de Servidores deberá dar atención inmediata en caso de presentarse fallas en cualquiera de los equipos a su cargo, salvo situaciones que salgan de su conocimiento y que por lo tanto deban ser atendidas por personal de otras áreas de la DTI o por parte de personal externo a la misma.

23.2. El acceso a los servidores deberá ser realizado únicamente por los administradores asignados o personas facultadas para realizar esta labor o que hayan sido previamente autorizadas por la DTI.

23.3. El personal de la Unidad de Administración de Servidores o el Soporte Informático Departamental, debe acompañar y supervisar al personal externo que por razones de mantenimiento tenga acceso a los servidores dentro de las instalaciones del CNR.

Art 24. MONITOREO

24.1. El personal de la Unidad de Administración de Servidores, Administradores de Servidores de Aplicación y Administradores de Bases de Datos, deberán supervisar la operación de las aplicaciones y servicio institucional en cada uno de los servidores bajo su responsabilidad, con el objeto de verificar que los servicios estén disponibles y monitorear los niveles de utilización de los recursos que son demandados por parte de las aplicaciones o servicios.

24.2. Además, deberán informar de cualquier falla o mejora necesaria con el fin de garantizar los perímetros de seguridad, con las barreras de seguridad y controles de entrada apropiados; para evitar accesos no autorizados y posibles amenazas a la integridad de la información contenida en los servidores del CNR.

CAPÍTULO V
NORMATIVA PARA EL DESARROLLO Y MANTENIMIENTO DE SISTEMAS COMPUTARIZADOS

Art 25. OBJETO

Regular la implementación de un método sistemático de elaboración y mantenimiento de sistemas computarizados.

Art 26. SUJETOS DE LA NORMATIVA.

a. Analistas Programadores.
b. Administradores de Base de Datos

Art 27. METODOLOGÍA

La metodología a utilizar para el desarrollo y mantenimiento de sistemas del CNR se encuentra normada en el documento "METODOLOGÍA PARA EL DESARROLLO Y MANTENIMIENTO DE SISTEMAS COMPUTARIZADOS" para tal fin, bajo el Código I601.

Art 28. DESARROLLO Y MANTENIMIENTO DE SISTEMAS COMPUTARIZADOS

28.1 Se debe dar cumplimiento a la Metodología para el Desarrollo y Mantenimiento de Sistemas Computarizados (I601).

28.2 Las Gerencias de Sistemas de la DTI son las responsables de revisar periódicamente la Metodología y realizar las modificaciones necesarias para mantenerla acorde a los avances tecnológicos.

28.3 Los Analistas Programadores son responsables de cumplir con la Metodología para el Desarrollo y Mantenimiento de los Sistemas Computarizados, dejando registro documentado de todo el proceso de desarrollo y mantenimiento antes mencionado.

28.4 Los Analistas y Desarrolladores de Aplicaciones tienen como función analizar, diseñar, programar y mantener los distintos sistemas de aplicación requeridos por la Institución. Su ámbito de acción se limita a los ambientes de desarrollo y pruebas. El

ambiente de producción es administrado por la Unidad de Administración de Bases de Datos y la Gerencia de Infraestructura Informática.

28.5 La puesta en producción de las aplicaciones desarrolladas y/o sus modificaciones debe efectuarse en horarios fuera de la jornada laboral o durante fines de semana. Cualquier excepción deberá ser a solicitud del Titular de la Unidad Administrativa.

28.6 Se llevará un control de incidentes, con el fin de registrarlos y clasificarlos para su posterior análisis y depuración.

28.7 Las aplicaciones deben de cumplir con la Normativa de seguridad para claves de acceso a los servicios (DTI-NS-CA-02-V1).

28.8 Las aplicaciones deben de cumplir con la Normativa para la administración de pistas de auditoría de datos críticos (DTI-NS-PA-01-V1)

CAPITULO VI
NORMATIVA PARA LA ADMINISTRACIÓN DE BASES DE DATOS

Art 29. OBJETO

Establecer un marco normativo para la administración de las Bases de Datos utilizadas en el CNR.

Art 30. SUJETOS DE LA NORMATIVA

a. Administradores de Bases de Datos

Art. 31. CLASIFICACIÓN DE USUARIOS DE BASE DE DATOS

De acuerdo a los alcances y responsabilidades dentro del sistema en sí o el comportamiento hacia una o varias aplicaciones específicas, se clasifica a los usuarios de base de datos en distintos tipos:

a. Administradores de Bases de Datos
b. Usuarios:
    - Analistas, Diseñadores y Desarrolladores de Aplicaciones
    - Soportes Informáticos
    - Usuarios finales

31.1 ADMINISTRADORES DE BASES DE DATOS:

Para el caso del CNR las bases de datos de desarrollo, pruebas y producción tienden a ser de tamaño y complejidad considerable, conteniendo una gran cantidad de objetos de base de datos y son utilizadas por usuarios internos y externos. Por lo tanto, dichas bases de datos deben ser administradas por una o varias personas.

La Dirección de Tecnología de la Información (DTI) a través la Unidad de Administración de Bases de Datos realiza la función de administración de las bases de datos antes mencionadas.

31.2 USUARIOS:

Las cuentas de usuario, con excepción de las cuentas de los administradores de bases de datos, no deberán tener permisos de administración, modificación o eliminación de objetos de base de datos en ambiente de producción y los permisos antes mencionados deben ser controlados en los ambientes de desarrollo y pruebas.

31.2.1 Usuarios Finales: Los usuarios finales interactúan con las bases de datos a través de los aplicativos o programas desarrollados y proporcionados por la DTI.

Las responsabilidades típicas de los usuarios finales incluyen:

a) Consulta, digitación, modificación y/o eliminación de datos donde sea permitido, según las normas de seguridad de la aplicación y los roles y permisos asignados al usuario.
b) Generación de reportes predefinidos
c) Ejecución de procedimientos almacenados predefinidos

Los usuarios finales se clasifican de la siguiente forma:

a) Usuarios Internos: empleados del CNR, identificados por su número de carnet.
b) Usuarios Externos: todo aquel usuario ajeno al CNR, como clientes, contratistas, empleados de instituciones con las que se tengan convenios y/o contratos, y que estén debidamente autorizados por la institución para acceder a los servicios de información de la misma.

Art. 32. ADMINISTRACIÓN DE CUENTAS

32.1 CUENTA DE ADMINISTRADOR DE BASE DE DATOS

32.1.1 Las cuentas con capacidades para manejar los permisos requeridos para crear o eliminar usuarios de bases de datos serán manejadas por la Unidad de Administración de Bases de Datos.

32.1.2 Debe existir al menos un Administrador de Bases de Datos quién será responsable del mantenimiento y seguimiento de todos los aspectos de las políticas y normativas de seguridad de bases de datos como de la administración de usuarios.

32.1.3 Los Administradores de Base de Datos deben tener permisos de administración del sistema operativo de los servidores de bases de datos, tanto en la consola local como para acceso remoto.

32.1.4 Los Administradores de Base de Datos son responsables de mantener las cuentas de usuario personalizadas en la base de datos para que los programadores puedan realizar la función de soporte al usuario y así evitar el uso de cuentas genéricas.

32.2 CUENTAS DE USUARIO DE BASES DE DATOS

32.2.1 La cuenta de usuario asignada a una persona representa su identidad en el sistema, por lo que todas las acciones realizadas utilizando dicho usuario serán responsabilidad directa de la persona.

32.2.2 Creación, Modificación o Eliminación de Usuarios de Bases de Datos debe solicitarse mediante un requerimiento y anexando el formulario controlado F0227.

32.2.3 Autenticación de Usuarios: Los usuarios de Base de Datos deben ser autenticados en la aplicación o la base de datos a través de una clave de acceso. Se debe cumplir con los lineamientos de la Normativa para Claves de Acceso a los Servicios Informáticos del CNR. Dichas claves de acceso son personales, secretas, intransferibles y definidas por el usuario propietario de la misma.

32.3 RESGUARDO DE CUENTAS DE ADMINISTRADOR DE SERVIDOR

32.3.1 El Supervisor de Seguridad en Tecnología de la Información debe resguardar las claves de Administrador de las Bases de Datos y de los Servidores en sobre cerrado y sellado.

32.3.2 Se deben mantener dos juegos de sobres conteniendo las claves, uno para ser almacenado en caja de seguridad de la DTI y el otro bajo la custodia de Dirección Ejecutiva

32.3.3 Las claves de Administrador de las Bases de Datos y Servidores se deben cambiar al menos una vez al año o cuando la contraseña haya sido comprometida. Por lo tanto, se deben actualizar las claves en los sobres, dejando registro de dicha actualización.

32.3.4 En casos de fuerza mayor, se podrán abrir los sobres por el personal que debe cubrir la emergencia, dejando registro de las causas que dieron origen a su apertura.

32.3.5 Después de la emergencia, se deben actualizar las claves y almacenar las nuevas en los sobres sellados para su almacenamiento y custodia.

32.3.6 La Unidad de Auditoría Interna es responsable de certificar el sello de los sobres y su contenido.

Art. 33. ADMINISTRACION DE OBJETOS

33.1 La seguridad a nivel de datos en general debe estar basada en la sensibilidad de los datos mismos, y en los requerimientos de cada aplicación. Para datos considerados sensibles, se debe cumplir con los lineamientos de la Normativa de Seguridad para la Administración de Pistas de Auditoria de Datos Críticos del CNR.

33.2 Las Gerencias de Sistemas diseñarán el esquema de seguridad para cada aplicación, esto incluye la definición de roles y la asignación de derechos a nivel de objeto para cada rol.

33.3 El esquema de seguridad de la aplicación será implementado por la Unidad de Administración de Bases de Datos, según los requerimientos específicos de seguridad para cada caso.

33.4 Como parte del proceso de implementación de un sistema de aplicación, la Unidad de Administración de Bases de Datos asignará los roles definidos a

usuarios específicos según el requerimiento debidamente autorizado por el titular de la Unidad Administrativa solicitante.

33.5 El diseño de cada aplicación debe incluir como parte importante de la seguridad de datos, todas aquellas bitácoras, registros históricos y de auditoría de datos que sean necesarios.

Art. 34. MANTENIMIENTO DE LA BASE DE DATOS

34.1 Se debe dar cumplimiento a la Normativa de Seguridad para la Administración de Servidores para garantizar el buen funcionamiento de los Servidores en donde residen las bases de datos.

34.2 Se deberá mantener los respaldos necesarios para recuperar el buen funcionamiento de las Bases de Datos en caso de fallas.

34.3 La Unidad de Administración de Bases de Datos deberá registrar y documentar la configuración y actualizaciones realizadas a las Bases de Datos, así como la gestión de cambios de estructuras.

34.4 La Unidad de Administración de Bases de Datos es responsable de llevar registro de los incidentes que se presenten, así como de las medidas tomadas para resolver dichos incidentes.

Art. 35. MONITOREO

35.1 La Unidad de Administración de Bases de Datos debe verificar periódicamente el uso de los recursos y servicios habilitados de las Bases de Datos.

35.2 La Unidad de Administración de Bases de Datos es responsable de llevar registro del estado de los recursos y en caso de detectar algún indicador anormal, efectuar su análisis y corrección de dicha situación.

CAPÍTULO VII
NORMATIVA PARA LA ADMINISTRACIÓN DE PISTAS DE AUDITORÍA DE DATOS CRÍTICOS DEL CNR

Art. 36. OBJETO

Definir y documentar los mecanismos de administración y control de las pistas de auditoría de cambios efectuados sobre datos críticos del CNR.

Art. 37. SUJETOS DE LA NORMATIVA

Todo el personal relacionado con el manejo de datos considerados críticos por la organización, ya sea a través de aplicaciones o accesos directos a las bases de datos, imágenes y/o mapas catastrales.

Art. 38. DEFINICIÓN DE DATOS CRÍTICOS

La Dirección o sustantiva propietaria de los datos que se generan y administran bajo su responsabilidad, junto con la Dirección de Tecnología de la Información, debe definir cuáles son los datos considerados como críticos y el tipo de control a implementar.

Art. 39 PISTAS DE AUDITORÍA

39.1 La DTI, a través de las Gerencias de Sistemas, es responsable de definir técnicamente el método de registro de cambios o pistas de auditoría sobre la base de la definición de los datos críticos.

39.2 Los Administradores de Bases de Datos (DBA) son responsables de implementar y monitorear el método previamente definido y documentado, que tenga como resultado el registro de los cambios en un archivo independiente de la base de datos donde se encuentra el dato crítico.

39.3 Serán las pistas de auditoría el mecanismo a utilizar para definir responsabilidades sobre el uso de la información, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información almacenada en los servidores del CNR.

Art. 40. REPOSITORIO HISTÓRICO

El repositorio tendrá un tiempo de retención de los registros en línea de un año, luego de esto se pasarán a medios de almacenamiento secundario.

Art. 41. MONITOREO

Los Administradores de Bases de Datos (DBA) son responsables de monitorear periódicamente:

a. El tamaño de los archivos de registro
b. La realización efectiva de los traslados hacia el repositorio histórico

Art. 42. AUDITORÍAS

Auditoría Interna y cualquier otra instancia que la Dirección Ejecutiva autorice, tendrá acceso al repositorio histórico para realizar consultas y auditorías sobre los cambios realizados en los datos críticos del CNR.

CAPITULO VIII
PROHIBICIONES

Se prohíbe la toma de fotografías y videos de los cuartos de servidores a nivel nacional sin previa autorización

Se prohíbe el almacenamiento de fotografías, videos, música, películas, juegos y datos personales dentro de ninguno de los servidores propiedad del CNR, salvo que dichos archivos pertenezcan al CNR y formen parte de sus activos de información.

CAPÍTULO IX
SANCIONES

El incumplimiento de las obligaciones y la violación de las prohibiciones establecidas en el presente Marco Normativo, hará incurrir al usuario infractor en las sanciones dispuestas en el Reglamento Interno de Trabajo del CNR, las cuales serán impuestas conforme al procedimiento establecido en la Cláusula No. 41 del Contrato Colectivo de Trabajo.

La aplicación de tales sanciones se efectuará sin perjuicio de la responsabilidad penal que pueda corresponder al usuario infractor, o de la civil que pueda caberle para la satisfacción y pago de los daños y/o costos, que sus actos u omisiones hayan causado al CNR o a terceros, por cualquier concepto.

CAPITULO X
DIVULGACIÓN

La DTI será responsable que los Controles Específicos de los Recursos Informáticos del CNR, sean hechas del conocimiento de los usuarios.

Se garantizará de ello utilizando los medios y recursos que estime convenientes, entre ellos, el de su puesta a disposición en la Intranet.

CAPITULO XI
VIGENCIA

El presente Marco Normativo de Controles Específicos de Recursos Informáticos del CNR, entrará en vigencia a partir de la aprobación por parte del Consejo Directivo.