REGISTRADURÍA
NACIONAL DEL ESTADO CIVIL

RESOLUCIÓN No. 4173 DE 2016
20 MAYO 2016

Por la cual se derogan las Resoluciones 13829 de diciembre 12 de 2011 y 9025 de octubre 30 de 2012, generando nuevas Políticas de Seguridad de la Información

EL REGISTRADOR NACIONAL DEL ESTADO CIVIL

En ejercicio de las atribuciones establecidas en el artículo 25 del Decreto 1010 de 2000, y

CONSIDERANDO

Que, las Políticas de Seguridad de la Información son objeto de actualización y para su elaboración metodológica se tuvo en cuenta cada uno de los 14 dominios, con sus respectivos objetivos de control, los cuales se encuentran identificados en en el estándar ISO/IEC 27001 de 2013.

Que, la Registraduría Nacional del Estado Civil identifica la información como un componente indispensable para sus funciones, razón por la cual se deben establecer unas políticas, estrategias y acciones que aseguren que la información sea protegida de una manera adecuada, independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.

Que, en esta resolución se describen las políticas y normas de seguridad de la información definidas por la Registraduría Nacional del Estado Civil, las cuales se constituyen como bases para la creación del Sistema de Gestión de Seguridad de la RNEC.

Que, la Seguridad de la Información es una prioridad para la Registraduría Nacional del Estado Civil y, por tanto, es responsabilidad de todos los funcionarios, proveedores y colaboradores velar por que no se realicen actividades que generen vulnerabilidades sobre la información en cualquiera de las presentaciones que esta pueda tener, e independientemente de la forma que esta pueda revestir.

Que, la seguridad de la información implica procurar su protección de manera preventiva contra las amenazas o riesgos existentes que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e Integridad de la misma.

La Registraduría Nacional del Estado Civil toma como referencia las leyes y regulaciones adoptadas por el Gobierno Colombiano, entre ellas la Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales, Decreto Reglamentario 1377 de 2013, Ley 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan

otras disposiciones, Decreto Reglamentario 103 de 2015, Ley 527 de 1999 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se dictan otras disposiciones, así como las recomendaciones y buenas prácticas de los estándares adoptadas por el ICONTEC NTC/ISO 27001 y NTC/ISO 27002.

RESUELVE

ARTÍCULO PRIMERO: Derogar las resoluciones 13829 de diciembre 12 de 2011 y 9025 de octubre 30 de 2012 y formular una nueva estrategia para la Seguridad de la Información, de acuerdo con las siguientes premisas:

Los requisitos de seguridad de la información y de todos sus activos, son prioridad para la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, y por lo tanto es responsabilidad y compromiso del nivel directivo, y de todos los funcionarios de la Entidad garantizar el continuo cumplimiento de las políticas definidas en este documento.

I. OBJETIVOS

Los objetivos de este documento son:

1. Actualizar y reformular las Políticas de Seguridad de la Información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, con el fin de regular la Gestión de la Seguridad de la Información al interior de la Entidad.
2. Informar al mayor nivel de detalle a los usuarios, directivos, funcionarios y contratistas las normas y mecanismos que deben cumplir en las interacciones con los activos de información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.
3. Establecer el alcance de las responsabilidades del nivel directivo, con la participación del personal de planta, supernumerarios, provisionales, contratistas, y terceros en cuanto a la utilización y mantenimiento confidencial e íntegro de la información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.

II. ALCANCE

Las Políticas de Seguridad de la Información cubren los aspectos de privacidad, acceso, autenticación, mantenimiento y divulgación relacionados con cualquier activo de información, que conllevan a disponer guías y controles que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros, que laboren o tengan relación con la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, para alcanzar un adecuado nivel de protección en cuanto a confidencialidad, integridad y disponibilidad de la información.

Este documento debe ser de conocimiento de todos los funcionarios de la Registraduría Nacional del Estado Civil. Así mismo, se exigirá su cumplimiento en los procesos de contratación de la entidad, y su lectura debe ser requisito necesario antes de realizar cualquier proceso de contratación.

La Alta Dirección de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL será responsable de facilitar los recursos humanos, técnicos, financieros y demás necesarios para llevar a cabo la implantación, control y auditoría de estas políticas.

№ 4173

III. MARCO TEÓRICO

20 MAYO 2016

ISO/IEC 27001 es la única norma internacional auditable que define los requisitos necesarios para establecer, implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI), la norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales. El SGSI permite evaluar cuáles son los riesgos a los que se expone la información relevante e importante para las organizaciones, la cual es fundamental para el normal proceder de sus funciones y a su vez implementar los controles adecuados y necesarios para mantener la confidencialidad, integridad y disponibilidad de los activos de información identificados dentro de la operación de la organización.

La norma ISO/IEC 27001 contiene una serie de controles divididos en catorce (14) dominios, así:

1. Política de Seguridad: Se estipulan las políticas con respecto a la seguridad de la información para la Registraduría Nacional del Estado Civil.

2. Organización de la Seguridad de la información: Agrupa los temas de administración de la seguridad dentro de la organización (roles, compromisos, autorizaciones, acuerdos, manejo con terceros).

3. Seguridad de los Recursos Humanos: Temas para asegurar que empleados, contratistas y terceros entiendan sus responsabilidades y sus roles sean adecuados para su desempeño, minimizando los riesgos relacionados con personal. Incluye los procesos para antes de la Contratación, durante y por cese o cambio de puesto de trabajo.

4. Gestión de Activos: Trata sobre la responsabilidad de los activos, clasificación de la información y manejo de los soportes de los mismos.

5. Control de Acceso: Requisitos de negocio para el control de acceso, gestión de acceso de los usuarios, responsabilidades del usuario, control de acceso a sistemas y aplicaciones.

6. Cifrado: Relativo a los controles criptográficos en los activos de la información.

7. Seguridad Física y Ambiental: Pretende prevenir accesos físicos no autorizados (perímetro), daños o interferencias a las instalaciones de la organización y a su información.

8. Seguridad en la operación tecnológica: Responsabilidades y procedimientos de operación, protección contra código malicioso, copias de seguridad, registros de actividad y supervisión, gestión de vulnerabilidades técnicas.

9. Seguridad en las telecomunicaciones: Referente a la gestión de la seguridad en las redes e intercambio de información con partes externas.

10. Adquisición, desarrollo y mantenimiento de sistemas de información: Asegurar la inclusión de todos los controles de seguridad en los sistemas de información (infraestructura, aplicaciones, servicios, etc.). Incluye seguridad en los procesos de desarrollo de software y soporte.

11. Proveedores y Terceros: políticas de seguridad para con los terceros, tratamiento de riesgos y gestión de la prestación del servicio contratado.

12. Gestión de Incidentes de Seguridad de la información: referente a la gestión de incidentes de seguridad (notificación, valoración, respuesta a incidentes, evidencias) y proceso de mejora continua.

13. Gestión de la continuidad del negocio: enfocado hacia la continuidad de la prestación de los servicios misionales.

14. Cumplimiento: Propende por el cumplimiento de los requisitos legales, revisiones y auditoria.

IV. MARCO LEGAL

Con el objeto de mitigar los riesgos relacionados con la autenticidad, la integridad, la disponibilidad, el no repudio, la confidencialidad y la trazabilidad de la información; se tiene que cualquier incidente que viole el marco normativo legal vigente en Colombia, en materia de políticas de seguridad de la Información estará sujeto, entre otras, a lo establecido en las siguientes disposiciones legales:

1. Normatividad Especifica:
   CPC Articulo 266 Funciones de la Registraduría Nacional del Estado Civil, Decreto 1260 de 1970 Por el cual se expide el Estatuto del Registro del Estado Civil de las personas, Decreto 2246 de 1986 por el cual se adopta el Código Electoral, Decreto 1010 de 2000 De la organización interna de la Registraduría Nacional del Estado Civil.

2. Marco normativo de buenas prácticas para el tratamiento de la información:
   Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la protección de datos personales, Decreto Reglamentario 1377 de 2013, Ley 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones, Decreto Reglamentario 103 de 2015, Ley 527 de 1999 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se dictan otras disposiciones. Las recomendaciones y buenas prácticas de los estándares adoptadas por el ICONTEC NTC/ISO 27001 y NTC/ISO 27002.

3. Marco Normativo Sancionatorio:

   Ley 734 de 2002 por la cual se expide el Código Disciplinario Único.

   Ley 1273 de Enero 5 de 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

V. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

Los siguientes principios básicos fundamentan las políticas de seguridad de la información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL:

1. Disponibilidad

Los activos de información deben estar disponibles para soportar los procesos misionales de la Registraduría Nacional del Estado Civil. Deben tomarse medidas adecuadas para asegurar el tiempo de recuperación de toda la información y el acceso por personas autorizadas.

2. Integridad

Los activos de información deben estar adecuadamente protegidos para asegurar su exactitud y totalidad. Las medidas de validación definidas permitirán detectar la modificación inapropiada, eliminación o adulteración de los activos de información.

3. Confidencialidad

Debe brindar la seguridad de que la información es accesible solamente por quienes están autorizados para consultarla y utilizarla.

La información considerada de Reserva Legal de la Registraduría Nacional del Estado Civil, no podrá ser revelada y será utilizada exclusivamente para el cumplimiento de la misión institucional.

VI. VIGENCIA Y ACTUALIZACIÓN

Este documento de Políticas de seguridad de la información estará vigente a partir de su expedición y deberá tenerse en cuenta en cada uno de los contratos que la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL realice con funcionarios, contratistas, o terceros.

La actualización de este documento es responsabilidad de la Gerencia de Informática de la RNEC y debe contar con el asesoramiento y aprobación del Comité de Seguridad de la Información.

Para su actualización se tendrán en cuenta entre otros factores los siguientes:

- Actualización y/o cambios en los sistemas de información de la entidad.
- Nuevas políticas de contratación de recursos humano y de servicios
- Análisis de riesgos, incidentes de seguridad y vulnerabilidades detectadas
- Cambios dentro de la infraestructura organizacional o tecnológica.
- Cambios en los procesos, en los objetivos del sistema, o en la normatividad que afecten las políticas de seguridad.

VII. TÉRMINOS Y DEFINICIONES

Se definen a continuación los siguientes términos técnicos:

Activo: Recurso del sistema de información o cualquier elemento que tenga valor para la organización.

Activo de Información: Todo aquel elemento lógico o físico que conforme cualquiera de los sistemas de información de la institución. Ej. Bases de datos, sistemas operacionales, redes, sistemas de información y comunicaciones, documentos impresos, fichas, formularios y recursos humanos

Administrador del Sistema: Persona responsable de administrar, controlar, supervisar y garantizar la operatividad y funcionalidad de los sistemas. Dicha administración está dirigida por la Gerencia de informática y se realizará por conducto de las Coordinaciones de la misma.

En las Delegaciones Departamentales, la administración será responsabilidad del profesional designado para inspeccionar el área de sistemas.

Administrador de Correo: Persona responsable de solucionar problemas en el correo electrónico, responder preguntas a los usuarios y otros asuntos en un servidor.

ANI: Archivo Nacional de Identificación

Análisis de riesgos: Proceso sistemático que permite identificar y determinar el impacto o grado de vulnerabilidad de los activos de la organización.

Ataque Cibernético: Intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado, por lo general con intenciones insanas y perjudiciales.

Brecha de Seguridad: deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

Buzón: También conocido como cuenta de correo, es un receptáculo exclusivo, asignado en el servidor de correo, para almacenar los mensajes y archivos adjuntos enviados por otros usuarios internos o externos a la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

Centro de Cómputo: También conocido como Centro de Procesamiento de Datos, o Data Center es una instalación que se encarga del procesamiento de datos e información de manera sistematizada. El procesamiento se lleva a cabo con la utilización de computadoras (Hardware) y programas (Software) necesarios para cumplir con dicha tarea.

Centro de Acopio: Es el lugar determinado para que cada Registraduría Municipal envíe sus solicitudes de documentos (cédulas de ciudadanía y tarjetas de identidad) en donde ocurre la digitalización de las formas que se envían a las Oficinas Centrales de la Dirección Nacional de Identificación para la producción de documentos; excepcionalmente algunas Registradurías Municipales envían directamente sus solicitudes al Centro de Acopio de las Oficinas Centrales de la Dirección Nacional de Identificación

Chat: Comunicación simultánea y sincronizada entre dos o más personas a través de Internet.

Confidencialidad: Característica de la información por medio de la cual no se revela ni se encuentra a disposición de individuos, organizaciones o procesos no autorizados. La información debe ser vista o estar disponible solo a las personas autorizadas.

Control: Mecanismo para manejar el riesgo, incluyendo políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.

CSTI: Coordinación de Soporte Técnico de Identificación

Correo Electrónico: También conocido como E-mail, es un servicio de red que permite a los usuarios enviar y recibir textos, imágenes, videos, audio, programas, a través de internet.

Cuentas de Correo: Son espacios de buzones para la recepción, envío y almacenamiento de mensajes de correo electrónico en internet.

Contraseña o Password: Es una forma de autenticación privada, compuesta por un conjunto de números, letras y caracteres, que permiten al usuario tener acceso a un computador, a un archivo y/o a un programa.

Disponibilidad: Es la garantía de poder acceder a los activos de la información cuando sea necesario, por personal autorizado.

DBA: Administrador de la Base de Datos, persona cuya función radica en mantener una base de datos optimizada y disponible.

Electricidad Estática: Exceso de carga eléctrica en un objeto.

Evento de Seguridad de La Información: Ocurrencia identificada de una situación de sistema, servicio o red que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad de un activo de información.

Firma Digital: La firma digital hace referencia, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento.

Incidente de Seguridad de la Información: Es la identificación de la ocurrencia de un hecho que esta relacionado con los activos de información, que indica una posible brecha en las Políticas de Seguridad o falla en los controles y/o protecciones establecidas.

Infraestructura de Procesamiento de Información: Es cualquier sistema de procesamiento de información, servicio, plataforma tecnológica, o instalación física que los contenga.

Firewall: Dispositivo que permite bloquear o filtrar el acceso en redes de comunicación.

Hacker: Persona dedicada a realizar entradas no autorizadas a los sistemas, por medio de redes de comunicación como Internet, con el objeto de alterar en forma nociva su funcionamiento.

Host: Término usado en informática para referirse a los computadores conectados a la red, que proveen y/o utilizan servicios de ella. Los usuarios deben utilizar hosts para tener acceso a la red

Integridad: La propiedad de salvaguardar la exactitud y completitud de los activos de información.

Internet: Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse entre sí.

Intranet: Red privada dentro de una empresa, que utiliza el mismo software y protocolos empleados en la Internet global, pero que es de uso interno.

LAN: (Local Area Network). (Red de Área Local). Red de computadoras ubicadas en el mismo ambiente, piso o edificio.

Messenger. Mensajería instantánea disponible en Internet.

PMT: Proyecto de Modernización Tecnológica de la RNEC.

Política: Son instrucciones mandatarias que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños

Red: Se tiene una red, cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos.

Riesgo residual: Es el riesgo remanente, después de la implantación de las medidas de seguridad determinadas en el plan de seguridad de la información.

Sistema de Gestión de Seguridad de la Información: SGSI La parte del sistema total de gestión, basada en un enfoque de riesgo de negocios, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Seguridad: Mecanismos de control que evitan el uso no autorizado de recursos.

Seguridad de la Información: Son medidas preventivas que incluyen factores de confidencialidad, integridad, disponibilidad, autenticidad, responsabilidad, aceptabilidad y confiabilidad de la información.

Servidor: Computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red.

Servidor de Correo: Dispositivo y/o aplicación informática, cuya función es gestionar el tráfico de ficheros a través del correo electrónico, su misión es la de almacenar, en su disco duro, los mensajes que envía y que reciben los usuarios.

SO: (Sistema Operativo). Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora

Terceros: Se entiende por tercero a toda persona, jurídica o natural ajena a la RNEC, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

Virus: Software malicioso que tiene por objeto alterar el normal funcionamiento de una computadora, reemplazando así programas ejecutables, sin la autorización ni el conocimiento del usuario.

VIII. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Acorde con la metodología definida en la norma NTC-ISO-IEC 27001 de 2013, la Registraduría Nacional del Estado Civil adopta las siguientes políticas de seguridad de la Información.

1. Políticas de seguridad de la información
2. Organización de la seguridad de la información
3. Seguridad de los recursos humanos
4. Gestión de activos de información
5. Control de acceso.
6. Cifrado.
7. Seguridad física y ambiental
8. Seguridad en la operación
9. Seguridad en las telecomunicaciones
10. Adquisición, desarrollo y mantenimiento de los sistemas de información.
11. Relación con Proveedores y Terceros.
12. Gestión de incidentes de seguridad
13. Gestión de la continuidad del negocio
14. Cumplimiento.

Existirá un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información (SGSI).

Los activos de información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, serán identificados y clasificados para establecer los mecanismos de protección necesarios.

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL definirá e implantará controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los ciudadanos y usuarios de los servicios ofrecidos.

Todos los funcionarios y/o terceros contratados serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

Se realizarán auditorías y controles periódicos sobre el modelo de gestión de Seguridad de la Información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL solo permitirá el uso de software autorizado que haya sido adquirido legalmente.

Es responsabilidad de funcionarios y/o terceros contratados por REGISTRADURÍA NACIONAL DEL ESTADO CIVIL reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

Las violaciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL contará con un Plan de Continuidad que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales.

1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

REF: ISO/IEC/ 27001 CL. A.5

La información es un activo fundamental para la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL. Por tanto, la entidad está comprometida con la protección de su confidencialidad, integridad y disponibilidad. Todo esto como parte de una estrategia orientada al cumplimiento de sus procesos misionales y a la continuidad del negocio, entendiendo como tal los procesos de identificación, el proceso electoral, la administración de riesgos y la consolidación de una cultura de seguridad.

Para dar cumplimiento a nuestra misión[1], la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL ha implantado las políticas de seguridad que a continuación se mencionan, en la cual se definen directrices claras, acordes con los objetivos institucionales, en cuanto a los procesos administrativos, de identificación y realización de eventos electorales. Estas políticas se encuentran ajustadas a los cambios tecnológicos y marcos jurídicos vigentes de orden legal y constitucional.

El propósito de estas políticas es definir el ambiente en el cual la información será protegida contra amenazas, internas o externas, intencionales o accidentales, en las diferentes formas en las cuales se pueda encontrar la información.

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL elaborará planes y acciones específicas de manera que se minimice la ocurrencia y el impacto de incidentes de seguridad de la información.

REGULACIÓN

Las políticas contenidas en este documento deberán ser conocidas, aceptadas y cumplidas por todos los funcionarios, proveedores, contratistas y terceros de la

[1] Es misión de la Registraduría Nacional del Estado Civil, garantizar la organización y transparencia del proceso electoral, la oportunidad y confiabilidad de los escrutinios y resultados electorales, contribuir al fortalecimiento de la democracia mediante su neutralidad y objetividad, promover la participación social en la cual se requiere la expresión de la voluntad popular mediante sistemas de tipo electoral en cualquiera de sus modalidades, así como promover y garantizar en cada evento legal en que deba registrarse la situación civil de las personas, que se registren tales eventos, se disponga de su información a quien deba legalmente solicitarla, se certifique mediante los instrumentos idóneos establecidos por las disposiciones legales y se garantice su confiabilidad y seguridad plenas".

REGISTRADURÍA NACIONAL DEL ESTADO CIVIL. El incumplimiento de las mismas se considerará un incidente de seguridad que, de acuerdo con el caso, podrá dar lugar a un proceso disciplinario para los funcionarios y se convertirá en una causa válida de terminación del contrato con los contratistas, sin perjuicio de la iniciación de otro tipo de acciones a las que hubiere lugar.

Cada usuario será responsable por todas las actividades realizadas con los activos de la información que están a su cargo y custodia, o desde las cuentas asignadas para su acceso a los servicios informáticos de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.

Son actos no autorizados en el uso de los activos informáticos de la Registraduría Nacional del Estado Civil:

A. El intento o violación de los controles de seguridad establecidos para la protección de los activos de la información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

B. Realizar cualquier actividad que pudiera comprometer la seguridad de cualquier activo de la información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

C. El uso sin autorización de los activos de la información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.

D. El uso no autorizado o impropio de la conexión al Sistema.

E. Intentar evadir o violar la seguridad o autenticación de usuario de cualquier host, red o cuenta.

F. El uso indebido de las contraseñas, firmas digitales o dispositivos de autenticación.

G. El acceso a servicios informáticos utilizando cuentas o medios de autenticación de otros usuarios. Aún con la autorización expresa del usuario propietario de la misma.

H. El uso, distribución y ejecución de software o código malicioso que cause daño, hostigamiento, molestias a personas, daño o alteración de información o traumatismos en la continuidad de los servicios informáticos o vulnere la seguridad de los sistemas.

I. El hurto, robo, sustracción o uso no autorizado de datos, información, materiales, equipos y otros elementos pertenecientes a los activos de la información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

J. El retiro de las instalaciones de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL o áreas bajo su administración o control, de cualquier activo de la información sin autorización previa.

K. El acceso, modificación o alteración no autorizada de componentes, datos o información de los activos de la información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

L. El uso de medios electrónicos, medios de almacenamiento, software, hardware, datos o información en medios digitales provenientes de fuentes no certificadas o de terceros, sin la previa revisión y autorización del Administrador del Sistema.

M. El uso con fines no autorizados o ilegales del Servicio de Internet

N. La transmisión, difusión o almacenamiento de cualquier material digital o impreso en

violación de cualquier ley o regulación aplicable. Esto incluye, sin limitación alguna, todo material protegido por los derechos de autor, marcas, secretos comerciales u otros derechos de propiedad intelectual usados sin la debida autorización, y todo material obsceno o pornográfico, difamatorio.

O. La realización por Internet, o a través de los activos informáticos, de cualquier actividad que pudiera potencialmente traer desprestigio a la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

P. Los mensajes contenidos en los correos electrónicos que sean contrarios a las disposiciones del orden Público, la moral, las buenas costumbres nacionales e internacionales y a los usos y costumbres aplicables en Internet, así mismo, que sean contrarios al respeto por los derechos de terceras personas.

Q. El almacenamiento y reproducción de aplicaciones, programas o archivos de audio ó vídeo que no están relacionados con las actividades propias de las funciones que cumple la dependencia o el usuario.

R. Cualquier violación o sospecha de violación de las medidas o controles de seguridad de los sistemas de información, o de las políticas de seguridad de la información de LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, debe ser reportada inmediatamente por quien conozca de ellas al comité de Seguridad de la Información.

2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

REF: ISO/IEC 27001/:2013 A.6

COMPROMISO INSTITUCIONAL DE LA DIRECCIÓN

El Registrador Nacional del Estado Civil, los Registradores Delegados, los Gerentes y el personal Directivo de la Entidad deben apoyar activamente la seguridad de la información dentro de la organización como muestra de su compromiso en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información. Este compromiso se verá reflejado a través de:

a. La aprobación del Manual de Políticas de Seguridad de la Información.
b. La aprobación de un Comité de Seguridad de la Información.
c. La aprobación para la divulgación de este manual a todos los funcionarios de la Organización.
d. Velar por el cumplimiento de las políticas de seguridad de la información.

COORDINACION DE LA FUNCION DE SEGURIDAD DE LA INFORMACIÓN

Las actividades de la seguridad de la información deben ser coordinadas por representantes de las áreas de la organización con roles y funciones relevantes. LA REGISTRADURÍA NACIONAL DEL ESTADO CIVIL creó mediante la Resolución 13860 de 2011 el Comité de Seguridad de la Información (CSI), modificada por la Resolución 4154 del 19 de mayo de 2016 y que está conformado por el siguiente grupo de directivos:

a. Registrador Nacional del Estado Civil o su delegado
b. Gerente Administrativo y Financiero
c. Gerente de Informática.
d. Gerente de Gestión Humana
e. Registrador delegado en lo electoral o su delegado
f. Registrador delegado para el Registro Civil y la Identificación o su delegado
g. Jefe de la Oficina de Control Interno o su delegado

h. Jefe de la Oficina de Planeación o su delegado.
i. Jefe de la Oficina Jurídica
j. Asesor del Despacho asignado a la Gerencia de Informática.

FUNCIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

a. Proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como las bases de datos e información en general.
b. Revisar el estado general de la seguridad de la información.
c. Revisar y analizar los incidentes de seguridad de la información existentes.
d. Revisar y aprobar los proyectos de seguridad de la información.
e. Aprobar las modificaciones o nuevas políticas de seguridad de la información.
f. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
g. Identificar necesidades de evaluación de los procesos soportados por los recursos informáticos y su plataforma tecnológica.
h. Realizar otras actividades inherentes a la naturaleza del comité relacionadas con la seguridad de la información.

RESPONSABILIDADES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN.

a. Responsables del análisis, revisión y centralización de todas las acciones referidas a la gestión de Seguridad de la Información de la organización y de mantener la vigencia de las políticas de acuerdo con las necesidades y requerimientos del negocio.

b. Asegurar que exista una dirección y apoyo gerencial sobre los principios y las metas para soportar la administración y desarrollo de iniciativas sobre la gestión de la seguridad de los activos de la información, a través de compromisos apropiados y de recursos adecuados, como la formulación y mantenimiento de las políticas de seguridad de la información a través de todos los funcionarios de la organización.

c. Validar las políticas de seguridad de la información y procedimientos para el uso adecuado y administración de los recursos informáticos asignados a los funcionarios de la organización, asegurando que la información se encuentre protegida.
d. Impulsar la implementación del Sistema de Gestión de Seguridad de la Información —SGSI.

Procesos de Autorización para instalaciones de procesamiento de información (ISO/IEC 27001 27001 CL. A.6)

Cuando se inicie el trámite para la adquisición de una nueva infraestructura de procesamiento de información (hardware, software, aplicaciones) o la actualización de la existente, debe ser consultada y autorizada por el Gerente de Informática.

No se permite el almacenamiento y/o procesamiento de información de propiedad de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL en equipos o dispositivos de propiedad de los funcionarios, o contratistas, a menos que cuente con la autorización del Comité de Seguridad de la Información. La autorización se tramitará a través de una solicitud que se debe presentar mediante oficio donde se justifique la necesidad de almacenar y/o procesar información de propiedad de la Registraduría Nacional del Estado Civil en equipos diferentes a los activos de la Entidad.

Convenios de confidencialidad

Para todos los contratos de prestación de servicios, La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, hará firmar al personal que por razón de su cargo o funciones acceda información considerada confidencial para la entidad, un acuerdo de

confidencialidad o de no divulgación que reflejen las necesidades de la organización para protección de la misma, no permitiendo tal acceso al resto del personal.

Los contratistas, deben comprometerse para con la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, a que el uso que le dé a dicha información debe corresponder a las obligaciones que desempeña y como también se obligará a mantener la reserva que corresponda para su manejo y divulgación, so pena de las sanciones legales a que haya lugar.

Todos los funcionarios y contratistas que manejen información confidencial, deben firmar la cláusula y/o acuerdo de confidencialidad definido por la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL y este debe ser parte integral de cada uno de los contratos.

Este requerimiento también se debe aplicar para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos de la institución por parte de personas o entidades externas.

Contacto con las Autoridades

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL establecerá y mantendrá un plan de emergencias que describe la relación cercana con autoridades relevantes (policía, bomberos, defensa civil), para que puedan ser contactados de manera oportuna en el caso de que se presente situaciones de emergencia o incidente de seguridad que ameriten el uso de estas autoridades.

Auditorías Internas

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL realizará revisiones internas a su Gestión de Seguridad de la Información con el fin de determinar si las políticas, procesos, procedimientos y controles establecidos dentro del sistema de gestión de seguridad de la información, están conformes con los requerimientos institucionales, requerimientos de seguridad, regulaciones aplicables, y si éstos se encuentran implementados y mantenidos eficazmente. Estas auditorías se ejecutan según lo establecido en el programa de auditorías definido por La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL y, en caso de ser necesario, se podrán programar revisiones parciales o totales sobre un proceso o área.

Revisión independiente de la Seguridad de la Información

El Comité de Seguridad de la información será responsable de garantizar que se realicen revisiones periódicas a las Políticas de Seguridad de la Información, según el procedimiento que se defina para tal fin, con el objeto de verificar su vigencia, su correcto funcionamiento y su efectividad.

Riesgos relacionados con Terceros

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL debe identificar los posibles riesgos que pueden generar el acceso, procesamiento, comunicación o gestión de la información y la infraestructura para su procesamiento, en forma independiente y de acuerdo al contrato o servicio que se preste por parte de los terceros, con el fin de establecer los mecanismos de control necesarios para controlar la seguridad de la información.

Los controles que se establezcan como necesarios a partir del análisis de riesgos, deben ser comunicados y aceptados por el tercero mediante la firma de acuerdos, previamente a la entrega de los accesos requeridos.

Los contratos que se firmen con terceros, en los que se tiene acceso a recursos informáticos, deben hacer referencia expresa a la aceptación de las políticas de seguridad.

3. SEGURIDAD DE LOS RECURSOS HUMANOS

Ref: ISO/IEC 27001/2005 CL. A.7.

Funciones y Responsabilidades

Todos los funcionarios de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, sus proveedores o contratistas, así como los terceros autorizados para acceder a la infraestructura de procesamiento de información, serán responsables del cumplimiento de las políticas, procedimientos y estándares definidos por la Entidad.

La información almacenada en los equipos de cómputo de la Entidad es propiedad de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad.

Se prohíbe la realización de actividades tales como borrar, alterar o eliminar información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL de manera malintencionada, por parte de los funcionarios y/o contratistas.

Todos los funcionarios y contratistas de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL deberán mantener especial cuidado de no divulgar información reservada en lugares públicos o privados, mediante conversaciones o situaciones que puedan comprometer la seguridad o el buen nombre de la organización. Esta restricción se extiende inclusive con posterioridad a la terminación de los contratos, y estará incluida en las condiciones de los mismos.

Tamizaje (Investigación de Antecedentes- Contratación de personal) (ISO/IEC 27001 CL. A.7.1.1)

Todos los procesos de contratación deberán cumplir con los requerimientos propios del cargo descritos en el *"Manual de Funciones"*.

Términos y condiciones del empleo (ISO/IEC 27001 CL. A.7.1, 2 y 3)

Todos los funcionarios y contratistas de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL deberán cumplir con los siguientes requerimientos de seguridad de la información:

A. Firmar acuerdo de confidencialidad.

B. Leer las políticas de Seguridad de la Información y firmar la aceptación de las mismas.

Todos los funcionarios, durante el proceso de vinculación a la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, deberán recibir una inducción sobre las Políticas de Seguridad de la Información de la organización de acuerdo con el "*Programa de Inducción*" que la Gerencia del Talento Humano disponga para tal fin.

Concientización, Educación, Entrenamiento de Seguridad de la Información

Los funcionarios de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL serán entrenados y capacitados para las funciones y cargos a desempeñar con el fin de

proteger adecuadamente los recursos y la información de la institución; y garantizar la compresión del alcance y contenido de las políticas de Seguridad de la Información y la necesidad de respaldarlas y aplicarlas de manera permanente. En los casos en que así se establezca, este entrenamiento deberá cubrir a personal de contratistas, o terceros, cuando sus responsabilidades lo exijan. Para ello, se podrá solicitar acompañamiento a la Gerencia de Informática y se realizará en Coordinación con la Gerencia del Talento Humano.

Proceso Disciplinario:

Todos los incidentes de seguridad ocurridos en la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL serán registrados e investigados disciplinariamente con el fin de determinar sus causas y responsables. Los procesos derivados de los reportes y del análisis de los Incidentes de Seguridad serán investigados y teniendo en cuenta la gravedad y las responsabilidades identificadas, se tomarán las acciones legales que correspondan.

Devolución de Activos

Todo activo propiedad de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL que sea asignado a un funcionario o a un tercero, deberá ser entregado al responsable de éste, como parte de las actividades definidas en el proceso de finalización del contrato o cambio de cargo.

Así mismo, es necesario tener en cuenta que: "*Todo funcionario de la Registraduría Nacional del Estado Civil que sea trasladado de dependencia, o se retire de la Entidad, está obligado y tiene el deber legal de entregar formalmente todos los bienes que tenía a su cargo al jefe inmediato, o a quien éste designe según lo estipulado en el Decreto 1010 de 2000, el cambio se informará inmediatamente a la Coordinación de Almacén e Inventarios para el registro oportuno de la novedad y deberá solicitar la expedición del paz y salvo respectivo de inventarios*", (Circular 168 del 19 de noviembre de 2010).

Retiro de derechos de Acceso:

Los derechos de acceso de todos los empleados, contratistas y usuarios de terceros a la información y a las instalaciones de procesamiento de información, deberán retirarse al terminar su empleo, contrato o convenio, o modificarse según el cambio.

Procedimiento que se realizará de acuerdo con los requerimientos e información recibida en las Delegaciones Departamentales, Registraduría Distrital y la Gerencia de Informática por parte de la Gerencia del Talento Humano.

4. GESTIÓN DE ACTIVOS DE INFORMACIÓN

Ref: ISO/IEC 27001 CL. A.8

Inventario de Activos (ISO/IEC 27001, CL 8.1.1)

La Gerencia de Informática debe mantener un inventario actualizado de los activos de información que se encuentran dentro de los Centros de Cómputo, sean estos propios o de terceros y del licenciamiento asociado a los equipos.

Los Directores de las áreas deben tener un inventario de los activos de información sea esta física o magnética.

La Gerencia Administrativa y Financiera, a través de la Dirección Administrativa Grupo de Almacén Grupo de Almacén e Inventarios, designará un responsable para cada uno de los activos, el cual debe estar distinguido por su respectiva placa de inventario. Dicho responsable velará por el buen uso y aplicación de las medidas necesarias para la salvaguarda del activo a su cargo.

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, a través de la Gerencia Administrativa y Financiera desarrollará una lista de todos los servicios y proveedores (ej.: proveedores de equipos y comunicaciones, utilidades generales, calefacción, aire acondicionado, energía).

La entidad a través de la Gerencia Administrativa y Financiera desarrollará y mantendrá un catálogo de todos los activos incluyendo software de terceros (ej., aplicaciones, herramientas de desarrollo y todo el software comprado a terceros). Este catálogo debe contener información descriptiva del activo (ej., tipo de activo, ubicación física (si aplica), dueño o responsable del activo y clasificación). *"Formato Único de Control de Bienes"*

Uso aceptable de los activos (ISO/IEC 27001, CL 8.1.3)

Toda la información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL debe ser procesada y almacenada de acuerdo con su nivel de clasificación o de acuerdo a la funcionalidad que cumplen, con el objetivo de señalar como ha de ser tratada y protegida dicha información.

El dueño de la información, entendiéndose como tal la Registraduría Nacional del Estado Civil es responsable de definir el uso de la información y los activos.

Uso de Internet

Internet es una herramienta de trabajo que ofrece múltiples sitios y páginas Web para consultar e investigar. La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, a través de la Gerencia de Informática, controlará el uso adecuado de este recurso, y se prohíbe el acceso de esta herramienta para consultar información que no corresponda con la naturaleza de nuestros procesos de identificación, desarrollo de eventos electorales y procesos transversales de la Organización.

Al respecto se establecen las siguientes políticas de acuerdo con el perfil y rol que desempeñe cada funcionario, el cual podrá solicitar bajo previa autorización del director, coordinador o jefe de oficina respectivo y visto bueno de la Gerencia Informática, acceso a ciertas páginas o sitios web mediante el "Formato solicitud de ingreso a páginas y servicios web"

A. Se prohíbe el acceso a páginas relacionadas con pornografía, nueva era, música, videos, concursos, entre otros.

B. Se prohíbe el acceso y el uso de servicios interactivos o mensajería instantánea como ICQ, NetMeeting, Kazaa, Chat, MSN Messenger, Facebook, Twitter, Yahoo, Skype, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información o bien para fines diferentes a las actividades propias del negocio de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

C. Se prohíbe la descarga, uso, intercambio y/o instalación de programas, juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten

contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas de hacking, entre otros.

D. Se prohíbe el intercambio no autorizado de información de propiedad de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, de sus usuarios y/o de sus funcionarios, con terceros.

E. La Gerencia de Informática, a través de la Coordinación de Administración e Infraestructura Tecnológica, podrá realizar monitoreo en cuanto a tiempos de navegación y páginas visitadas por parte de los funcionarios y/o contratistas. Así mismo podrá inspeccionar, registrar y evaluar las actividades realizadas durante la navegación de manera programada.

F. Cada uno de los funcionarios será responsable de dar un uso adecuado de este recurso y en ningún momento podrá ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y las políticas de seguridad de la información.

G. Los funcionarios y/o contratistas, al igual que los empleados o subcontratistas, no podrán asumir en nombre de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL posiciones personales en encuestas de opinión, foros u otros medios similares.

H. Este recurso podrá ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad, protección y la confidencialidad de la información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

Correo Electrónico

La **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL** asignará una cuenta de correo electrónico como herramienta de trabajo a cada uno de sus funcionarios, previa solicitud del Director, Coordinador o Jefe de Oficina respectivo. Para tal efecto se empleará el formato diseñado para tal fin

Su uso se encuentra sujeto a los siguientes parámetros:

a) La asignación de la cuenta de correo electrónico a los funcionarios de la entidad debe solicitarse con el formato "Formato de solicitud de cuentas de usuario institucional".

b) La cuenta de correo electrónico deberá ser usada para el desempeño de las funciones asignadas dentro de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.

c) Los mensajes y la información contenida en los buzones de correo son de propiedad de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL. El usuario podrá crear un histórico de su correo siempre y cuando sea almacenado en el disco duro del usuario y bajo su propia responsabilidad.

d) El tamaño de los buzones de correo lo determinará la Gerencia de Informática y podrá ser modificado de acuerdo con los perfiles de trabajo de los usuarios.

e) Se prohíbe enviar o reenviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y/o que inciten a

realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.

f) La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL en el envío masivo de mensajes corporativos a cuentas externas deberá incluir un texto que le indique al destinatario como ser eliminado de la lista de distribución.

g) Todos los mensajes enviados deberán contener como mínimo la siguiente información: nombres y apellidos, oficina donde labora, teléfono, extensión y correo electrónico.

Recursos Tecnológicos

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL asignará diferentes recursos tecnológicos como herramientas de trabajo para uso exclusivo de sus funcionarios y contratistas autorizados. El uso adecuado de estos recursos se reglamenta bajo las siguientes condiciones:

a) La instalación de cualquier tipo de software, actualizaciones y reinstalación del sistema operativo en los equipos de cómputo de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL será responsabilidad de la Gerencia de Informática y por tanto es la única dependencia autorizada para realizar esta labor.

b) Los usuarios no podrán realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo. Estos cambios podrán ser realizados únicamente por la Gerencia de Informática a través de la Coordinación de Soporte Técnico y Telecomunicaciones y diligenciando previamente el formato "Administración de cambios a sistemas de información".

c) El personal autorizado por el Comité de Seguridad de la Información podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL. Las conexiones establecidas para este fin, utilizarán los esquemas de seguridad que defina el Comité de Seguridad de la información.

Clasificación de la Información (ISO/IEC 27001 CL. A 8.2)

La información que se estime pertinente y que pertenezca a la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL deberá ser identificada y clasificada con base en los criterios de clasificación que defina el Comité de Seguridad de la Información.

5. CONTROL DE ACCESO

REF: ISO/IEC 27001 CL. A.9

Política de control de acceso *(ISO/IEC 27001, CL 9.1.1)*

Los sistemas de información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL contarán con mecanismos de identificación de usuarios, privilegios y procedimientos para la autenticación y el control de acceso a los mismos.

El acceso a los activos de información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL estará permitido únicamente a los usuarios autorizados, el cual deberá utilizar durante el proceso de autenticación, previo al acceso de los activos de

información autorizados según su perfil. La creación, modificación e inactivación de usuarios en la infraestructura de procesamiento de información deberá seguir el *"Procedimiento de Gestión de Usuarios y Contraseñas"*

En las Oficinas Centrales de la Entidad, la Gerencia de Talento Humano debe reportar oportunamente a la Gerencia de Informática, los funcionarios, contratistas y terceros que cesan sus actividades y solicitar la desactivación de su cuenta de correo o cualquier otra. Para los departamentos, los Delegados Departamentales deberán solicitar la desactivación de cuentas como las de Registradurías Especiales y Municipales y para la Registraduría Distrital, los Registradores Distritales realizarán estas solicitudes

Se implementará un procedimiento formal documentado de todas las operaciones relacionadas con la creación, inactivación y eliminación de usuarios del servicio de correo por parte de la Gerencia del Talento Humano. Así mismo, el cambio de privilegios, deberá hacerse por medio del formato "Solicitud de cuentas de usuario institucional" y ser debidamente autorizada por la Gerencia de Informática.

Cada funcionario tendrá un código único de identificación ante el sistema y será responsable de todo registro a su nombre.

El funcionario que disponga de usuario(s) de acceso a los activos de información, será responsable de su uso, el cual es personal e intransferible.

Gestión de contraseñas de usuario.

La gestión y la entrega de las contraseñas a los usuarios deberá seguir el *"Procedimiento de Gestión de contraseñas"* establecido.

Los usuarios deberán seguir las siguientes políticas para el uso y selección de las contraseñas de acceso y, por tanto, se responsabilizan de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados. (ISO/IEC 27001 CL. A.9.3.1):

Así mismo se tendrá en cuenta lo siguiente:

a. Mantener la confidencialidad de las contraseñas.
b. La asignación de contraseñas de acceso a los aplicativos debe ser utilizada de forma individual e independiente para cada usuario.
c. Todo tipo de contraseña debe ser secreta, personal y no puede prestarse ni permitir que la use otra persona.
d. Al digitar la contraseña, el usuario debe cerciorarse de que nadie lo está viendo en ese momento.
e. Las contraseñas son de uso personal y por ningún motivo se deberán prestar a otros usuarios.
f. Cuando el administrador del servicio del correo asigne la contraseña por primera vez, el usuario la utilizará solo en el primer inicio de sesión. En los subsiguientes es obligatorio realizar el cambio de contraseña para garantizar que solo el usuario la conoce.
g. La contraseña de cada perfil de usuario deberá cambiarse al menos una vez cada trimestre, así la aplicación no lo exija.
h. Las contraseñas no deberán ser reveladas por vía telefónica, correo electrónico o por ningún otro medio, con las excepciones pertinentes.

i. Se deberá reportar cualquier incidente que afecte la Confidencialidad de la contraseña.

j. Toda contraseña debe tener por lo menos un (1) carácter alfabético en mayúscula, uno en minúscula y un carácter numérico. Adicionalmente se deben usar caracteres especiales como: (#$&-_...*).

k. Las cuentas de los usuarios que hagan más de 3 intentos fallidos de acceso quedarán deshabilitadas y los usuarios deberán solicitar su desbloqueo.

l. Las contraseñas no se deberán escribir en ningún medio, excepto cuando son entregadas en custodia de acuerdo al *"Procedimiento de Gestión de contraseñas"*

m. Si un usuario tiene acceso a varios sistemas de información, se recomienda emplear contraseñas diferentes para cada uno de los sistemas a los cuales tiene acceso.

Revisión de derechos de acceso de usuario (ISO/IEC 27001 CL. A.9.2.5).

Los derechos de acceso de los usuarios a la información y a la infraestructura de procesamiento de información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, deberán ser documentados y revisados periódicamente y cada vez que se realicen cambios en la asignación de las áreas de responsabilidad de los funcionarios (cambio de cargo).

Cada mes la Gerencia de Informática debe realizar la depuración de usuarios en los sistemas de información para asegurar que no existen identificadores de usuario activos pertenecientes a funcionarios que se hayan retirado de la institución, de acuerdo con el reporte enviado por la Gerencia de Talento Humano.

SI durante dos meses se encuentra que no ha hecho uso de un recurso tecnológico asignado sin justificación alguna, es decir no se ha realizado LOGIN, la Gerencia de Informática procederá a inactivar el usuario.

Cuando un funcionario, contratista o colaborador a quien le haya sido autorizado el uso al acceso a la red y al servicio de Internet se retire de la entidad, su acceso a los servicios debe ser cancelado o inactivado.

Las cuentas de correo que no hayan sido utilizadas en el último mes deben ser eliminadas o inactivadas, dependiendo del caso.

El uso inapropiado o el abuso en el servicio de correo electrónico pueden ocasionar la desactivación temporal o permanente de las cuentas. Las acciones en este sentido pueden llevarse a cabo en función de incidencias que puedan suponer un problema para el buen funcionamiento del servicio.

Deben conservarse los registros que demuestren el historial de las actividades realizadas por los usuarios.

Equipo de Usuario desatendido y Política de puesto de trabajo despejado y pantalla limpia (ISO/IEC 27001 CL. A.11.2.8 11.2.9).

Todos los usuarios (funcionarios, contratistas y colaboradores) de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL que utilizan estaciones de trabajo, equipos de cómputo y portátiles, para la realización de su labor, deben acoger como práctica permanente el bloqueo de la pantalla al ausentarse de su puesto de

trabajo.

20 MAYO 2016

Todas las estaciones de trabajo, a excepción de aquellas que se encuentran en áreas con estrictas medidas de control de acceso o que hagan parte de las consolas de los sistemas misionales de la entidad, deben ser apagadas al final de la jornada laboral.

En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deben dejar la información confidencial protegida del acceso no autorizado. Esto incluye documentos impresos, discos compactos CD´s, dispositivos de almacenamiento USB y medios removibles en general.

Los usuarios al finalizar sus actividades diarias, deben salir de todas las aplicaciones y asegurarse de apagar la estación de trabajo.

Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo definido dentro de los elementos de la imagen corporativa, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

Los usuarios deberán retirar de forma inmediata todos los documentos confidenciales que envíen a las impresoras. Así mismo, no se deberá reutilizar papel que contenga información confidencial

Uso de los Sistemas de Información, Desconexión Automática de Sesión, Restricción de Acceso a la Información .

Los sistemas de información y comunicación de la entidad deben usarse solamente para las actividades de la función asignada y no deben utilizarse para ningún otro fin.

Todos los accesos para el uso de los sistemas de información de la entidad terminarán después de que el funcionario, contratista o colaborador cesa de prestar sus servicios a la Entidad.

La Entidad deberá implementar controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por los sistemas de información. Para mantener estos objetivos, la Gerencia de Informática tiene privilegios para: (1) restringir o derogar cualquiera de los privilegios del usuario, (2) inspeccionar, copiar, remover, o bien modificar algún dato, programa, u otro sistema que pueda evitar el cumplimiento de estos objetivos, y (3) tomar cualquier otra acción que estime necesaria para manejar y proteger sus sistemas de información. Estos privilegios pueden realizarse con o sin notificación a los usuarios, sin embargo, siempre se dejará evidencia de las acciones tomadas y las razones que obligaron a estas decisiones.

Las estaciones de trabajo de los usuarios finales deben ser bloqueadas automáticamente si superan un tiempo de inactividad, determinado en cada caso según el nivel de riesgo que corresponda, siendo necesario digitar nuevamente la clave de acceso en el momento que requiera continuar con la conexión.

Los sistemas de información incluirán un adecuado control de acceso basado en el análisis de las funciones que la aplicación tiene desarrolladas y las autorizaciones por grupos de usuarios, roles y perfiles.

Política de uso de los servicios en red, autenticación de usuario para conexiones externas, Control de conexión a la red, Control de encaminamiento de red, Aislamiento se sistemas sensibles.

La Entidad proporcionará tecnologías de acceso remoto a sus funcionarios y autorizará su uso de forma particular cuando así se requiera. La Gerencia de Informática garantizará un adecuado esquema de seguridad para los mismos.

Las direcciones internas, configuraciones e información relacionada con la topología y diseño de los sistemas de comunicación y redes de la entidad serán restringidas, de tal forma que no sean conocidas por usuarios internos, clientes o personas ajenas a la entidad sin la previa autorización de la Gerencia Informática.

Todas las conexiones a redes externas que accedan a la red interna de la entidad pasarán a través de un punto adicional de control como: firewall, gateway, o servidor de acceso.

Todos los computadores de la entidad que puedan ser accedidos remotamente a través de mecanismos como Internet, enlaces dedicados, y otros, deben ser protegidos por mecanismos de control de acceso aprobados por la Gerencia de Informática.

La conexión directa entre los sistemas de información de la entidad y otra organización vía redes públicas de datos como Internet requieren de la aprobación de la Gerencia Informática, que para este caso, definirá los mecanismos de seguridad apropiados.

Como requisito para interconectar las redes de la entidad con las de terceros, los sistemas de comunicación de terceros deben cumplir con los requisitos establecidos por REGISTRADURÍA NACIONAL DEL ESTADO CIVIL. La entidad se reserva el derecho de monitorear estos sistemas de terceros, sin previo aviso, para evaluar la seguridad de los mismos. La entidad se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos a establecer por la entidad.

Los usuarios que tengan acceso a direcciones IP públicas no pueden establecer conexiones a redes de acceso a información privadas, a menos que hayan sido aprobadas por la Gerencia Informática de la entidad.

Los empleados, contratistas y colaboradores que laboren para la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL en sitios de trabajo alternos, deben utilizar equipos de cómputo y red provistos por la entidad. Se hará excepción si otros equipos han sido aprobados como compatibles con el sistema de información y los controles de la entidad.

La arquitectura de los equipos de cómputo de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL no debe ser alterada ni mejorada en ninguna forma (ejemplo: actualización de procesador, expansión de memoria o adición de otras tarjetas) sin el conocimiento y autorización del responsable del área.

Segregación en redes.

La infraestructura tecnológica de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL que soporta aplicaciones debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La separación de estos segmentos debe ser realizada por medio de elementos de conectividad perimetrales e internos de enrutamiento y de seguridad.

Es responsabilidad de los administradores de los sistemas de información garantizar que los puertos físicos y lógicos de configuración y acceso privilegiado de las plataformas de infraestructura que soportan los sistemas de información deben estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

Ordenadores Portátiles y teletrabajo .

20 MAYO 2016

El uso de los equipos portátiles fuera de las instalaciones de la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL** únicamente se permitirá a usuarios autorizados por Gerencia de Informática.

Los equipos de cómputo de la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL** utilizados fuera de la entidad y en funciones propias de la Registraduría, deben ser exclusivamente utilizados para brindar apoyo a las actividades de la entidad y deben ser sujetos a un grado equivalente de protección igual al de los equipos que se encuentran dentro de las instalaciones de la Registraduría.

Para los equipos portátiles se deben aplicar las siguientes pautas:

a. Los equipos portátiles asignados a los funcionarios, contratistas y colaboradores deben atender todas las recomendaciones de seguridad.

b. Durante los viajes, los equipos (y medios) no se deben dejar desatendidos en lugares públicos. Los computadores portátiles se deben llevar como equipaje de mano.

c. Los portátiles son vulnerables al robo, pérdida o acceso no autorizado durante los viajes. Se les debe proporcionar una forma apropiada de protección de acceso y a la información almacenada en el mismo.

d. Se deben atender las instrucciones del fabricante concernientes a la protección del equipo.

e. Los equipos portátiles se deberán tener estos controles:

- Antivirus.
- Cifrado de datos.
- Restricción en la ejecución de aplicaciones.
- Restricción de conexión de dispositivos USB.

Control de Acceso Remoto

La administración remota de equipos o de la infraestructura de computo debe dejar evidencia escrita de la justificación por las que se asigna, al igual que de la responsabilidad que tiene el funcionario a quien se otorga este permiso

La solicitud debe ser realizada por el Gerente del Área correspondiente (Propietario de la información) y avalada por la Gerencia de Informática.

Para las entidades y proveedores que requieran conectarse de forma externa, cada esquema deberá ser validado por la Gerencia de Informática, quien determinara para cada caso el esquema de conexión segura.

6. CIFRADO.

Ref: ISO/IEC 27001/ CL. A.10

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de computo de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, sea por cualquier medio tecnológico existente, siempre deberá estar autenticado y sus conexiones deberán estar cifradas.

Toda la red de telecomunicaciones de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL deberá estar cifrada.

Toda información que se extraiga de los aplicativos misionales deberá estar cifrada para evitar que esta pierda su confidencialidad.

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL delegará en un área el desarrollo e implementación de procedimientos para el uso, protección y tiempo de vida de las llaves criptográficas, a cargo de la Gerencia de Informática.

7. SEGURIDAD FÍSICA Y AMBIENTAL

Ref: ISO/IEC 27001/ CL. A.11

Perímetro de Seguridad Física (ISO/IEC 27001, CL 11.1.1)

Todas las áreas destinadas al procesamiento de documentos de identidad o almacenamiento de documentos o información, así como aquellas en las que se encuentren los equipos de cómputo y demás infraestructura de los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. Por tanto, contarán con medidas de control de acceso físico en el perímetro de tal forma que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, los documentos de identificación, las tarjetas decadactilares, el software y el hardware de daños intencionales o accidentales.

Todas las puertas que utilizan sistemas de control de acceso deberán permanecer cerradas y es responsabilidad de todos los funcionarios y contratistas autorizados evitar que las puertas se dejen abiertas.

Las áreas de archivo de documentos, los Centro de Cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos de temperatura, humedad, estática, detectores de incendio, control y extinción etc., que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

Se deberá exigir a todos los visitantes, sin excepción, el porte de la ficha o escarapela que lo identifica, en un lugar visible. Así mismo, todos los funcionarios deberán portar su carné en un lugar visible mientras permanezcan dentro de las instalaciones de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.

Las instalaciones de las Oficinas Centrales de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, estarán dotadas de un circuito cerrado de TV con el fin de monitorear y registrar las actividades de funcionarios, terceros y visitantes. La Gerencia Administrativa y Financiera, en asocio con la Gerencia de Informática, asegurará utilizar la mejor tecnología disponible.

El acceso a las oficinas y áreas de trabajo que contienen información sensitiva, deberá ser restringido.

Barreras Perimetrales

Los centros de cómputo de la entidad (segundo y quinto piso de Oficinas Centrales y Centros de Acopio ubicados en las Delegaciones Departamentales), están definidos como áreas restringidas, por lo cual deben cumplir las normas y procedimientos establecidos para tales sitios, entre las cuales se tienen las siguientes:

a) En las áreas de centros de cómputo, se deberán establecer los mecanismos de seguridad necesarios para la correcta protección de los servidores que contienen la información confidencial de la entidad, de manera que se mantenga la confidencialidad y seguridad de la información que se procesa, así como la integridad de los equipos a través de procedimientos preventivos y correctivos de posibles situaciones que pongan en peligro la integridad del centro de cómputo.

b) Las puertas de los centros de cómputo deben estar siempre cerradas con algún mecanismo de seguridad, como: biometría, tarjetas de seguridad, claves de ingreso u otro que garantice la seguridad del sitio.

c) Los centros de cómputo de la entidad deben contar con planta de generación de energía, y UPS que proporcionan tiempos de respaldo adecuados.

d) Se debe evitar al máximo la permanencia de papelería y materiales que representen riesgo de propagación de fuego.

e) Se prohíbe a los funcionarios que trabajen en el área de los servidores, a excepción de una situación de emergencia o eventual.

f) El acceso físico al área de los servidores está permitido únicamente para el personal autorizado.

g) El ingreso y salida de funcionarios, personal autorizad debe ser registrado en el formato "Bitácora acceso a áreas restringidas de TI".

h) Es responsabilidad del administrador del centro de cómputo, informar las fallas en la seguridad física de los centros de cómputo, de tal manera que permitan prevenir, detectar y corregir ingresos o intentos de ingreso no autorizados.

i) En las áreas de centro de cómputo y procesamiento de información está prohibido fumar, consumir bebidas y alimentos, ingresar y/o almacenar material cuando no lo requiera la actividad a realizar.

j) Los centros de cómputo deben mantener las condiciones físicas y ambientales óptimas recomendadas, así como controles automáticos para incendio, temperatura, y cuando sea posible, monitoreo por Circuito Cerrado de Televisión.

k) Los centros de cómputo deben mantener condiciones óptimas de limpieza, seguridad y funcionalidad sobre cada uno de los elementos que contiene y cumplir con las recomendaciones que sobre cada elemento provea el fabricante.

Aseguramiento de oficinas, cuartos e instalaciones (ISO/IEC 27001 A.11.1.3)

La empresa de seguridad contratada para las sedes de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL se encargará de la seguridad interna de los edificios e instalaciones.

Se debe disponer de protocolos y elementos de control para el ingreso de personas y vehículos a las instalaciones así:

a) Fichas de control para el ingreso vehicular tanto de funcionarios y contratistas como de visitantes ocasionales.

b) Fichas de ingreso para las personas que acceden al restaurante ubicado en primer nivel de las instalaciones.

c) Porte de carnets por parte de los funcionarios.

Protección contra amenazas exteriores y ambientales ISO/IEC 27001 CL. 11.1.4

La entidad deberá contar con un plan de emergencia que permita tener debidamente organizados los equipos de funcionarios preparados y dotados para enfrentar emergencias, con el fin de preservar la vida y la integridad física de los funcionarios, contratistas y visitantes en las instalaciones, así como de salvaguardar los bienes materiales de la REGISTRADURÍA NACIONAL DE ESTADO CIVIL.

Áreas de carga, despacho y acceso público ISO/IEC 27001 CL. 11.1.6

El cargue y descargue de mercancías, en la sede de oficinas centrales de la Registraduría Nacional, se debe efectuar por la portería del sótano, en cuyo lugar se encuentra un guarda de seguridad las 24 horas, quien se encarga de la verificación física de los elementos que ingresan y salen de las instalaciones.

Seguridad de los equipos (ISO/IEC 27001 27001, CL A.11.2)

La infraestructura de procesamiento de información (equipos de hardware, software, elementos de red y comunicaciones, instalaciones físicas) deberá contar con las medidas de protección eléctricas y de comunicaciones para evitar daños a la información procesada. Se deberán instalar sistemas de protección eléctrica en los centros de cómputo y comunicaciones de manera que no se interrumpa el suministro de energía en caso de emergencia. Así mismo, se protegerá la disponibilidad e integridad de la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

Para resguardar la seguridad patrimonial de las oficinas centrales de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, la Gerencia de Informática y Asesoría de Seguridad deben implementar procesos de control de personal, estrategias de acceso y salida de equipos de cómputo, así como seguridad perimetral, vigilancia continua tanto en cámaras, como lectoras de control biométrico entre otros.

De la misma manera la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL debe poseer la infraestructura necesaria, con el fin de actuar contra eventos que pongan en riesgo la integridad y confidencialidad de la información, y es así, que los equipos de cómputo están conectados a las instalaciones eléctricas apropiadas de corriente regulada, fase, neutro y polo a tierra, para evitar pérdidas o daños de la información como activo fundamental de la Entidad.

Política de Mantenimiento de Equipos – Control ISO/IEC 27001 A.11.2.4)

La Gerencia de Informática gestionará el mantenimiento preventivo y correctivo de los equipos de cómputo, incluyendo periféricos comunes, con la finalidad de reducir posibles daños en el hardware y software, en toda su plataforma tecnológica, acorde con la disponibilidad presupuestal destinada por la Entidad y de acuerdo con el procedimiento "Soporte Técnico" desarrollado por la Gerencia de Informática.

Los generadores de energía, sistemas de aire acondicionado y los equipos de UPS, se deberán revisar y probar frecuentemente, para asegurar la continuidad del servicio en el evento de una pérdida de energía desde la red externa, con el fin de mantener la operatividad y estabilidad de los sistemas.

Todo mantenimiento realizado en equipos, debe ser registrado y se debe programar y avisar previamente a los usuarios que se puedan ver afectados. Esta actividad debe realizarse exclusivamente por el personal autorizado.

Equipos fuera de las instalaciones (ISO/IEC 27001, CL A.11.2.6)

Los equipos portátiles de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL no deberán dejarse a la vista en el interior de los vehículos. En casos de viaje siempre se deberán llevar como equipaje de mano.

En caso de pérdida o robo de un equipo portátil se deberá informar inmediatamente a la Gerencia de Informática y a la Gerencia Administrativa y Financiera y se deberá denunciar ante la autoridad competente.

Los equipos portátiles deberán cumplir con el siguiente control: Cuando un equipo de cómputo deba retirarse de las instalaciones de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL se deberá seguir el procedimiento definido por la Asesoría en Seguridad.

Eliminación y/o reutilización segura de equipos *(ISO/IEC 27001, CL A.11.2.7)*

Cuando un equipo sea reasignado o dado de baja, se deberá realizar una copia de respaldo de la información que allí se encuentre almacenada y posteriormente eliminada del equipo en mención.

8. SEGURIDAD DE LAS OPERACIONES

Ref: ISO/IEC 27001/ CL. A.12

Procedimientos de Operación y Responsabilidades *(ISO/IEC 27001, CL A.12.1)*

Se definirán procedimientos, registros e instructivos de trabajo debidamente documentados, los cuales serán progresivamente implementados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura tecnológica de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL. Cada procedimiento tendrá un responsable para su definición, mantenimiento e implementación.

Control de cambios operativos (ISO/IEC 27001, CL A.12.1.2)

Todo cambio a la infraestructura de procesamiento de información se controlará según el formato "*Control de Cambio a TI*" definido por la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, para asegurar que los cambios efectuados no afecten la disponibilidad, integridad o confidencialidad de la información.

La Gerencia de Informática deberá realizar seguimiento al uso de los recursos computacionales, realizará los ajustes del caso procurando su disponibilidad y realizará las proyecciones de capacidad futura requerida para asegurar los servicios misionales de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.

Segregación de tareas

Para la gestión de las operaciones de la infraestructura de procesamiento de información en la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, la Gerencia de Informática, con el apoyo de las áreas, establecerá mecanismos que permitan segregar las funciones de administración (sistemas operativos, bases de datos y aplicaciones), monitoreo y operación, separando entre estos los diferentes ambientes de desarrollo, pruebas y producción.

Separación de los recursos de desarrollo, prueba y operación ***(ISO/IEC27001, CL A.12.1.4)***

Dentro de la infraestructura de procesamiento de información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, se establecerán ambientes separados para el desarrollo, calidad y producción, de tal manera que se controle la transición de software y aplicaciones de un ambiente a otro.

No deberán realizarse pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad o confidencialidad de la información. Así mismo, en los ambientes de desarrollo y calidad si se llegaran a utilizar datos reales del ambiente de producción, se debe definir el protocolo de seguridad que permita salvaguardar la integridad de la información.

El software de aplicación en desarrollo o personalización será guardado separado del que se encuentra en producción y del respectivo de pruebas. Se deberán separar los directorios y librerías, y hacer cumplir estrictamente los controles de acceso a los usuarios.

Antes de instalar una nueva versión de aplicaciones o software, se deberá aplicar el plan de pruebas respectivo y éste debe ser aprobado en su totalidad, así como, disponer de lo necesario para reservar esta implementación de ser necesario.

Los funcionarios, contratistas o colaboradores que estén vinculados específicamente con el desarrollo de software no deberán ser los responsables de aprobar las funcionalidades ni deberían tener acceso al ambiente de producción.

Gestión de Servicios de Terceros

Es necesario implementar y mantener un nivel adecuado de seguridad de información y servicios en línea con los convenios de servicios por terceros. Esto incluye segregación de funciones y auditoria a las funciones.

Entrega de Servicios

En esta temática deberá tenerse en cuenta que:

a. Los contratistas son responsables por la actualización de los sistemas operativos, el software base y los aplicativos objeto del contrato instalados en los servidores de producción, propiedad de la RNEC, actividades que deberán desarrollar bajo la supervisión y coordinación de la Gerencia de Informática.
b. Los contratistas se obligan a hacer buen uso de los elementos dispuestos por la RNEC para la prestación del servicio en las instalaciones en donde estos operan (computadores, dispositivos de seguridad, mobiliario, edificación, etc.)
c. Los contratistas solo realizarán maniobras sobre los equipos que forman parte del objeto del contrato y que están bajo su cargo, siempre y cuando la actividad haya sido previamente aprobada por la Gerencia de Informática.
d. No se concederá acceso remoto al servidor de producción o ningún otro, para labores de mantenimiento fuera de las instalaciones de la RNEC. El acceso remoto desde fuera de las instalaciones está prohibido.
e. Los contratistas realizarán periódicamente "backups" de las bases de datos y aplicaciones a su cargo y entregarán copias de los mismos a la RNEC acorde con lo establecido en los contratos.
f. Los contratistas protegerán todo documento relacionado con el proyecto, y dispondrán de copias de respaldo como medida preventiva ante una eventual pérdida o daño.

g. Los contratistas deben aplicar periódicamente las actualizaciones de seguridad y del software base de los sistemas que se encuentran a su cargo, previa presentación de un plan de trabajo y su posterior aprobación por la Gerencia de Informática.
h. Los empleados de los contratistas, deberán firmar un convenio de confidencialidad de la información a su cargo
i. Los equipos portátiles o medios magnéticos de los contratistas y que contengan información del proyecto objeto de contratación, solo podrán ser retirados de las instalaciones de la RNEC con autorización del Director del Proyecto.
j. Toda la información de los sistemas de la RNEC que sean objeto de contratación es considerada confidencial y su uso es exclusivo de la entidad.
k. Los datos extraídos de los sistemas de la RNEC, objeto de contratación y puestos en un medio externo (impresiones, CDs, memorias USB, etc), con ocasión de las pruebas habituales, deberán ser destruidos dentro de las instalaciones de la RNEC tan pronto termine su utilidad.
l. Las copias de respaldo de la información manipulada por los contratistas, deberán estar debidamente rotuladas y de igual manera todos los documentos relacionados con los proyectos a su cargo.
m. Los contratistas deben informar a sus empleados las responsabilidades que asumen al ejercer el rol que van a desempeñar en el proyecto.
n. Los contratistas deben informar a sus empleados sobre las políticas de seguridad de la RNEC y verificar regularmente el cumplimiento de las mismas.
o. Los contratistas notificarán oportunamente a la RNEC los cambios en la planta de personal con sede en las instalaciones de la RNEC y que se encuentre asignada al proyecto.
p. Los contratistas evaluarán junto con la Gerencia de Informática las incidencias generadas por la violación a las políticas de seguridad y determinarán las acciones propias a seguir.
q. Los contratistas deberán incluir el tema de "seguridad de la información" en sus reuniones periódicas internas.
r. Los contratistas deben asegurar que se eliminan todos los privilegios de acceso a los sistemas para aquellos empleados que se retiran de los proyectos objeto de contratación.
s. Al área de trabajo critica de los contratistas, pueden entrar el personal autorizado y que está relacionado directamente con el desarrollo del proyecto.
t. Al área de trabajo crítica de los contratistas se puede acceder con reconocimiento de huella o por autorización expresa de un funcionario asignado por el mismo contratista.
u. Los sistemas a cargo de los contratistas deben contar con registros de auditoría de las operaciones que se realicen en ellos y este registro solo estará disponible para el área que determine la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.
v. Los contratistas deben monitorear permanentemente la actividad sobre la base de datos, sus aplicaciones y sobre el sistema operativo, informando a la RNEC de acuerdo con el contrato cualquier incidente que ocurra y que pueda afectar el normal desarrollo del proyecto.
w. Ninguna persona ajena a los contratistas debe tener acceso a la base de datos de auditoría ni a los archivos con "logs" de los sistemas objeto de contratación. El contratista los entregará a la RNEC cuándo sean requeridos por esta.
x. Los contratistas administrarán la creación de usuarios para acceder a los sistemas por ellos administrados, siguiendo las reglas que se establezcan para tal efecto por parte de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.
y. Las contraseñas de los usuarios del sistema operativo, de la base de datos y de los sistemas de información en general deben estar encriptadas.
z. El sistema de información deberá cerrar la sesión de un usuario que no registre actividad ("timeout")

aa. Los contratistas deben asegurar que las transacciones realizadas se completan satisfactoriamente o, en caso de fallos, se rechazan para mantener la integridad de la información.
bb. El código fuente de los sistemas administrados por los contratistas, las bases de datos y demás archivos relacionados con los proyectos son de carácter confidencial y ninguna persona está autorizada para llevarlos fuera de la entidad.
cc. La modificación del código fuente de los sistemas administrados por los contratistas solo deberá realizarse a través del contratista, previa solicitud y autorización de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.
dd. Los sistemas administrados por los contratistas deberán contar con sistemas alternos de contingencia debidamente documentados y su activación debe ser ordenada por la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL
ee. Cuando el sistema de contingencia se encuentra en otro espacio físico distinto al principal, ha de asegurarse que la seguridad de acceso al sitio y a los servidores sea limitada para personal autorizado por la Gerencia de Informática.
ff. Todo Software y programas ejecutables (código objeto de software) provistos por entidades externas, deberán probarse por la entidad antes de la instalación en el ambiente de producción.
gg. El código fuente del software provisto por entidades externas deberá ser revisado y probado en cuanto a sus compilaciones y los programas ejecutables por el equipo de trabajo asignado por la Gerencia Informática, antes de su instalación en producción.
hh. La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL establecerá mecanismos de auditoría y control sobre sus contratistas para garantizar la Confidencialidad, Disponibilidad e Integridad de sus activos de información.

Controles contra el código malicioso *(ISO/IEC 27001, CL A 12.2.1)*

Para prevenir infecciones por virus informático, los usuarios de **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL** no deben hacer uso de software que no haya sido proporcionado y validado por la Gerencia de Informática.

La infraestructura informática deberá contar con una plataforma Antivirus y de Web Gateway, con el fin de minimizar la ejecución de virus o código malicioso.

Se debe ejecutar el escaneo de virus con las herramientas antivirus disponibles, cada vez que se detecte que algún equipo o dispositivo informático está funcionando de manera irregular o se sospeche de la presencia de virus en equipos, archivos y/o correos electrónicos.

Si algún usuario sospecha que hay infección por un virus, se debe dejar de usar el computador, desconectarlo de todas las redes y llamar a la mesa de ayuda de la Gerencia de Informática.

Ningún usuario de la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL** debe intentar eliminar virus de los computadores. Cuando observe la alerta de un virus el conducto regular es informar al área de Mesa de Ayuda de la Gerencia de Informática para evitar que el virus pase a la red u otros equipos.

Se prohíbe abrir y/o descargar archivos o documentos de remitente desconocido, no confiable o sospechoso. En lo posible deberán ser borrados de las carpetas donde se encuentren y eliminarlos de la papelera de reciclaje en el computador.

El usuario debe revisar siempre con el programa antivirus, los archivos recibidos a través de la red.

Se prohíbe intercambiar archivos que hayan sido identificados como infectados por

virus o código malicioso o sean sospechosos de estar infectados.

Se prohíbe desactivar o eliminar los programas antivirus y/o de detección de código malicioso en los equipos o sistemas de información en que estén instalados.

Se prohíbe instalar y/o emplear software no autorizado. Los programas deben ser instalados por la Gerencia de Informática o con autorización expresa de ésta y en los equipos de cómputo de la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL**.

Se prohíbe instalar, conectar y/o emplear dispositivos de almacenamiento fijos y/o removibles o dispositivos informáticos no autorizados en los computadores, portátiles y/o servidores.

Copias de Seguridad *(ISO/IEC 27001, CL A.12.3)*

La información previamente definida y contenida en los servidores de la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL** se respaldará de forma periódica, determinada según el procedimiento "*Gestión de copias de respaldo y Backup de Información*" y los medios que se consideren necesarios se almacenarán en una custodia externa que cuente con mecanismos de protección ambiental como detección de humo, incendio, humedad, y mecanismos de control de acceso físico. Adicionalmente, se realizarán pruebas periódicas de recuperación y verificación de la información almacenada en los medios con el fin de verificar su integridad y disponibilidad.

Copias de seguridad de la información

Toda la información de valor confidencial y crítica de la entidad, debe ser periódicamente respaldada en medio magnético, debidamente rotulada y en lo posible, estar bajo custodia en un lugar seguro.

Los usuarios que usen computadores portátiles deben hacer respaldo de su información crítica, entendiéndose como tal, aquella indispensable o necesaria para el cumplimiento de sus funciones, antes de sacarlos fuera del lugar de trabajo, debido al riesgo de robo o pérdida de los mismos.

Todos los usuarios son responsables de realizar una copia de respaldo del original de la información de valor, confidencial o crítica a su cargo. Estas copias separadas deben ser efectuadas con la periodicidad requerida de acuerdo con los cambios que se presenten en la información.

El backup de información de valor, confidencial o crítica, que esté almacenada por largos periodos de tiempo, debe ser validada en forma periódica, de tal forma que se pueda garantizar que no ha sufrido deterioro.

Es responsabilidad de las áreas realizar seguimiento en la elaboración de los backup de información que permitan la continuidad de los servicios de la plataforma tecnológica.

La información respaldada que sea de uso confidencial, por ningún motivo podrá ser utilizada o divulgada para fines personales.

Es responsabilidad de cada funcionario, que la información que ya no sea necesaria sea eliminada dentro de las instalaciones de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL y si existe algún tipo de duda, deberá consultarse a la Gerencia de Informática.

Controles de Red (ISO/IEC 27001, CL A.13.1.1)

a) El acceso remoto a la red de datos de la **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL** se brindará para recursos como el correo electrónico corporativo y el acceso a otros sistemas de información que por su carácter descentralizado requiera usuarios externos y en este caso se seguirá el procedimiento establecido.

b) La **REGISTRADURÍA NACIONAL DEL ESTADO CIVIL** por medio de la Gerencia de Informática controlará con las herramientas disponibles, el acceso a los diferentes sistemas de información.

c) La información referente a las direcciones IP, configuraciones, topologías de red y diseño de los sistemas de información de la entidad, debe ser restringida, de tal forma que no sean conocidas ni por usuarios internos, ni terceros a la entidad sin la previa autorización de la Gerencia Informática.

d) Los sistemas de información de la entidad que contengan información confidencial y reservada, se deben mantener en niveles de protección más estrictos, con el fin de velar por su confidencialidad, integridad y disponibilidad.

e) Todos los computadores de la entidad que permitan ser accedidos por terceros a través de mecanismos como Internet, redes de valor agregado, y otros, deben ser protegidos por mecanismos de control de acceso aprobados por la Gerencia de Informática.

f) Los entes de control, durante su estancia en la entidad, tendrán acceso únicamente en modalidad de consulta a través de estaciones de trabajo a los sistemas de información sujetos a su control, con previa aprobación del Comité de Seguridad de la información.

g) La conexión entre sistemas de información de la entidad y otros de terceros debe ser aprobada previamente por la Gerencia Informática, con el fin de no comprometer la seguridad de la información de la entidad.

h) Como requisito para interconectar las redes de la entidad con las de terceros, los sistemas de comunicación de terceros deben cumplir con los requisitos de seguridad y confidencialidad a establecer por la Entidad. La entidad se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos.

i) La entidad se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos de seguridad y confidencialidad a establecer.

Gestión de medios removibles – Manipulación de los Soportes

Toda la información impresa y/o almacenada en medios y unidades de almacenamiento removibles, tales como, memorias USB o discos duros externos, estará controlada en cuanto a su acceso, uso, transporte, almacenamiento y eliminación, acorde con el nivel de clasificación de la información almacenada.

Para evitar la salida de la información no autorizada, procedente de los sistemas que tratan información clasificada como misional o crítica, en los computadores se podrá utilizar controles como la inhabilitación de los puertos USB y Unidades de CD que evitan la extracción de la información en medios externos.

Intercambio de información (ISO/IEC 27001, CL A.13.2)

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL firmará acuerdos de confidencialidad con funcionarios y terceros que por diferentes razones requieran conocer o intercambiar información reservada de la Entidad. En estos acuerdos quedarán especificadas las responsabilidades para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

Los medios de almacenamiento transportados fuera de las instalaciones de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL deberán cumplir con los controles a establecer para tal fin.

Toda la información que sea objeto de intercambio entre los diferentes sistemas de información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL estará controlada en cuanto a su acceso, envío, uso, almacenamiento y eliminación, de acuerdo a los controles a establecer.

Información puesta a disposición pública

Los funcionarios, contratistas o terceros responsables de la publicación de la información en el sitio WEB de la entidad, deberán atender el cumplimiento a las normas en materia de propiedad intelectual.

Los funcionarios, contratistas o terceros tienen prohibido instalar o utilizar software o productos no licenciados por la Entidad. En todo caso, cualquier instalación de software debe ser solicitada, obtenida y autorizada a través de la Gerencia de Informática.

Todos los cambios que se hagan en la página web de la entidad deben ser aprobados por la Oficina de Comunicaciones y Prensa antes de ser publicados.

La Oficina de Comunicaciones y Prensa se asegurará que el material puesto en la página web contenga información consistente, esté de acuerdo con la misión de la entidad y de acuerdo a las medidas de seguridad de la información que la entidad requiere.

La entidad efectuará constantes revisiones al cumplimiento de las normas en materia de propiedad intelectual

Registro de Auditoría

Todos los sistemas de aplicación en producción que la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL estime pertinentes y que contengan información misional de la entidad deben generar log o rastros de auditoría; igualmente los sistemas que operen y administren información misional, valiosa o critica para la entidad, deben tener archivos de log que contengan la evidencia sobre todos los eventos relevantes asociados a los activos informáticos.

La información de auditoría solo estará disponible para el Comité de Seguridad Informática o el área que determine la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.

Todos los log del sistema y de las aplicaciones deben mantenerse en forma segura, de tal forma que eviten que personas no autorizadas puedan acceder a ellos. Se deberá garantizar la confidencialidad, disponibilidad e integridad de los mismos.

Todo software aplicativo habilitado en ambiente de producción de la entidad debe incluir archivos Logs que registren como mínimo la siguiente información: (1) la actividad realizada en la sesión abierta por el usuario incluyendo la identificación del

código del usuario, fecha/hora de la entrada y de la salida de cada sesión del sistema y las aplicaciones invocadas, (2) cambios de información en los archivos de las aplicaciones críticas (3) adiciones y/o cambios a los privilegios de los usuarios, y (4) fecha/hora de iniciación y terminación de ingreso al sistema de información, (5) modificaciones realizadas por los usuarios DBA´s.

Supervisión del Uso del Sistema

Todos los accesos de usuarios a los sistemas, redes de datos y aplicaciones de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, serán registrados y monitoreados, de acuerdo con las pautas establecidas por el Comité de Seguridad de la información y de conformidad con las herramientas y recursos humanos disponibles para tal fin.

9. SEGURIDAD EN LAS COMUNICACIONES

Ref: ISO/IEC 27001/ CL. A.13

La Gerencia de Informática, controlará y gestionará la totalidad de las redes de comunicaciones con que cuenta la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.

La Gerencia de Informática identificará los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión sobre los servicios de red, incluyendo los mismos en los contratos con sus contratistas.

La Gerencia de Informática deberá propender por la transferencia segura de información entre la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL y las entidades externas.

10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Ref: ISO/IEC 27001-2005 CL. A.14

Análisis y especificación de los requisitos de seguridad. ***(ISO/ 27001 CL. A.14.1.1)***

La inclusión de un nuevo producto de software o aplicativo en la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, o los cambios y/o actualizaciones a los sistemas existentes, deberán estar precedidos de la definición de los requisitos y controles necesarios.

Todas las solicitudes para compra, actualización y/o desarrollo de software deberán contar con las revisiones y autorizaciones según el procedimiento *"Gestión y desarrollo de proyectos de tecnología"*. ".

El Desarrollo de tecnologías informáticas se debe orientar sobre herramientas basadas en tecnologías de última generación, que permitan la portabilidad y escalabilidad de las aplicaciones

La supervisión y seguimiento a proyectos de infraestructura informática, deben incorporar como un elemento básico de la supervisión, el cumplimiento de la aplicación de políticas de seguridad tanto en el desarrollo de la solución como en el producto final que será entregado a la Entidad y de ser necesario, dentro de la

documentación entregada, se debe incluir un capítulo que demuestre el cumplimiento de estas políticas.

El mantenimiento de software realizado por la entidad o por terceros no podrá desconocer la inversión en desarrollos anteriores, a menos que los mismos en razón a las plataformas subyacentes deban considerarse como soluciones obsoletas.

La Gerencia de Informática es el área responsable de mantener a disposición de la entidad la infraestructura tecnológica conveniente de acuerdo con sus requerimientos y con la disponibilidad presupuestal asignada.

Validación de datos de entrada (ISO/IEC 27001-CL A.14.1.3)

Todos los desarrollos de software deben surtir una fase de pruebas de funcionalidad en la cual se evidencien los controles establecidos en relación con la integridad de la información que será ingresada una vez se lleve a cabo su implementación.

Cuando el mantenimiento de software involucre cambios en uno o más componentes del sistema se deberán ejecutar pruebas de regresión para las soluciones que se definan y que permitan asegurar que la funcionalidad del software no fue afectada.

La supervisión y seguimiento a proyectos de infraestructura informática que involucren desarrollo de aplicaciones deberán contar con una fase de pruebas que incluyan, pruebas de ingreso de información y la validación de entrada de datos independientemente del medio utilizado o aplicado.

Control de Procesamiento Interno

Los desarrollos de software deben surtir una fase de pruebas en la cual se valide que la información generada por el sistema no sufre ninguna alteración para casos particulares que evidencien errores en la funcionalidad interna del software.

Los desarrollos de software deben involucrar la correspondiente documentación interna y externa que permitan identificar su seguimiento hasta el nivel de rutinas y procedimientos.

Dentro del proceso de aceptación de un software adquirido a terceros, se deberá evidenciar la realización de las correspondientes pruebas con datos reales a fin de evitar que el mismo presente errores en la funcionalidad interna.

Integridad del mensaje

Se garantizará que los desarrollos de software en especial los que deben hacer uso de conexión WAN y servicios vía Internet integren las herramientas de seguridad basadas en recursos tales como funciones Hash y protocolos de seguridad, que permitan garantizar la integridad del mensaje.

Validación de datos de salida

Antes de la puesta en producción y durante la fase de pruebas y ajustes se deberán realizar las correspondientes pruebas y verificación de resultados con el fin de evidenciar que las salidas de información generada por las aplicaciones corresponden a lo solicitado por el usuario y a las necesidades de la entidad.

Es imprescindible que en todas las fases de aceptación de software de terceros se

integre al usuario final, con el fin de verificar que la información que genera el sistema se ajusta a lo requerido para cada uno de los módulos que integren la solución.

Durante el mantenimiento de aplicaciones y en las pruebas de no regresión se deberá verificar que las salidas de los sistemas, mantengan la consistencia en la información entregada por los mismos.

Seguridad de los Archivos del Sistema - Control del software operacional

Los responsables de la administración de las plataformas de producción estarán obligados a controlar el acceso y uso de los programas fuente, el acceso a los archivos de los sistemas y/o a las aplicaciones que operan en ellas, así como a la programación de las actualizaciones necesarias a realizar.

No se permitirá la instalación de herramientas de desarrollo ni programas fuente en los sistemas de producción, a menos que sea autorizado por el Comité de Seguridad de la información y la Gerencia de Informática.

No se permitirá el uso de versiones de software en los sistemas de producción que no sean soportadas por los fabricantes, ni versiones de prueba que no hayan sido liberadas al mercado (Beta), a menos que sea autorizado por el Comité de Seguridad de la información y la Gerencia de Informática.

El acceso de los proveedores a los sistemas de producción solo será permitido para realizar labores de soporte o mantenimiento, previa autorización del administrador de la plataforma, quien deberá informar con anterioridad al Comité de Seguridad de la Información sobre la programación de esa actividad

Control del "software" operativo

La instalación de software operativo deberá seguir las políticas de seguridad para la instalación de cualquier tipo de software en los equipos utilizados por la Entidad. En consecuencia, requerirá de un usuario con roles de administrador para la correspondiente instalación.

Para el caso de software desarrollado por terceros se deberá verificar que el mismo no incluya funciones o rutinas que alteren la seguridad de los sistemas operativos.

Dentro de las actividades de mantenimiento de software se debe garantizar la seguridad de la información de tal manera que si se utilizan herramientas o procedimientos que puedan generan riesgos de seguridad, los mismos serán desinstalados para no afectar el sistema en producción.

Protección de datos de prueba del sistema

Para las pruebas de software solo se deberán generar los archivos que contengan la información estrictamente requerida para las pruebas.

Así mismo, en los ambientes de desarrollo y calidad si se llegaran a utilizar datos reales del ambiente de producción, se debe definir el protocolo de seguridad que permita salvaguardar la integridad de la información.

Control del acceso a código fuente de programas Control

La protección sobre el código fuente deberá tener los mismos controles que aplican a la utilización de datos de prueba de las aplicaciones y adicionalmente contar con mecanismos de custodia y protección de acceso no autorizado.

Seguridad en los procesos de desarrollo y soporte.

Todo sistema utilizado para el procesamiento de la información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL deberá ser instalado y actualizado siguiendo el *formato "Control de cambios a TI"*, estableciendo y cumpliendo con los requerimientos de seguridad definidos para el sistema.

Los contratos de desarrollo de software con terceros deberán tener claramente definidos los alcances de las licencias, los derechos de propiedad del código desarrollado y los derechos de propiedad intelectual, junto con los requerimientos contractuales relacionados con la calidad y seguridad del código desarrollado.

Se debe garantizar que en las fases de desarrollo y/o actualización y prueba de software no pondrán en riesgo el software instalado, como tampoco la información, la seguridad y la integridad de la plataforma con la que la entidad cuenta para soportar sus sistemas de información.

Todos los sistemas (sistemas cliente/servidor, redes, computadoras personales, etc.) deberán ser provistos de software licenciado.

Los módulos ejecutables nunca deberán ser trasladados directamente de los ambientes de pruebas a los ambientes de producción, sin que previamente sean probados, revisados y compilados. Las actividades de revisión y compilación deberán ser ejecutadas por un nivel técnico no asociado con las pruebas del proceso.

Antes de comenzar a usar un nuevo aplicativo en producción o con cambios sustanciales, deberán documentarse los controles de seguridad a implementar, con el fin de ser evaluados por las áreas pertinentes de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.

Revisión técnica de aplicaciones después de cambios en el sistema operativo

Todos los procesos de implementación de soluciones informáticas y en especial los procesos de migración de aplicaciones, deberán prever los ajustes y evoluciones correspondientes de tal manera que la solución se integre a la nueva plataforma sin que se ponga en riesgo la estabilidad del sistema en producción.

Filtraciones de información.

Las claves y mecanismos de acceso a servidores y otros recursos de información, así como cualquier procedimiento, estrategia y controles establecidos que garanticen la seguridad de la plataforma informática de la Entidad, deberán ser de uso exclusivo y restringido a los responsables de los mismos. La entidad implementara la plataforma adecuada para la prevención de pérdida de datos salientes.

Desarrollo de programas por terceros (ISO/IEC 27001 CL A.12.5.7).

La supervisión y seguimiento a proyectos de infraestructura informática, deben incorporar como un elemento básico de la supervisión, el cumplimiento de la aplicación de políticas de seguridad tanto en el desarrollo de la solución como en el producto final que será entregado a la Entidad y de ser necesario, dentro de la documentación entregada, se debe incluir un capítulo que demuestre el cumplimiento de estas políticas.

Gestión de la vulnerabilidad técnica

Se realizarán por lo menos dos (2) pruebas de vulnerabilidad por año a los sistemas

previamente establecidos de la plataforma tecnológica de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

Los administradores de las plataformas serán responsables de mantener protegida la infraestructura a su cargo, de los riesgos derivados de las vulnerabilidades técnicas identificadas .

Una vez identificadas las vulnerabilidades técnicas potenciales, la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL identificará los riesgos asociados y los controles de seguridad a ser tenidos en cuenta (esta acción puede implicar la actualización de sistemas vulnerables y/o aplicación de las medidas de acción necesarias).

Si una actualización se encuentra disponible, se deben tratar los riesgos asociados con la instalación (los riesgos planteados por la vulnerabilidad deben ser comparados con los riesgos de la instalación de la actualización).

Los correctivos que requieran ser aplicados en la plataforma tecnológica, derivados de la identificación de vulnerabilidades, deberán seguir el formato *"Control de Cambios a TI"* .

El Comité de Seguridad de la información realizará el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas.

Las claves y mecanismos de acceso a servidores y otros recursos de información así como cualquier procedimiento, estrategia y controles establecidos que garanticen la seguridad de la plataforma informática de la Entidad, deberán ser de uso exclusivo y restringido a los responsables de los mismos.

11. SEGURIDAD CON LOS PROVEEDORES
Ref: ISO/IEC 27001/ CL. A.15

Seguridad de la información en las relaciones con los proveedores

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL asegurará la protección de los activos de la organización que sean accesibles a los proveedores.

El Comité de Seguridad de la Información establecerá los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de información. Estos requisitos se deberán documentar y formarán parte del contrato con el proveedor.

Los Contratos con los proveedores deberán incluir los requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos, servicios de tecnología de información y comunicaciones.

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL por medio de la Gerencia de Informática realizará las labores de auditoria de la información a los servicios prestados por sus proveedores.

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL establecerá las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información relacionados con sus proveedores.

12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Ref: ISO/IEC 27001 CL. A.16

Reportes de eventos y debilidades de seguridad de la información: (ISO/IEC 27001 CI A.16.1)

Los funcionarios y contratistas de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL deberán informar inmediatamente al Comité de Seguridad de la Información cualquier situación sospechosa, o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información.

El Comité de Seguridad de la Información será el encargado de realizar la investigación y seguimiento a los eventos e incidentes de seguridad reportados.

Notificación de los eventos de seguridad de la información, Notificación de puntos débiles de la seguridad.

Todos los Incidentes que se presenten en la seguridad de la información, deben ser de manera inmediata reportados a través correo electrónico, atención telefónica, notificación verbal y/o escrita.

Todos los usuarios de la plataforma tecnológica de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL deben reportar cualquier incidente de seguridad que detecten al Comité de Seguridad de la Información, en el menor tiempo posible después de haber sido detectado.

Los funcionarios, contratistas y terceros de la entidad deben reportar todas las violaciones relacionadas con la seguridad de la información al Comité de Seguridad de la Información en el menor tiempo posible, con el fin de que se puedan tomar las acciones pertinentes.

Las fallas que se detectan en los sistemas de información y/o aplicaciones de la entidad se consideran un incidente de seguridad porque afectan la disponibilidad de la información y deben ser tratados como incidentes de seguridad de la información.

Manejo de incidentes de seguridad

Todos los incidentes de seguridad reportados serán investigados y se les hará seguimiento por parte del Comité de Seguridad de la Información. Los resultados de las investigaciones serán informados a la Gerencia de Informática de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL, especificando las causas, consecuencias, responsabilidades, solución y acciones para evitar que se presenten nuevamente.

13. GESTIÓN DE LA CONTINUIDAD DE LA OPERACIÓN

REF: ISO/IEC 27001CL. A.17

Seguridad de la información en la continuidad de la operación (ISO/IEC 27001 CL. A.17.1).

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL contará y/o complementará un Plan de Continuidad de la operación que permita la continuidad de las operaciones de los procesos críticos, ante la ocurrencia de eventos no previstos o desastres naturales.

Los encargados de las áreas funcionales serán los responsables de mantener documentados y actualizados los procesos de contingencia a su cargo, e informar cualquier cambio al Comité de Seguridad de la información

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL verificará a intervalos regulares los controles de continuidad de negocio establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

La Gerencia de Informática, de acuerdo con los recursos con que disponga, implementará instalaciones de procesamientos de información con redundancia suficiente para cumplir los requisitos de disponibilidad que establece los procesos misionales de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.

14. CUMPLIMIENTO DE REQUERIMIENTOS

REF: ISO/IEC 27001CL. A.18

Cumplimiento de las obligaciones legales (ISO/IEC 27001 CL. A.18.1)

Está prohibido el uso de software ilegal o no licenciado. Los usuarios serán responsables por la instalación y utilización de software no autorizado en sus estaciones de trabajo y en caso dado se someterá a las consecuencias establecidas en las leyes.

Derechos de propiedad intelectual (ISO/IEC 27001 CL. A.18.1.2)

Se prohíbe el almacenamiento, descarga de Internet, intercambio, uso, copia, reproducción y/o instalación de software no autorizado, música, videos, documentos, textos, fotografías, gráficas y demás obras protegidas por derechos de propiedad intelectual, que no cuenten con la debida licencia o autorización legal, y con la autorización de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.

Se permitirá el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de los mismos, con el fin de preservar los derechos intelectuales de las obras o referencias citadas.

Protección de registros (ISO/IEC 27001 CL. A.18.1.3).

La información personal de los funcionarios, usuarios y/o contratistas es de carácter reservado. Por tanto, la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL la utilizará únicamente según lo establecido en los acuerdos o contratos laborales y en ningún momento podrá divulgarla a terceras partes a menos que cuente con la autorización formal del funcionario, usuario y/o contratista o de orden judicial.

Prevención de la utilización indebida de los equipos de procesamiento

Los recursos tecnológicos asignados a los funcionarios y contratistas de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL deberán ser usados para el desempeño de las funciones asignadas dentro de la organización; así mismo, éstos podrán ser utilizados para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.

Cada uno de los funcionarios y contratistas es responsable de hacer un buen uso de los recursos tecnológicos de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL y en ningún momento podrán ser usados para beneficio propio o para realizar prácticas ilícitas

o mal intencionadas que atenten contra otros funcionarios, terceros, la legislación vigente y las políticas de seguridad de la información de la REGISTRADURÍA NACIONAL DEL ESTADO CIVIL.

Auditoria a los sistemas de información (ISO/IEC 27001 CL. A.18.2).

La REGISTRADURÍA NACIONAL DEL ESTADO CIVIL realizará auditorías periódicas con el fin de verificar la correcta aplicación de controles y estándares técnicos.

Dada en Bogotá D.C., a los 20 MAYO 2016

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

JUAN CARLOS GALINDO VACHA
Registrador Nacional del Estado Civil

ORLANDO BELTRÁN CAMACHO
Secretario General

Elaboró: JCP-CAGR
Revisó: DCH-LAM
Aprobó: AFL-LFGC-CMP-ABP-CAGR