RESOLUCIÓN DEL SECRETARIO GENERAL DE LA SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS Nº 192 -2014-SUNARP/SG

Lima, 15 AGO. 2014

CONSIDERANDO:

Que, la Superintendencia Nacional de los Registros Públicos es un Organismo Público Técnico Especializado del Sector Justicia y Ente Rector del Sistema Nacional de los Registros Públicos, dotado de personería jurídica de derecho público, con patrimonio propio y autonomía, funcional, jurídica, registral, técnica, económica, financiera y administrativa;

Que, mediante Resolución 060-2010-SUNARP/SN se aprobó el Reglamento de Seguridad de la Información de la SUNARP;

Que, es necesario disponer de una herramienta normativa que establezca los lineamientos de gestión y control a las diferentes actividades y procesos vinculados a la seguridad de la información y a seguridad informática que se debe observar en las áreas de catastro;

Que, mediante el Informe N° 177-2014-SUNARP/OGTI, la Oficina General de Tecnologías de la Información remite el "Proyecto de Lineamientos de Gestión y Tratamiento de la Información para el área de Catastro", para su aplicación en las Zonas Registrales y en la Sede Central;

Que, estando a lo señalado en el inciso r) del artículo 12 del Reglamento de Organización y Funciones de la Sunarp, aprobado mediante Decreto Supremo Nº 012-2013-JUS;

Que, con el visado de la Dirección Técnica Registral y de la Oficina General de Tecnologías de la Información;

SE RESUELVE;

ARTÍCULO PRIMERO.- Aprobar los *"Lineamientos de Gestión y Tratamiento de la Información para el área de Catastro"*, que forman parte integrante de la presente resolución;

ARTÍCULO SEGUNDO.- Disponer que son responsables de la supervisión y cumplimiento de los presentes lineamientos los jefes de los órganos desconcentrados, los jefes de las unidades registrales, los coordinadores y personal de catastro y el personal de las Unidades de Tecnología de la Información, a nivel de la Zona Registral y el personal de la Subdirección de Catastro y personal de la Oficina General de Tecnologías de la Información a nivel de la Sede Central;

ARTÍCULO TERCERO.- Encargar a las jefaturas de las zonas registrales que dispongan la notificación de la presente resolución al personal de su respectiva zona registral.

Regístrese, comuníquese y publíquese en el portal institucional.

CARLOS ALBERTO DIAZ CHUNGA
Secretario General
sunarp

sunarp
Superintendencia Nacional
de los Registros Públicos

LINEAMIENTO

Gestión y Tratamiento de la Información para el Área de Catastro

Código: OGTI-01-L

Elaborado por:	Revisado por:	Aprobado por:
Frank Gonzales Espinoza OGTI	Javier Segura Carrera OGTI	Dr. Carlos A. Díaz Chunga SG
Firma:	Firma:	Firma:

Superintendencia Nacional de los Registros Públicos – Secretaría General

CARLOS ALBERTO DIAZ CHUNGA
Secretario General
sunarp

Índice

1.- OBJETIVO

En el marco del Reglamento de Seguridad de la Información aprobado por la Sede Central, así como en las Normas Técnicas de Seguridad de la Información, se considera recomendable implementar procedimientos de gestión y control a las diferentes actividades y procesos vinculados a la seguridad de la información y seguridad informática que están vinculadas al área de catastro.

2.- ALCANCE

El lineamiento es de cumplimiento obligatorio en la Sede Central y todas las Zonas Registrales, tanto por el personal de la Sub Unidad de Catastro y el personal de la Oficina General de de Tecnologías de la Información, y sus áreas equivalentes a nivel de las Zonas Registrales.

3.- BASE LEGAL

- Norma Técnica Peruana NTP/ISO /IEC 17799:2007 Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información.
- Normas de Control Interno, aprobadas con Resolución de Contraloría 320-2006-CG
- Reglamento de Seguridad de la Información, aprobado con Resolución 060-2010-SUNARP/SN, del 17 de marzo del 2010

4.-GLOSARIO DE TÉRMINOS

OGTI: Oficina General de Tecnologías de la Información.

UTI: Unidad de Tecnologías de la Información.

SG: Secretario General.

NTP: Norma Técnica Peruana

5.- SEGURIDAD DEL CENTRO DE CÓMPUTO

La Sala de Servidores debe contar con características mínimas de configuración que garanticen su funcionamiento, en cuanto se emita un lineamiento institucional al respecto se utilizará los estándares de la industria Uptime Institute, TIA-942, tendiendo al nivel TIER2 en el caso de Oficinas Registrales de Sede Principal.

6.- SEGURIDAD DE DATOS EN EL CENTRO DE PROCESAMIENTO DE DATOS

En el área de Catastro, la Base Gráfica Registral y los Informes Técnicos de Catastro constituyen los activos más importantes que se deben salvaguardar, por lo que es necesario que los equipos que almacenan la información sean confiables y seguros.

La Sub Unidad de Catastro comunicará formalmente a la UTI la ubicación de esta Base Gráfica, y sus componentes para que aplique las medidas de seguridad establecidas.

La UTI trasladará esta información lógica a algún servidor ubicado en su centro de datos o sala de servidores de la Oficina Registral (Sede Principal) si esta no estuviera ya ubicada allí.

La Sub Unidad de Catastro solicitará accesos personalizados para cada una de las personas que labora en su área señalando explícitamente el nivel de perfil requerido.

La UTI configurará los accesos y activará las auditorías a nivel de sistema operativo de servidor.

La Sub Unidad de Catastro será responsable de la gestión y del contenido de la información de la Base Gráfica.

La UTI será responsable de implementar controles de seguridad informática a nivel de file server.

La UTI será responsable de la ejecución de las copias de seguridad de la información en el marco de sus funciones generales y de las Políticas de Backup y Restore, así como de los Procedimientos de Traslado y Custodia de las cintas de backup.

En caso Catastro cuente con bases de datos relacionales, estas pasarán bajo control y administración de las UTI, debiendo Catastro entregar formalmente los datos de acceso y configuración para que las UTI puedan realizar la migración o Traslado de la Base de Datos, a servidores y se aplique las mejores prácticas para su administración.

Es necesario garantizar que los datos almacenados sean fiel reflejo de la realidad, para lo cual es necesario deslindar responsabilidades. La UTI es un ente de apoyo cuya función principal es custodiar las fuentes de información y que no debe tener acceso a modificar los datos, por lo tanto la responsabilidad de la información mostrada debe ser totalmente del área que la ingresó o generó (áreas propietarias de la información).

7.- SEGURIDAD DE ACCESO A LOS SISTEMAS

El personal de Catastro hace uso de sistemas registrales y de un sistema de gestión de informes catastrales, es necesario que los empleados cuenten con claves únicas y con un perfil que se ajuste al trabajo que normalmente hacen, haciéndoles notar que no pueden hacer trabajos que no les están permitidos.

El Responsable de La Oficina de Catastro debe solicitar el acceso a los sistemas indicando explícitamente el perfil de acceso, el mismo que debe contar con el visto del Jefe de la Unidad Registral.

La UTI configurará los accesos una vez recibida la autorización correspondiente.

De acuerdo a su diseño algunas aplicaciones registrales generan al momento de la creación de usuarios, contraseñas temporales genéricas, las mismas que luego solicita cambiarlas o modificarlas para continuar operando en dicho sistema. En otros casos se debe asignar una contraseña temporal la misma que puede ser ingresada por el usuario al momento de su creación o entregada en forma personal a través de algún medio personalizado, debiéndose indicársele a los usuarios la necesidad de cambio de la misma por una contraseña de su manejo y uso personal, si el aplicativo no condiciona el cambio en el primer ingreso según su diseño.

La Gestión de Contraseñas de Acceso de los usuarios a los sistemas tendrá carácter de "personal, intransferible y confidencial", por lo que cada usuario será responsable de toda actividad que realice con su clave de acceso.

8.- SEGURIDAD DE ACCESO A LA RED.

Es necesario que a cada usuario que va a tener acceso a una PC o una estación gráfica en el área de Catastro y requiera acceder a la red de datos institucional, deba asignársele un identificador de usuario personalizado, de manera de poder distinguir quiénes están accediendo al sistema y cuáles programas están usando. Los recursos de red se le asignan en función de las funciones que ejecutan. Una vez autenticado, al perfil del usuario se le aplicarán las políticas restrictivas definidas en el Servidor de Dominio, básicamente restricciones de edición de registro, configuración de red, escritorio, etc.

Por lo tanto es necesario modificar los niveles de acceso y personalizar las claves para cada usuario, aprovechando para asignarles las carpetas a las cuales tiene accesos tanto personales como grupales y de ninguna manera deben dejar que su contraseña sea conocida por otros empleados.

La UTI debe asegurar que los usuarios no deban tener acceso a modificar datos de su perfil de trabajo, lo cuál sería un riesgo para la seguridad a todo nivel.

9.- SEGURIDAD EN LAS ESTACIONES DE TRABAJO

Las Estaciones de Trabajo de la Zona Registral deben tener configurado contraseñas de encendido o de acceso a la PC, a dos niveles según la capacidad del BIOS de la PC, un nivel de usuario y otro de Supervisor. El acceso de usuario debe ser entregado a los operadores del área en los equipos que estén a su cargo.

Se debe configurar el bloqueo automático de las estaciones para el uso de protector de pantalla cuando los equipos quedan desatendidos, de acuerdo a lo establecido en el Reglamento de Seguridad de la Información.

Los accesos a Internet deben estar restringidos a un número limitado de sites relacionados a la actividad del área y su función, se bloquean las páginas que son posibles fuentes de infección de virus o de fuga de información, se restringen correos gratuitos, páginas de almacenamiento de información, redes sociales, etc.

Todos los equipos deben contar con antivirus, configurado para que se ejecute y se actualice periódicamente.

Todos los equipos deben mantener los puertos USB, Bluetooth, IR deshabilitados, los lectores / grabadores de CD/DVD desactivados, así como cualquier puerto que permita el copiado de información, o servicio inalámbrico que permita la trasferencia de datos no controlada por la UTI debe ser desactivado

10.- IDENTIFICADOR DE USUARIO (USER ID)

Para lograr los niveles de seguridad antes señalados es necesario dotar a cada empleado que tenga o tendrá acceso a una PC, con un identificador de usuario y su contraseña. La Oficina de Personal es la encargada de velar por el buen funcionamiento de los identificadores, coordinando y solicitando a la Oficina de Informática los cambios necesarios (altas y bajas), según el estado del personal, por ejemplo de vacaciones, reingreso, cesante, cambio de puesto, suspendido, descanso por maternidad, etc.

Las personas que laboran en las áreas de Catastro deben contar con identificadores de usuario para el acceso de red, acceso a los sistemas, acceso al correo, entre otros, se procura que el identificador sea único, en función al diseño de los sistemas las contraseñas pueden ser distintas.

11.- LICENCIAMIENTO

Respecto del licenciamiento en el marco de la normatividad vigente (Decreto Supremo N° 013-2003-PCM), que regula la legalidad del software, todo software incluido o pre-cargado, debe disponer de autorización o licencia legalmente emitida:

a. La UTI es la única autorizada para la instalación de software en toda la Zona Registral, cualquier requerimiento al respecto debe canalizarse a través de ella.
b. La UTI se encargará de la detección de faltas en la instalación de software por personal no autorizado.
c. Toda adquisición de software debe contar con la aprobación y verificación de la UTI y contar con un Informe Técnico Previo de Evaluación del Software
d. Los empleados o usuarios finales serán considerados responsables de la existencia de cualquier tipo de software en su computadora para el cual la organización carezca de las licencias apropiadas y que no haya sido instalado por personal autorizado.
e. De requerirse la instalación de algún software específico, el empleado realizará el pedido a través de su Jefe inmediato, quien dirigirá la Solicitud a la UTI.
f. El usuario puede solicitar la desinstalación de programas que no utiliza para que la licencia sea aprovechada por otro usuario.
g. El personal de la UTI es el único responsable de la instalación y desinstalación de software en toda la Zona Registral.
h. Todo software y actualizaciones de software que sean adquiridos, se documentarán e identificarán ante la UTI, quien verificará que la institución posea la licencia pertinente para usar dicho software.
i. Todas las adquisiciones de equipos informáticos que incluyan software integrado o preinstalado se documentarán e identificarán ante la UTI, quien verificará que la institución posea la licencia pertinente para usar dicho software.
j. El Jefe de la UTI designará a los empleados de su área autorizados a instalar software en las computadoras de la organización.
k. Ningún empleado de la UTI instalará o distribuirá software para el cual la organización carezca de la licencia apropiada.
l. Ningún empleado instalará actualizaciones de software en una computadora que no tenga instalada ya una versión original del software.
m. La UTI instruirá a los nuevos empleados de su área sobre cómo mantener la política de administración de software y licenciamiento.
n. La UTI guardará en un lugar seguro, centralizado, todas las licencias de software originales, discos, CD ROM y documentación al recibir el software.

12.- ADQUISICIÓN DE EQUIPAMIENTO, SOFTWARE Y LICENCIAS

Toda adquisición de equipo informático, licencias de uso de software, desarrollo de sistemas personalizados deben ser validados previamente por la Oficina General de Tecnologías de la Información. Los requerimientos sustentados deben contener una Anexo de Libre Disponibilidad.

Cualquier inobservancia al lineamiento constituye una falta que ameritará el deslinde de responsabilidades administrativas.

13.- ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN

En el marco de las nomas vigentes el Jefe de la Unidad Registral se constituye en propietario de la información registral y de la información gráfica registral(Base Gráfica)[1] y la UTI es el principal custodio de la información[2] almacenada en medios digitales, por ello se deben tener en cuenta los siguientes aspectos generales de seguridad.

CONTROL DE ACCESOS A LOS SISTEMAS DE INFORMACIÓN

Todos los usuarios de los sistemas informáticos de la Zona Registral deberán manejar una cuenta o identificador de usuario (ID) y una Contraseña, que les permita acceder a la información asignada según sus funciones, y que deberán estar regulados por procedimientos estándares de identificación, autenticación, autorización, registros de acceso y monitoreo.

La Unidad de Tecnologías de la Información realizará verificaciones periódicas de los derechos o privilegios de acceso otorgados a los usuarios en los sistemas de información, cada seis meses y/o cuando se requiera de manera inopinada.

GESTIÓN DE CONTRASEÑAS DE ACCESO DE USUARIOS

Las Contraseñas de Acceso de usuario tendrán carácter de "personal, intransferible y confidencial", por lo que cada usuario será responsable de toda actividad que se realice con su clave de acceso. Los usuarios deben ser conscientes de sus responsabilidades en el mantenimiento de la eficacia de las medidas de control de acceso y deben seguir buenas prácticas de seguridad para la selección y uso de sus contraseñas.

---

[1] PROPIETARIO DE LA INFORMACIÓN.- Es el directivo, área o unidad orgánica que administra en el marco de su competencia información y que cuenta con la capacidad de distribuir o proporcionar recursos, así como con la capacidad de autorización de recursos para el tratamiento de la información en su área a cargo.

[2] CUSTODIO DE LA INFORMACIÓN.- Es el empleado o la unidad que protege y resguarda la información.

RESPONSABILIDADES DEL PERSONAL

Todo el personal de la Zona Registral, es responsable de la seguridad y el uso racional y responsable de la información y de los recursos informáticos en los que se procesan y/o tenga acceso, según las funciones que tenga asignado.

RESPALDO DE LA INFORMACIÓN

Toda información de la Zona Registral debidamente clasificada como activo crítico o sensible en el Sistema de Gestión de Seguridad de la Información, debe ser respaldada en medios magnéticos mientras dure su vigencia, de acuerdo a los procedimientos establecidos. Se deben realizar regularmente copias de seguridad de toda la información esencial del negocio y del software, en concordancia con la política acordada de recuperación.

SALIDA DE INFORMACIÓN

La salida de los activos de información de las áreas de custodia ya sea copias completas o parciales de dicha información es restringida, deben contar con la autorización expresa del Propietario de Información, y con un respaldo documentario como registro de control.

CONFORMIDAD CON LA POLÍTICA DE SEGURIDAD

Los Jefes Zonales, Jefes de Unidades, Coordinadores de Catastro y propietarios de información deben asegurarse que se cumplan los procedimientos de seguridad en su área de responsabilidad, cumpliendo las políticas y estándares de seguridad, mediante revisiones regulares. El personal debe ser disuadido de utilizar los recursos de tratamiento de la información o activos informáticos para propósitos no autorizados.

PROCEDIMIENTOS COMPLEMENTARIOS

Todo procedimiento relativo a la seguridad de información que no esté reglamentado explícitamente, deberá contar con la autorización del responsable de la información y de acuerdo a su criticidad y alcance debe ser coordinado con el Oficial de Seguridad de la SUNARP.