POLÍTICAS DE SEGURIDAD DE ACTIVOS DE INFORMACIÓN PARA EL REGISTRO AGRARIO NACIONAL

ABRIL, 2014

AUTORIZÓ:

ING. JUAN DE DIOS GONZÁLEZ RUÍZ
Director General de Operación y Sistemas

ELABORÓ Y REVISÓ:

ING. JOSÉ MANUEL HERRERA PRECIADO
Director de Informática

Índice

I.- Introducción.

Uno de los aspectos fundamentales considerados en los objetivos estratégicos del Registro Agrario Nacional (RAN), versa sobre la implementación de una administración integral de información que permita estandarizar bajo las mejores prácticas, la información que emplea el RAN para el desarrollo de sus funciones. Por tal motivo, la institución ha establecido un proceso de trabajo que le ha permitido el desarrollo y adopción de esquemas y prácticas para asegurar no sólo la calidad en la información, sino su seguridad, disponibilidad y resguardo para reducir las vulnerabilidades a que se encuentra sujeta día a día.

La información es un activo fundamental para la institución, por ello, el aseguramiento de la misma y de los sistemas que la procesan es de gran importancia. Para llevar a cabo una adecuada gestión de la seguridad de la información dentro del RAN, es importante dar a conocer y difundir a su personal, las políticas de seguridad establecidas para el correcto uso de la información que emplean en el desarrollo de sus funciones.

Por ello, en cumplimiento al artículo 19 de la Ley Orgánica de la Administración Pública Federal; referente a la obligación que tienen las Secretarías de Estado de elaborar y actualizar sus Manuales de Organización Específicos y de Procedimientos y demás documentos administrativos, la Dirección General de Operación y Sistemas, a través de la Dirección de Informática, ha elaborado el presente documento con el propósito de instrumentar en el marco de su competencia, las políticas de seguridad sobre los activos de información y que sean el instrumento de apoyo para el adecuado desarrollo de las funciones y actividades encomendadas al personal de este Órgano Desconcentrado, salvaguardando en todo momento el correcto manejo de la información.

Bajo este contexto, es importante señalar que el presente documento ha sido conformado por un objetivo y alcance, así mismo, por políticas que establecen cada uno de los elementos que el personal del área debe conocer y aplicar en el desarrollo de sus funciones.

Cabe mencionar que, con el propósito de mantener actualizado el presente documento, se deberán realizar revisiones periódicas por parte del personal responsable, una vez al año o, en su caso, cuando existan modificaciones a los procesos sustantivos que se operan en el RAN.

Finalmente, es menester hacer hincapié que la observancia de las mejores prácticas para la salvaguarda de los activos de información del RAN, tienen un impacto directo y preventivo en la seguridad de los funcionarios a ella adscritos.

II.- Objetivo.

Dar a conocer las políticas que deberá adoptar el personal del RAN para proteger, resguardar y asegurar sus activos de información.

III.- Alcance.

Las presentes políticas son de aplicación obligatoria para el personal que integra cada una de las áreas adscritas al RAN y que tienen bajo su responsabilidad explotar, analizar, transmitir y valorar información generada por los sistemas y bases de datos internas y externas, medios de comunicación alámbrica e inalámbrica, así como el soporte y flujo documental que se requieren para el desarrollo y cumplimiento de sus funciones, siendo extensivas para el personal externo que en forma temporal o semipermanente preste sus servicios en el área.

IV.- Políticas.

Será responsabilidad de la Dirección de Informática:

a. Establecer, diseñar o implementar procedimientos que permitan administrar la seguridad de sus activos de información, contenida en medios electrónicos, sistemas de información, equipos de cómputo, bases de datos y soporte documental.
b. Mantener informados a sus colaboradores sobre las Políticas de Seguridad emitidas de manera interna sobre el correcto uso y manejo de todos los activos de información, de tal forma que todo el personal tenga plenamente identificado, dentro de sus funciones, las medidas de seguridad que deberá tomar en cuenta para salvaguardar dichos activos.
c. Revisar periódicamente las presentes políticas, de manera que se mantengan actualizadas ante posibles modificaciones a los procesos sustantivos que se operan en el área.
d. Establecer los mecanismos necesarios para la implementación de las disposiciones contenidas en las presentes políticas, así como para vigilar su cumplimiento.
e. Otorgar el apoyo para respaldar o borrar en forma segura la información contenida en equipos o dispositivos de almacenamiento que se den de baja, se reutilicen o entreguen a un tercero para reparación.
f. Actuar en consecuencia ante los eventos detectados acerca del incumplimiento de las presentes políticas, así como aquellos casos relacionados con incidentes de seguridad en la información.
g. Solicitar conforme a los procedimientos autorizados y vigentes, las cuentas de acceso a las aplicaciones, sistemas y recursos de activos de información del RAN, de acuerdo a las funciones previamente encomendadas.
h. Aplicar las políticas de dominio correspondiente para inhabilitar la funcionalidad de los puertos USB y dispositivos de grabación externa como CD/DVD, salvo en los casos que la Direccion General correspondiente conceda dicha funcionalidad.

i. Revisar los reportes de monitoreo mensual entregados por la Subdirección de Estrategia Tecnológica y detonar las acciones que se consideren necesarias cuando se detecten incidencias.

Será responsabilidad del personal adscrito al Registro Agrario Nacional:

a. Custodiar y proteger los recursos informáticos, documentación e información que por razón de su empleo, cargo o comisión, tenga bajo su resguardo, así como impedir y denunciar el uso, sustracción, destrucción, ocultamiento o utilización indebidos.
b. Enviar a las áreas competentes, las cartas responsivas ANEXO I debidamente firmadas, en donde cada usuario expresa su aceptación de la responsabilidad sobre el uso de los recursos (aplicativos o sistemas) para los fines que se encuentra facultado, así como el compromiso de no utilizarlos de forma indebida o dolosa en contra del RAN.
c. Solicitar la eliminación de las claves de usuario a los sistemas y aplicaciones otorgadas al personal del Registro Agrario Nacional que por cualquier razón se ausenten o dejen de prestar sus servicios en el área.
d. Hacer buen uso de la información que está a su alcance, la cual debe ser propia de las funciones que le fueron asignadas.
e. Mantener confidencialidad estricta respecto a los procesos, planes y datos en general a los que por sus funciones asignadas tenga acceso.
f. Salvaguardar todo tipo de información a la que por sus funciones asignadas tenga acceso, cuidando en todo momento tener un almacenamiento seguro de la misma, tanto de manera digital como física.
g. En casos de ausencia física en periodos mayores a dos semanas por motivos tales como vacaciones, incapacidad, comisión o la cesantía de labores en el área, el usuario deberá solicitar y/o realizar el bloqueo temporal o permanente, según sea el caso, de las cuentas autorizadas e informando a su superior inmediato.
h. Evitar realizar conexiones informáticas a redes institucionales o Internet en los equipos propiedad del RAN a través de mecanismos que no sean provistos por la Dirección de Informática, tales como servicios de banda ancha móvil (telcel, movistar, iusacel, o cualquier otro proveedor) contratados por el propio usuario para utilizar a través de teléfonos celulares, tabletas electrónicas, equipos de cómputo propio, etc.
i. Evitar hacer uso de dispositivos extraíbles como USB, discos duros u ópticos y dispositivos de acceso remoto sin previa autorización por escrito de la Dirección General correspondiente donde indique el motivo de la necesidad operativa.
j. Queda prohibido enviar información propiedad del RAN a cuentas de correo externas propias o ajenas (hotmail, gmail, yahoo o cualquier otro proveedor), tabletas electrónicas, acceso al correo electrónico interno y/o Communicator desde una conexión pública o de Internet (OWA-Outlook Web Access) u otros dispositivos, así como compartir recursos tales como redes inalámbricas, carpetas electrónicas, etc., sin previa justificación y autorización por escrito de su superior inmediato.
k. Evitar acceder a sitios restringidos de Internet, tales como redes sociales, blogs, correos personales, etc. sin previa autorización por escrito del Director General del área que pertenezca.

l. Evitar el uso de cualquier instrumento de software o hardware que intente anular las políticas de seguridad instrumentada por la Direccion de Informática, tales como proxys, surf anónimos, vpns.
m. Evitar utilizar los recursos de comunicación institucionales para fines distintos a las funciones encomendadas.
n. Realizar la solicitud a la Dirección de Informática para que la información contenida sea borrada en forma segura o transferida según las indicaciones del superior, en los casos que algún equipo sea reutilizado o entregado a un tercero para reparación.
o. Evitar descargar e instalar software ajeno a las aplicaciones institucionales.
p. Evitar compartir, prestar o asignar cuentas de acceso, contraseñas, certificados digitales y otros mecanismos de autenticación a sistemas y aplicaciones del RAN, ya que son de carácter personal, confidencial e intransferible, y sujetas a monitoreo para ser auditadas en el momento en que se requiera o se determine que los activos de información están en riesgo.
q. Verificar que su equipo de cómputo asignado tenga configurado y activado el protector de pantalla con contraseña a los 10 min de inactividad, con la finalidad de evitar el acceso por un tercero no autorizado a su información.
r. Notificar al jefe inmediato o al Director del área cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido modificada, alterada o borrada.
s. Dejar su equipo de cómputo encendido los días miércoles para permitir tareas automatizadas de mantenimiento del mismo, actualizaciones de sistema operativo y escaneo del antivirus.
t. Conducirse en todo momento con estricto apego a las presentes Políticas.

El incumplimiento a las presentes políticas que en materia de seguridad de la información se encuentran contenidas de manera enunciativa más no limitativa en el presente documento, podrá dar lugar a consecuencias legales que conforme a la legislación federal vigente en materia de responsabilidades administrativas y/o penales apliquen las autoridades competentes, con fundamento en el artículo 13 de la Ley de Federal de Responsabilidades Administrativa de los Servidores Públicos vigente.

VII.- Glosario

SEDATU: Secretaria de Desarrollo Agrario, Territorial y Urbano
RAN: Registro Agrario Nacional
DGOS: Dirección General de Operación y Sistemas
Políticas: Políticas de seguridad en la información.
Personal: Cada una de las personas que laboran en el RAN.
Personal externo: Personal que presta sus servicios dentro del RAN y conoce del funcionamiento de la misma (proveedores, servicio social, outsorcing por honorarios etc.)
OWA: Outlook Web Access – Mecanismo de acceso vía Internet al correo institucional, a través de un equipo de cómputo o teléfono celular, desde un punto externo a las instalaciones.

VIII.- Anexos

ANEXO I

DIRECCIÓN GENERAL DE OPERACIÓN Y SISTEMAS
DIRECCION DE INFORMÁTICA

CARTA RESPONSIVA DE LA CUENTA DE ACCESO AL SISTEMA INTERNET

México, [illegible]es, 08 de mayo de 2014

Por este medio, quién suscribe C.JOSÉ MANUEL HERRERA PRECIADO con clave de R[illegible]ederal de Contribuyente HEPM700904K36 , declaro que recibo en este acto, de la Dirección de Informática, la cuenta de usuario c[illegible]identific[illegible]a acceder al sistema denominado INTERNET

El uso y manejo de la cuenta de usuario recibida en dicho acto y mi prop[illegible]onu[illegible]ña establecida, lo haré de conformidad con el Manual Administrativo de Aplicación General en Materia de Tecnologías de la I[illegible]rmación y [illegible]municac[illegible]ones (acuerdo expedido por el D.O.F.13-VII-2010).

Así mismo me manifiesto sabedor de que esta cuenta asignada y [illegible]ropia c[illegible]ña establecida, son únicamente para el uso exclusivo del desempeño de mis funciones como empleado a servicio d[illegible]egistro A[illegible]o Nacional y que el uso distinto de estas, implica un quebranto a la normatividad vigente relacionada con el control de cuentas [illegible]cceso a siste[illegible]e información institucionales.

Por lo anterior, quedo apercibido de la obligación de dar cump[illegible]o a la n[illegible]atividad aplicable en la materia respecto al uso adecuado de la cuenta de usuario asignada y mi propia contraseña estab[illegible] y que[illegible]gado a guardar absoluta y estricta confidencialidad de la información y documentación que conozca con motivo del uso de las[illegible]mas, en[illegible]o de las responsabilidades civiles y penales a las que me haré acreedor al quebrantar la citada reserva, asi como al m[illegible]car, copia[illegible]izar o sustraer ilícita y/o indebidamente, inutilizar, destruir o provocar pérdida de la información contenida en los sistemas o ec[illegible]s de informátic[illegible] Registro Agrario Nacional, violentando lo contenido en los articulos 7, 8 fracción V y 13 de la Ley Federal de Responsabilid[illegible] Adm[illegible]rativas[illegible]os Servidores Públicos, contenido en los articulos 210 y 211BIS 1, 211 BIS 2, 211 BIS 3 y 214 del Código Penal Federal, asi c[illegible]s demá[illegible]delitos que puedan resultar.

En este acto, asumo el compromiso del buen uso[illegible]cuenta asignada y mi propia contraseña establecida por mi y me obligo a no revelarlas bajo ningún concepto, declarándome responsable de su uso y de la información que con ellas se conozca, sustraiga, modifique o altere en los sistemas de información del Registro Agrario Nacional.

Con mi nombre y firma autógrafa garantizo el legal uso de la cuenta de usuario asignada de mi propia contraseña establecida personalmente en este acto.

NOMBRE COMPLETO (escrito de manera autografa) FIRMA