RESOLUCION DE LA SUPERINTENDENTA NACIONAL DE LOS REGISTROS PÚBLICOS Nº 060-2010-SUNARP/SN

Lima, 17 MAR. 2010

Visto el Informe Nº 28-2009-SUNARP/GI por medio del cual la Gerencia de Informática de la Sede Central pone a consideración el Reglamento de Políticas de Seguridad de la Información aprobado por el Comité de Gestión de Seguridad de la Información en su Acta de Reunión Nº 003-2009-CGSI;

CONSIDERANDO:

Que, la información generada en la Superintendencia Nacional de los Registros Públicos constituye un activo que corresponde ser protegida bajo los criterios de buenas prácticas en gestión de la seguridad establecida para este fin;

Que, la Resolución Ministerial Nº 246-2007-PCM, aprobó la segunda edición de la Norma Técnica Peruana "NTP_ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición" y aprueba su uso obligatorio en todas las entidades integrantes del sistema nacional de informática, de la cual forma parte la Superintendencia Nacional de los Registros Públicos;

Que, el Reglamento de Seguridad de la Información de la Superintendencia Nacional de los Registros Públicos – SUNARP, aprobado por el Comité de Gestión de la Seguridad de la Información constituye un documento que debe ser incorporado para implementar la norma técnica peruana NTP-ISO/IEC 17799:2007 EDI.

De conformidad con lo dispuesto en los literales m) y v) del artículo 7º del Estatuto de la Superintendencia Nacional de los Registros Públicos – SUNARP, aprobado con Resolución Suprema Nº 135-2002-JUS;

Con la visación de la Gerencia General, Gerencia Legal, Gerencia de Informática y de Presupuesto y Desarrollo;

SE RESUELVE:

Artículo Primero.- Aprobar el Reglamento de Seguridad de la Información de la Superintendencia Nacional de los Registros Públicos – SUNARP, el mismo que forma parte de la Presente Resolución.

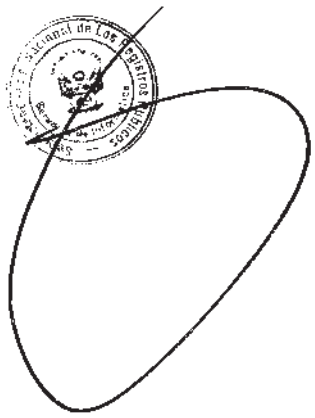
Artículo Segundo.- Las Gerencias de Informática o las que hagan sus veces, dentro del ámbito de su competencia, son responsables de comunicar y difundir entre el personal a su cargo el nuevo Reglamento de Políticas de Seguridad de la Información aprobada en el Artículo primero.

Artículo Tercero.- Encargar a la Gerencia de Imagen Institucional y Relaciones Públicas la publicación de la presente Resolución en el Portal Web y en la intranet de la Superintendencia Nacional de los Registros Públicos.

Regístrese y comuníquese.

María D. Camboursano Garagorri
Superintendente Nacional
de los Registros Públicos

REGLAMENTO DE SEGURIDAD DE LA INFORMACIÓN DE LA SUPERINTENDENCIA NACIONAL DE REGISTROS PÚBLICOS (SUNARP)



INDICE

TITULO I
DISPOSICIONES GENERALES

Artículo 1º.- Objetivo
Artículo 2º.- Base Legal y Normativa
Artículo 3º.- Ámbito de Aplicación
Artículo 4º.- Roles y Funciones de Seguridad de la Información
Artículo 5 º.- Glosario

TITULO II
CAPITULO I. PROPIEDADES DE LA INFORMACIÓN

Artículo 6°.- Confidencialidad
Artículo 7°.- Integridad
Artículo 8°.- Disponibilidad

TITULO III
CAPITULO I. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Artículo 9°.- Política de Seguridad de la Información

CAPÍTULO II. REVISIÓN DE POLITICAS Y DIRECTIVAS DE SEGURIDAD DE LA INFORMACIÓN
Artículo 10°.- Objetivo
Artículo 11°.- Revisión de Políticas y Directivas de Seguridad de la Información

CAPÍTULO III. SEGURIDAD FÍSICA Y AMBIENTAL

Artículo 12°.- Objetivo
Artículo 13°.- Seguridad Física y Ambiental

CAPÍTULO IV. CONTROL DE ACCESOS A LOS SISTEMAS DE INFORMACIÓN Y RECURSOS INFORMÁTICOS

Artículo 14°.- Objetivo
Artículo 15°.- Control de Accesos
Artículo 16°.- Selección y uso de contraseñas o claves de acceso de usuarios

CAPÍTULO V. SEGURIDAD DE LA INFORMACIÓN CONFIDENCIAL DEL PERSONAL

Artículo 17º.- Objetivo
Artículo 18º.- Protección de datos y privacidad de la información personal
Artículo 19º.- Riesgos de Seguridad de los Servicios Ofimáticos

CAPÍTULO VI. CONTRATOS CON TERCEROS

Artículo 20°.- Objetivo
Artículo 21°.- Contratos

CAPÍTULO VII. ADMINISTRACIÓN DE ACTIVOS DE INFORMACIÓN

Artículo 22°.- Objetivo
Artículo 23°.- Administración de equipos informáticos
Artículo 24°.- Retención de Registros
Artículo 25°.- Informática Móvil
Artículo 26°.- Pantalla y Escritorio Limpio
Artículo 27°.- Intercambio de Voz, Fax y/o Video
Artículo 28°.- Protección de Información Registral

CAPÍTULO VIII. SEGURIDAD DE LAS COMUNICACIONES

Artículo 29°.- Objetivo
Artículo 30°.- Acceso a Directorios de Red
Artículo 31°.- Uso de Servicios de Red
Artículo 32°.- Servicios Especiales
Artículo 33°.- Uso de Correo Electrónico
Artículo 34°.- Controles Criptográficos
Artículo 35°.- Transmisión de Información
Artículo 36°.- Acceso a Páginas Web Especiales
Artículo 37°.- Acceso a entornos Web

CAPÍTULO IX. DESARROLLO, ADQUISICIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Artículo 38°.- Objetivo
Artículo 39°.- Planificación y Aceptación de Sistemas
Artículo 40°.- Protección contra software malicioso
Artículo 41°.- Mantenimiento de Sistemas

CAPÍTULO X. CONTINUIDAD DE OPERACIONES

Artículo 42°.- Objetivo
Artículo 43°.- Definir, Revisar y Actualizar el Plan de Continuidad de Negocios

CAPÍTULO XI. MANEJO DE INCIDENCIAS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN

Artículo 44°.- Objetivo
Artículo 45°.- Respuesta ante Incidencias y Debilidades de Seguridad de la Información

TÍTULO I
DISPOSICIONES GENERALES

Artículo 1°.- Objetivo
Integrar los lineamientos de seguridad de la información, asegurando la confidencialidad, disponibilidad e integridad de la información almacenada y procesada mediante los recursos informáticos con que cuenta la SUNARP, minimizando los riesgos y asegurando la continuidad del negocio.

Artículo 2°.- Base Legal

- NORMA TÉCNICA PERUANA NTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. ed.
- Resolución Ministerial N° 246-2007-PCM Aprueban uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la gestión de la seguridad de la información.2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.

Artículo 3°.- Ámbito de Aplicación
Corresponde a:

- Todo personal que labore en la SUNARP bajo cualquier modalidad de contrato.
- Proveedores y su personal e Instituciones con las que la SUNARP firma Convenios de Colaboración Interinstitucional y su personal.

Artículo 4°.- Responsabilidades en temas de Seguridad de la Información
Las actividades de seguridad de la Información deben coordinarse con representantes de diferentes unidades orgánicas de la Institución con roles y funciones de trabajo pertinentes.

La seguridad de la Información en la SUNARP está a cargo de: El Comité de Gestión de Seguridad de la Información, Equipo de Trabajo, Responsable de Seguridad de la Información (Oficial de Seguridad de la Información), Propietarios, Custodios y Usuarios, cuyas responsabilidades se describen en las siguientes líneas.

El Comité de Gestión de Seguridad de la Información tiene las siguientes funciones y/o responsabilidades según Resolución N° 321-2008-SUNARP/SN:

a. Formular, revisar y aprobar la política de seguridad de información.
b. Evaluar y proponer a la Superintendencia Nacional la política, directivas y responsabilidades generales en materia seguridad de información.
c. Asegurar que las metas de la seguridad de información sean identificadas.
d. Revisión de la efectividad en la implementación de la política de información y; en su caso, adoptar las medidas necesarias para que esta sea cumplidas.
e. Garantizar que la seguridad de la información sea parte del proceso de planificación de la información.
f. Evaluar, coordinar y monitorear la implementación de controles específicos de seguridad de la información para los sistemas o servicios actuales o nuevos.
g. Promover y disponer la difusión y apoyo a la seguridad de la información al interior de la SUNARP.
h. Proveer direcciones claras y un visible apoyo en la gestión para iniciativas de seguridad.

i. Iniciar planes y programas para mantener la conciencia en seguridad de información entre el personal de la SUNARP.
j. Asegurar que la implementación de los controles de la seguridad información sea coordinada a través de la SUNARP.
k. Identificar y proponer los cambios en seguridad de información en respuesta a los cambios del ambiente organizacional, circunstancias del negocio, condiciones legales o cambios en el ambiente técnico.
l. Las demás funciones que se le encarguen, y otras necesarias para cumplir con las disposiciones contenidas en la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información 2° edición".

El Equipo de Trabajo tiene las siguientes funciones y/o responsabilidades:

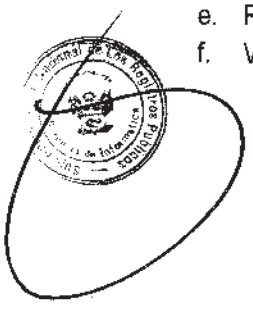
a. Evaluar metodologías, herramientas y procesos para la seguridad de la información
b. Evaluar la estrategia de capacitación y entrenamiento en seguridad de la información.
c. Evaluar los reportes de indicadores consolidados así como la efectividad de los controles implementados.
d. Evaluar la propuesta del responsable de seguridad de la información (Oficial de Seguridad de la Información) para la implementación de controles

Responsable de Seguridad de la Información (Oficial de Seguridad de la Información)

a. Supervisar el cumplimiento de las políticas y controles de seguridad de la información.
b. Proponer metodologías, herramientas y procesos para la seguridad de la información.
c. Definir la estrategia de capacitación y entrenamiento. Así como preparar los programas de capacitación de seguridad de la información.
d. Evaluar los incidentes y vulnerabilidades de la seguridad de la información a fin de identificar los controles a implementar.
e. Coordinar con los propietarios de los activos la ejecución de los procesos de análisis y evaluación de riesgos.
f. Comunicar al equipo de trabajo las amenazas, incidentes y debilidades emergentes. Así como la efectividad de los controles implementados.
g. Elaborar y actualizar el Plan de Seguridad de la Información.

Propietario

a. Identificar y Clasificar los activos de su propiedad.
b. Determinar los periodos de retención de los activos de información (electrónica e impresa).
c. Determinar los criterios y niveles de acceso a los activos de su propiedad.
d. Revisar periódicamente la clasificación de la información con la finalidad de verificar el cumplimiento de los requerimientos de seguridad de la Institución.
e. Revisar periódicamente los niveles de acceso de los usuarios a los activos de su propiedad.
f. Verificar que los controles de seguridad aplicados sean consistentes con la clasificación realizada.



g. En coordinación con el Responsable de Seguridad de la Información (Oficial de Seguridad de la Información), revisar y evaluar los resultados de la implementación de controles aplicados a los activos de su propiedad.

Custodio de la Información (electrónico y físico)

a. Dar acceso a los usuarios de acuerdo con las especificaciones establecidas por los propietarios.
b. Administrar los accesos a los activos.
c. Cumplir con los controles implementados para la protección de los activos asignados para su custodia.

Usuario

a. Cumplimiento a las políticas y directivas de seguridad de la información.
b. Mantener la confidencialidad de las contraseñas para el acceso a aplicaciones, sistemas de información y recursos informáticos.
c. Utilizar la información de la SUNARP sólo para el cumplimiento de sus funciones y/o fines de institucionales.
d. Reportar incidentes y debilidades de seguridad de la información.
e. En caso de identificar oportunidades de mejora, debe comunicarlas a los responsables de Seguridad de la Información (Oficial de Seguridad de la Información).

Artículo 5º.- Glosario de Términos

Para la interpretación adecuada del presente reglamento se debe tener en cuenta las definiciones establecidas en la Norma ISO/IEC 27001, la NTP-ISO/IEC 17799:2007 y las que listan a continuación:

- ***Clasificación de información.-*** Es un proceso que permite asignar un nivel de protección adecuada a los activos de información, de acuerdo a su nivel de confidencialidad, integridad y disponibilidad.
- ***Custodio de la información.-*** Es el empleado o la unidad que protege y resguarda la información.
- ***Encriptación.-*** Medida de seguridad que permite codificar y decodificar la información de la SUNARP, de tal manera que no sea legible o fácil de entender por personas no autorizadas.
- ***Perfil de usuario.-*** Es el nivel de autorización a la información de la SUNARP que se le asigna a un empleado de acuerdo a las funciones encomendadas.
- ***Plan de Continuidad.-*** Conjunto de procedimientos a seguir en caso se presente una ocurrencia inesperada, permitiendo asegurar la continuidad de los procesos de negocio.
- ***Propietario de la información.-*** Es el empleado de la Unidad Orgánica dueña de la información que le fuera asignada para el desempeño de las actividades a su cargo.
- ***Riesgo informático.-*** Es la posibilidad de ocurrencia de alguna situación inesperada que no permita operar normalmente los medios de tecnología de información.

TÍTULO II

CAPITULO I. PROPIEDADES DE LA INFORMACIÓN

Artículo 6º.- Confidencialidad
Sólo las personas autorizadas podrán tener acceso a la información clasificada, teniendo en cuenta los criterios que sobre el particular se establecen en las normas internas.

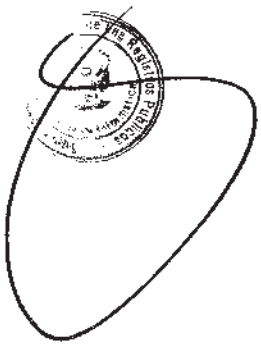
Artículo 7º.- Integridad
Toda información que la SUNARP genere, procese, resguarde y distribuye, deberá contar con adecuados mecanismos de protección para que no sea alterada voluntaria e involuntariamente de forma no autorizada.

Artículo 8º.- Disponibilidad
La información necesaria para realizar las funciones de la SUNARP, deberá estar disponible donde y cuando sea requerida por los usuarios autorizados de la información y deberá ser confiable.

TÍTULO III

CAPITULO I. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Artículo 9º.- Dirigir y dar soporte a la gestión de la seguridad de la información de acuerdo con los requerimientos del negocio, las leyes y las regulaciones.



SUNARP

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

SUNARP es el ente rector del Sistema Nacional de Registros Públicos y está encargada de otorgar seguridad jurídica y brindar certidumbre respecto a la titularidad de los diferentes derechos que en él se registran.

SUNARP reconoce a la información como activo importante, con la finalidad de mantener su integridad, confidencialidad y disponibilidad, cuenta con un Sistema de Gestión de Seguridad de Información, cuyo alcance corresponde a los siguientes procesos: **Administrativo - Financiero y Presupuestal, Catastro, Registral y Servicios Informáticos de Tecnología de Información de la SUNARP.**

El Sistema de Gestión de Seguridad de la Información se basa en los siguientes lineamientos:

- Cada unidad orgánica tiene la responsabilidad de garantizar la integridad, confidencialidad e disponibilidad de la información que producen o utilizan en el marco de sus competencias.
- Cada unidad orgánica en coordinación con el Responsable de Seguridad de la Información (Oficial de Seguridad de la Información) debe proponer, diseñar, coordinar la implementación de los controles eficaces en sus procesos y actividades, manteniendo un equilibrio entre la productividad y la seguridad de la información.
- El Comité de Seguridad de la Información debe aprobar los lineamientos del sistema de gestión de seguridad de la información, proveer los recursos necesarios para su implementación y verificar su eficacia.
- El Equipo de Trabajo debe proponer los lineamientos del sistema de gestión de seguridad de la información y coordinar con el Comité de Seguridad de la Información la aprobación de los mismos.
- El Responsable de Seguridad de la Información (Oficial de Seguridad de la Información) debe supervisar la implementación y ejecución de los controles y políticas de seguridad de la información. Asimismo, gestionar los incidentes de seguridad de la información.
- Todo trabajador que labore, preste o reciba servicios en la SUNARP (personal que labora en la SUNARP, proveedores y su personal e Instituciones con las que la SUNARP firma Convenios de Colaboración Interinstitucional y su personal) debe manejar adecuadamente la información, de acuerdo a los parámetros definidos por la Institución.
- Todo trabajador que labore, preste o reciba servicios en la SUNARP (personal que labora en la SUNARP, proveedores y su personal e Instituciones con las que la SUNARP firma Convenios de Colaboración Interinstitucional y su personal) debe comunicar al Responsable de la Seguridad de la Información (Oficial de Seguridad de la Información), cualquier incidente o debilidad de la seguridad de la información.
- La SUNARP debe comunicar a las Instituciones con las que ha firmado Convenios de Colaboración Interinstitucional y a sus proveedores los lineamientos de Seguridad de la información de la Institución.
- Capacitar y sensibilizar periódicamente al personal de la SUNARP en temas, métodos y herramientas de seguridad de la Información.
- En caso de incumplimientos, se sancionará a los responsables teniendo como referencia el Reglamento Interno de Trabajo, contratos y convenios firmados.

Aprobado por resolución No ..... de fecha .....

CAPITULO II. REVISIÓN DE POLÍTICAS Y DIRECTIVAS DE SEGURIDAD DE LA INFORMACIÓN

Artículo 10°.- Objetivo

Mantener vigentes los documentos de seguridad de la información, teniendo en cuenta la periodicidad de la revisión de los mismos.

Artículo 11°.- Política de Revisión de Políticas y Directivas de Seguridad de la Información

11.1 Los documentos de seguridad de la información deben ser revisados regularmente a intervalos planeados (cada 6 meses) o si ocurren cambios significativos para asegurar su adecuación, y efectividad continua.

11.2 Los responsables de la revisión, actualización y aprobación de los documentos será de acuerdo a lo establecido en la Directiva para la Formulación, Aprobación y Control de Documentos Administrativos.

CAPÍTULO III. SEGURIDAD FÍSICA Y AMBIENTAL

Artículo 12°.- Objetivo

Establecer pautas y lineamientos necesarios para evitar el ingreso de personas no autorizadas a la institución con el fin de impedir daño al personal y pérdida de los activos de la información; asimismo, evitar la interrupción de las actividades de los procesos de la institución.

Artículo 13°.- Política de Seguridad Física y Ambiental

13.1 El personal de Seguridad y Vigilancia debe controlar el ingreso a la Institución mediante el uso de la credencial entregada. La misma que deberá mostrarse en un lugar visible.

13.2 Cada responsable de la Unidad Orgánica en coordinación con el Responsable de Seguridad de la Información (Oficial de Seguridad de la Información) debe identificar las zonas que requieren mayor nivel de seguridad de acuerdo con la criticidad o clasificación de la información que almacenan de manera permanente o temporal. La actualización las zonas se realizará en función de los cambios estructurales y físicos en la institución.

13.3 El Responsable de Seguridad de la Información (Oficial de Seguridad de la Información) en coordinación con el Personal de Seguridad Física deben supervisar y verificar respectivamente que las zonas que requieren mayor nivel de seguridad cumplan con los requerimientos de acceso físico.

13.4 El acceso a las áreas seguras es restringido y está bajo la responsabilidad de la unidad orgánica respectiva.

13.5 Cada unidad orgánica en coordinación con el Responsable de Seguridad de la Información (Oficial de Seguridad de la Información) debe proponer, diseñar, coordinar la implementación de controles de acceso físico a la información dependiendo de su clasificación.

13.6 Toda persona que labore, preste o reciba servicios en la SUNARP (personal que labora en la SUNARP, proveedores y su personal e Instituciones con las que la SUNARP firma Convenios de Colaboración Interinstitucional y su personal) detecta la presencia de personal no autorizado debe comunicar el hecho al personal de Seguridad y Vigilancia de la SUNARP.

13.7 La visita de personas externas a la Institución debe concluir con la entrega de la Papeleta firmada por la persona que autorizo el ingreso.

CAPITULO IV. CONTROL DE ACCESOS A LOS SISTEMAS DE INFORMACIÓN Y RECURSOS INFORMÁTICOS

Artículo 14º.- Objetivo
Establecer pautas que permitan controlar el acceso a los sistemas de información y recursos informáticos, gestionar los privilegios de usuarios y generar los registros (logs) que permitan mantener los accesos autorizados a los sistemas de información y recursos informáticos sobre la base de los requisitos de seguridad y del negocio.

Artículo 15°.- Política de Control de Accesos

15.1 El acceso a los servicios y recursos informáticos (aplicaciones, sistemas de información, archivos de red, correo electrónico, Internet, telefonia) debe ser solicitado al personal del Área de Informática a través del formato establecido en la directiva para la Gestión de Acceso a Usuarios que estará disponible en el File server. Estos formatos serán elaborados y actualizados por el área en mención. Cualquier requerimiento de cambio de estado a los privilegios de acceso a los recursos informáticos deberán realizarse utilizando el formato antes mencionado.

15.2 Los usuarios no deben utilizar o permitir que un tercero utilice las computadoras y/o recursos informáticos que se les ha asignado. El Responsable de Seguridad de la Información (Oficial de seguridad de la información) en coordinación con el jefe inmediato de cada área deben verificar que se cumpla con este lineamiento.

15.3 El acceso a las redes y recursos informáticos de la Institución será provisto únicamente a usuarios debidamente autorizados.

15.4 La unidad orgánica que dispone las altas y destaques del personal debe comunicar este hecho inmediatamente al área de Recursos Humanos y de Informática. Luego el área de Informática en un plazo de un día hábil debe realizar los cambios, creaciones y/o eliminaciones de accesos y privilegios.

15.5 Recursos Humanos debe comunicar a Informática la relación del personal que sale de vacaciones para el retiro parcial de los accesos a los sistemas de información.

15.6 En caso de despido inmediato, en la fecha en que se elabora la Carta de Despido, Recursos Humanos solicitará a Informática el retiro de todos los accesos a los sistemas y recursos de información que fueron asignados. El retiro de los accesos se debe realizar en un plazo máximo de un día laboral.

15.7 La suspensión y bajas de personal deben ser comunicados por la Jefatura de Recursos Humanos, al personal del área de Informática, inmediatamente. El personal del área de Informática debe canalizar este requerimiento a través del formato establecido, para finalmente proceder a realizar los cambios y/o eliminaciones de accesos, privilegios y nombre de usuario de todos los servicios y recursos informáticos asignados con anterioridad.

15.8 Cada unidad orgánica en coordinación con el Responsable de Seguridad de la Información (Oficial de Seguridad de la Información) y con Informática debe establecer y mantener los perfiles de acceso a los recursos informáticos y de los sistemas de información de acuerdo con los cargos y funciones del personal.

15.9 La asignación de Perfiles debe ser realizada por el responsable de la Unidad Orgánica asignado, de acuerdo con lo establecido en la política anterior (15.8)

15.10 Informática deber habilitar los accesos y privilegios con perfiles estandarizados según las categorías comunes de trabajo así como monitorear los registros o bitácoras de auditorías de accesos a los sistemas de información.

15.11 El acceso de terceros (personal ajeno a la institución) a la red y a sus servicios deben ser solicitados, por los jefes de las unidades orgánicas responsables del tercero, al personal del área de Informática. El personal del área de Informática debe canalizar este requerimiento a través del formato establecido, para finalmente proceder a realizar los cambios y/o eliminaciones de accesos y privilegios.

15.12 La documentación electrónica generada por los usuarios, durante sus actividades y desarrollo de sus funciones, inicialmente será almacenada en la carpeta "D:\mis documentos" de las computadoras asignadas. Periódicamente se deberá almacenar los documentos definitivos e importantes en el File server (unidad L). Asimismo, se prohíbe almacenar información no relacionada a la Institución.

Artículo 16°.- Política de Selección y uso de contraseñas o claves de acceso de usuarios

16.1 El acceso a Red y a los Sistemas de Información a través de las computadoras, tiene como mecanismos de acceso, la utilización de una clave de red, tarjeta u otros mecanismos. Dicho mecanismo de acceso es personal e intransferible y sólo deberá ser utilizado por el usuario del equipo, quien será el único responsable de su confidencialidad. (Los usuarios deben proteger la privacidad de las claves de red, tarjetas u otros mecanismos de acceso y autenticación a los servicios informáticos de la SUNARP).

16.2 Los usuarios deben tener en cuenta los siguientes criterios a fin de elegir adecuadamente las claves de encendido y de acceso a la Red:

a) No usar contraseñas que sólo sean palabras (aunque sean extranjeras), nombres y/o apellidos (del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares u otro relacionado).
b) No usar contraseñas completamente numéricas con algún significado (teléfono, D.N.I., fecha de nacimiento, otros).
c) La selección y generación de contraseñas debe combinar caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.
d) Informática debe supervisar que los usuarios cumplan con los criterios mencionados anteriormente para la elección adecuada de las claves de encendido y acceso a la red.

16.3 La Clave de Red deben tener una longitud de 6 caracteres alfanuméricos como mínimo y de 14 como máximo. No está permitido el uso de claves en blanco. Deberá ser cambiada cada 45 días. El sistema debe estar programado para que dicho cambio sea solicitado a cada usuario en forma automática.

16.4 Al tercer intento fallido utilizando una clave incorrecta, quedará bloqueado el acceso a la Red para el usuario a quien pertenece dicha contraseña. El bloqueo podrá levantarse por disposición de Informática, previa solicitud escrita del usuario o del responsable del área respectiva.

16.5 Los usuarios no deberán escribir la clave en un papel o agenda, deben procurar memorizarla. Asimismo, deberán adoptar las medidas necesarias para evitar que alguna otra persona (incluyendo al personal de informática) pueda ver su clave al momento de digitarla. En caso que ocurriese, se debe cambiar la clave nuevamente.

16.6 El área de Informática poseerá una 'Clave de Administrador' para poder acceder y/o cambiar dicha clave, ante necesidad justificada, previa solicitud y autorización escrita del Jefe del área involucrada.

16.7 Los usuarios deben cambiar inmediatamente la clave de acceso a la red y a los sistemas de información brindados por personal del área de Informática, que supervisará que los usuarios cambien sus claves de acceso a la red y a los sistemas de información de manera inmediata.

16.8 Informática debe supervisar que los usuarios cambien sus claves de acceso a la red y a los sistemas de información de manera inmediata.

16.9 Personal de Soporte y Producción del área de Informática deben implementar los controles de acceso a los recursos informáticos, enfocándose en claves de acceso a la red y a los Sistemas de Información de forma alfanumérica, cuentas privilegiadas con cambios de contraseñas periódicas, bloqueo de sesión automático y desbloqueo con clave o huella, entre otros.

16.10 Los usuarios no deben fumar o ingerir alimentos o bebidas, cuando se encuentren frente al teclado o cerca a orificios o rejillas de ventilación de los equipos. El Jefe de cada área deberá verificar el cumplimiento del presente ítem. Cualquier desperfecto imputable a estas conductas serán de responsabilidad única del usuario y dará lugar a que se le cargue a éste el costo de reparación correspondiente.

16.11 Los usuarios, al finalizar su labor diaria, deben apagar los equipos de cómputo (incluyendo estabilizadores y supresores de picos de ser el caso) que tienen asignados. En caso tenga un equipo compartido (impresoras, por ejemplo) debe coordinar con las personas que utilizarán dicho recurso posterior a su salida, para que éste sea correctamente apagado. El personal de Seguridad y Vigilancia será el encargado de verificar que los equipos queden apagados al finalizar el día de trabajo.

CAPÍTULO V. SEGURIDAD DE INFORMACIÓN CONFIDENCIAL DEL PERSONAL

Artículo 17°.- Objetivo

Establecer pautas y lineamientos respecto a la información confidencial del personal que labora en la Institución de manera que estos, puedan administrar adecuadamente los activos de información de la SUNARP.

Artículo 18°.- Política de Protección de datos y privacidad de la información personal

18.1 La recolección de datos personales no puede hacerse por medios desleales, fraudulentos, en forma contraria a las disposiciones de ley o sin el consentimiento del titular o persona natural a la que están referidos.

18.2 Los datos personales deben utilizarse para los fines que han sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público según lo señalado en la Ley de Transparencia y Acceso a la Información Pública (Ley N° 27806).

18.3 Los datos personales, que revelan origen racial y étnico, convicciones políticas y religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual, sólo pueden ser recolectados y ser objeto de tratamiento cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

18.4 Los datos personales deben ser almacenados en áreas seguras, ya sean físicas (restringiendo el acceso a personal no autorizado y haciendo uso de mecanismos de protección que garanticen la privacidad, legitimidad, confidencialidad e integridad), o lógicas (haciendo uso de privilegios para el acceso a las redes, sistemas de información, aplicaciones y/o bases de datos que contengan datos personales).

18.5 El área de Recursos Humanos será la responsable del registro de datos personales, y de supervisar la implantación de medidas técnicas y organizativas que resulten necesarias para garantizar la integridad, disponibilidad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado.

18.6 El área de Informática asesorará al área de Recursos Humanos en la implementación de controles de seguridad de la información usando las tecnologías de información y comunicaciones.

18.7 Los datos personales sólo podrán ser revelados a una autoridad pública, solicitados por mandato judicial salvo que medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Artículo 19°.- Política de Riesgos de Seguridad de los Servicios Ofimáticos

19.1 Cada usuario es responsable de recoger inmediatamente los documentos que imprima en las impresoras asignadas, a fin de mantener la reserva de la información, ya que podrían ser recogidas por personal de otras áreas o externos que no tendrían ningún tipo de injerencias en ellas. Asimismo, en el caso de información de uso interno y confidencial se deberá considerar lo señalado en la directiva "Establecimiento de Niveles de Confidencialidad y Gestión de Activos".

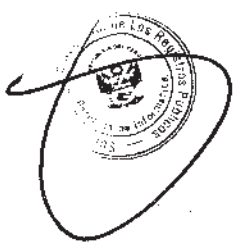
19.2 Los usuarios que generen información de uso interno y/o confidencial no deben enviar dicha información por fax u otro medio, a menos que cuenten previamente con la autorización del propietario de la información y con conocimiento del receptor de la transmisión. Asimismo, se deberá consignar que tipo de información (de uso interno y/o confidencial) se está transmitiendo.

19.3 Es responsabilidad de cada área, el destruir las impresiones que ya no sirven y que contienen información de uso interno y/o confidencial usando algún mecanismo de eliminación segura de información.

19.4 Los usuarios y/o áreas deben ubicar los servicios ofimáticos a su cargo y/o custodia (impresoras, fax, fotocopiadoras, etc.) en ambientes controlados para evitar que la información sea interceptada por personal no autorizado o externo a la institución.

19.5 Las fotocopiadoras, escáner, cámaras digitales o cualquier forma de tecnología de reproducción de la institución deben ser utilizadas solo y exclusivamente por personas autorizadas.

19.6 Los usuarios no deben hacer uso de los servicios ofimáticos de la institución para actividades que no guarden ningún tipo de relación directa con sus funciones.



CAPÍTULO VI. CONTRATOS CON TERCEROS

Artículo 20°.- Objetivo
Establecer lineamientos que permitan mantener la seguridad de los activos de información de la SUNARP que son utilizados por terceros.

Artículo 21°.- Política de Contratos

21.1 Los contratos con terceros deben también especificar el área de trabajo, funciones y responsabilidades en términos de seguridad de información. Todo contrato deberá de tener cláusulas de Confidencialidad de acuerdo a la normatividad vigente.

21.2 La Unidad Orgánica de Administración debe verificar la firma de los acuerdo de Confidencialidad por parte del personal de la empresa proveedora de productos o servicios. En el caso de ser Outsourcing, se debe incorporar adicionalmente la cláusula de confidencialidad en el contrato.

21.3 El Jefe de cada área usuaria debe solicitar la asignación de accesos para las labores del empleado a través del formato establecido en la directiva para la Gestión de Acceso a Usuarios

21.4 Al término del contrato de servicio, el jefe de la Unidad Orgánica usuaria debe comunicar a la Unidad Orgánica de Administración y al área de Informática la Salida del personal de la empresa contratada para la prestación del servicio.

CAPÍTULO VII. ADMINISTRACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Artículo 22°.- Objetivo
Establecer las políticas que permitan proteger adecuadamente los activos de información de la SUNARP, de acuerdo con su clasificación.

Artículo 23°.- Política de Administración de equipos informáticos

23.1 El requerimiento de hardware o software de cada Unidad Orgánica debe solicitarse al área de Informática.

23.2 El empleado responsable de una unidad orgánica puede solicitar se asigne a su área algún recurso informático adicional, en caso sea necesario brindar apoyo informático de carácter eventual a las personas naturales contratadas temporalmente para la prestación de servicios vinculados a las funciones o fines de la Institución.

23.3 Toda entrega de un recurso informático (hardware) se realiza en coordinación con el área de Administración y Finanzas y debe constar en el Pedido-Comprobante de Salida. El mismo que debe ser suscrito por un representante del área de Informática, el usuario a quien se haya asignado el respectivo recurso informático y su jefe inmediato superior.

23.4 Las computadoras personales se entregarán completamente operativas, incluyendo el software y hardware solicitado y autorizados.

23.5 Sólo personal del área de Informática puede abrir y manipular los equipos de cómputo y la instalación de partes o piezas dentro de los equipos de cómputo.

23.6 No deberá moverse o reubicarse ningún equipo de cómputo, ya sea en forma parcial o en su totalidad, sin la previa coordinación y aprobación del responsable de la unidad orgánica, del personal del área de Informática y Seguridad Física. Asimismo, se debe realizar el registro respectivo.

23.7 Las computadoras asignadas al personal de la Institución, serán utilizadas sólo para la realización de actividades referidas a fines institucionales.

Artículo 24º.- Política de Retención de Registros

24.1 Todos los registros de la Institución, incluyendo expedientes y documentos electrónicos deben ser protegidos y mantenidos adecuadamente hasta que sean necesarios y de acuerdo a lo establecido por requerimientos operativos, legales o contractuales.

24.2 El Cronograma de Retención de Registros debe considerar como periodos o tiempos de retención, los plazos establecidos por las entidades reguladoras a nivel nacional que ejercen control y supervisión sobre la empresa.

24.3 Los registros no deben ser destruidos antes de culminado el periodo de retención establecido.

24.4 El área responsable de la retención de los registros físicos es el Archivo Central y de los registros electrónicos es el área de Informática, quienes en coordinación con los responsables de las áreas y la Gerencia Legal definirán los periodos de retención para cada tipo de registros.

24.5 Los plazos de retención de registros deben ser revisados y actualizados por lo menos cada dos años, para garantizar que se mantiene vigente el esquema de clasificación y los requerimientos legales.

24.6 Una vez culminado el periodo de retención, los registros pueden ser eliminados de acuerdo a lo señalado en la directiva "Establecimiento de niveles de confidencialidad y gestión de activos".

24.7 Cada área debe adoptar mecanismos de protección necesarios para proteger los registros físicos o expedientes que se encuentran bajo su custodia.

24.8 El área de Informática deberá adoptar los mecanismos de protección necesaria para proteger la integridad, disponibilidad, y de ser el caso la confidencialidad, de los registros electrónicos que se encuentran bajo su custodia.

Artículo 25º.- Política de Informática Móvil

25.1 La autorización, para la conexión a la red interna de la Institución, de los dispositivos de informática móviles será otorgado por el responsable del área de Informática. El uso de estos equipos está restringido a los propósitos de la institución.

25.2 El Personal de Soporte y Producción del área de Informática realizará una revisión del dispositivo de informática móvil y aplicará los controles convenientes para asegurar los equipos, antes de avalar su conexión a la red.

Artículo 26°.- Política de Pantalla y Escritorio Limpio

26.1 Los usuarios deben cumplir con las medidas de seguridad respecto al uso de las contraseñas y en el manejo de los activos de información. Esta totalmente prohibido compartir las claves.

26.2 Los documentos clasificados como Confidenciales o de uso interno deben estar protegidos contra perdida o robo.

26.3 Los usuarios deben guardar los documentos y medios de almacenamiento de información cuando no se estén utilizando y en especial cuando la oficina se encuentre vacía, para evitar su divulgación, alteración, pérdida o deterioro. El jefe de la unidad orgánica en coordinación con el área de administración y finanzas debe adoptar las medidas pertinentes a efectos de que sea viable el cumplimiento de la presente disposición.

26.4 La información de la Institución, de acuerdo a su clasificación, debe guardarse en lugares bajo llave y a prueba de siniestros, especialmente en horarios fuera de oficina o cuando ésta se encuentre desocupada. El jefe de la unidad orgánica en coordinación con el área de administración y finanzas debe adoptar las medidas pertinentes a efectos de que sea viable el cumplimiento de la presente disposición

26.5 Los usuarios deben bloquear la pantalla y/o teclado de su computadora y protegerla con contraseña u otro mecanismo de autenticación cuando tenga que salir de su oficina de manera temporal. Esta medida se efectuará sin perjuicio del bloqueo automático.

26.6 Los usuarios deben supervisar el uso de su computadora cuando se acepta que el personal del área de Informática o personal designado por ésta, acceda remotamente al equipo. Asimismo, debe supervisar el acceso a su computadora mientras se brinde el servicio de soporte en la zona de trabajo.

26.7 Los usuarios deben evitar la grabación de archivos importantes en el escritorio de la computadora para evitar su divulgación, alteración o pérdida en caso de que un tercero obtenga acceso no autorizado al equipo.

26.8 Cada usuario es responsable de apagar los equipos informáticos de oficina asignada al finalizar su uso, para evitar que otras personas puedan acceder a su información.

26.9 Personal del área de Informática debe configurar el bloqueo de los equipos después de quince (15) minutos de estar inactivo. Asimismo, se configurará para que después de dos (02) horas de inactividad se apague el equipo.

26.10 El área de Informática debe configurar el cambio de contraseña de todas las computadoras después de 45 días.

Artículo 27°.- Política de Intercambio de Voz, Fax y/o Video

27.1 Los usuarios no deben dejar mensajes grabados con información interna y/o confidencial en máquinas contestadoras o sistemas de correo de voz; de acuerdo con lo señalado en la directiva "Establecimiento de niveles de confidencialidad y gestión de activos".

27.2 Ante la presencia de terceros ni en lugares llámese públicos (ambientes de la institución accesibles a terceros, los usuarios no deben tratar información de manera presencial o telefónicamente temas sensibles que correspondan a información de uso interno y/o confidencial.

27.3 Los usuarios no deben discutir temas sensibles (información de uso interno y/o confidencial) en conferencias telefónicas o videoconferencia cuando todos los participantes no estén involucrados directamente en el tema.

27.4 Los usuarios no deben enviar información de uso interno y/o confidencial por fax u otro medio de transferencia electrónica a menos que cuente con la autorización del propietario de la información. Para el envío de este tipo de información se debe tener en cuenta la directiva "Establecimiento de Niveles de Confidencialidad y Gestión de Activos"

Artículo 28°.- Política de protección de la información registral

28.1 La información registral no debe ser proporcionada a terceros, a menos que dicha información sea solicitada mediante los procedimientos establecidos por la Institución.

28.2 La información registral que es confidencial y reservada, debe ser transmitida de acuerdo a lo señalado en la "Política de transmisión de información" y la "Política de Uso de Correo Electrónico".

28.3 Los propietarios de la información registral deben controlar que dicha información sea accedida únicamente por el personal de la institución designado para las labores de inscripción y publicidad registral y que cuente con los debidos privilegios.

CAPÍTULO VIII. SEGURIDAD DE LAS COMUNICACIONES

Artículo 29°.- Objetivo

Definir lineamientos y pautas que permitan controlar las conexiones a la redes de la SUNARP, encriptar y desencriptar la información de acuerdo a su clasificación y regular el uso de los servicios de telefonía fija, correo electrónico e internet.

Artículo 30°.- Política de Acceso a Directorios de Red

30.1 Considérese Directorio de red a aquella carpeta creada en un determinado servidor de SUNARP con el fin de almacenar (temporal o permanentemente) un determinado tipo de información para su posterior acceso por usuarios debidamente autorizados.

30.2 El acceso a estos directorios, se solicita a través del formato correspondiente brindado por personal del área de Informática, y se hace efectivo a través del usuario de red, al cual se le asignará permisos y derechos para hacer uso del directorio de acuerdo al perfil de acceso al Sistema que éste posea.

30.3 Un determinado directorio debe ser usado exclusivamente para albergar información de índole e interés laboral o que esté relacionado con un determinado tipo de actividad relacionada con la

SUNARP. Está prohibido copiar a la Red archivos de entretenimiento, como videos, música, juegos, y otros.

30.4 Bajo ninguna circunstancia debe manipularse el contenido de un determinado directorio con fines ajenos a los estrictamente laborales ni hacer uso indiscriminado de éste sin la debida autorización del propietario de la información.

30.5 La creación, asignación de permisos y derechos, creación de unidades de red y su ruteo a un determinado directorio es absoluta responsabilidad del área de Informática que a través del Administrador de Red cumplirá esta función.

30.6 Los directorios creados deben ser visibles sólo a los usuarios que se les está permitido su acceso, con los niveles de lectura y/o escritura asignados por su custodio. Bajo ninguna circunstancia deben ser mostrados abiertamente dentro del árbol de directorios del servidor que lo alberga sin una justificación de por medio.

Artículo 31°.- Política de Uso de Servicios de Red

31.1 Los usuarios no deben usar los servicios de red para ver, descargar, guardar, recibir o enviar material relacionado con:

- Contenido ofensivo de cualquier clase, incluyendo material pornográfico, profano, erótico.
- Promover la discriminación sobre la base de la raza, género, nacionalidad, edad, estado civil, orientación sexual, religión o discapacidad.
- Comportamiento violento o intimidante, apuestas, juegos o beneficio económico personal.
- Los archivos ejecutables de cualquier tipo a menos que se requieran para el cumplimiento de las actividades diarias y hayan sido autorizados por el área de Informática y el responsable de la Unidad Orgánica.

31.2 Los usuarios no deben vulnerar o intentar vulnerar la seguridad de las computadoras, servidores y equipos de comunicaciones de la institución.

31.3 Sólo los responsables de las diversas unidades orgánicas según sus funciones pueden solicitar acceso para el personal a su cargo, en atención a las funciones y actividades que desempeña, a los diversos servicios de red a través de los formatos respectivos proveídos por el área de informática.

31.4 Los usuarios deben reportar al personal responsable de seguridad de la información (Oficial de seguridad de la información), las alertas de riesgo o fallas sospechosas u otras anomalías. Asimismo, no deben difundir las vulnerabilidades identificadas.

31.5 Personal de Soporte y Producción del área de Informática debe habilitar y controlar los accesos a los servicios de red, monitorear la actividad de la red interna y desde/hacia Internet, realizar pruebas de intrusión y evaluación de vulnerabilidades y proponer al Gerente del área en mención los mecanismos necesarios para reforzar el cumplimiento de esta política.

Artículo 32°.- Política de Servicios Especiales

32.1 El acceso remoto (hacia la red interna) debe ser a través de un canal exclusivo y seguro debidamente autorizado. Considérese esto también para el acceso via Telnet, sea interno o externo.

32.2 Crear las reglas de acceso con el fin de no interrumpir el buen funcionamiento de la estructura interna y los servicios que ésta brinda.

32.3 La Gerencia de Informática debe configurar los accesos y perfiles para el servicio FTP requerido por cada unidad orgánica de acuerdo con los niveles de seguridad de la información.

Artículo 33°.- Política de Uso de Correo Electrónico

33.1 El correo electrónico es personal e intransferible, los usuarios son responsables de todas las actividades que se realicen por medio de la cuenta de correo electrónico que le sea asignada por la SUNARP. Asimismo, es de uso exclusivo para las actividades que estén relacionadas con el cumplimiento directo de su función dentro de la Institución.

33.2 El nombre de la cuenta de correo electrónico institucional para cada usuario estará formado por la letra inicial del nombre de pila del usuario seguido inmediatamente del apellido paterno, ligado con el símbolo "@" al nombre del dominio "institución.gob.pe". Para casos de similitudes de cuentas, el área de Informática coordinará con las personas involucradas el nombre de la cuenta, tratando de seguir la regla antes mencionada. Las excepciones a lo dispuesto en el presente numeral las autorizará el área en mención.

33.3 El usuario de correo electrónico deberá ingresar su contraseña al momento de acceder a su sistema de correo electrónico. Esta contraseña es confidencial, personal e intransferible, bajo responsabilidad del usuario. Cualquier usuario que deje su cuenta de correo electrónico abierta en un lugar público es responsable de todo aquello que se realice desde dicha cuenta.

33.4 Los usuarios no deberán utilizar el correo para fines que no sean institucionales, salvo que las necesidades y naturaleza del servicio justifique su uso, lo cual deberá ser autorizado por el Gerente del Área en coordinación con el área de Informática.

33.5 Los usuarios deben mantener activo permanentemente el correo electrónico y conectarse, como mínimo, una vez al día, para leer los mensajes, comunicados o cualquier tipo de notificación institucional, debiéndose presumir su lectura y conocimiento por el titular del correo a partir de las 24 horas del día hábil siguiente de la recepción del mensaje correspondiente. No se aplica al personal con suspensión del vínculo laboral y/o servicios.

33.6 El usuario del servicio de correo electrónico tiene la responsabilidad de eliminar permanentemente los mensajes de correo innecesarios (existentes en la bandeja de entrada, enviados y en la papelera).

33.7 Los usuarios al enviar un correo electrónico deberán utilizar siempre el campo "asunto" o "subject" a fin de resumir el tema del mensaje.

33.8 Los usuarios deberán utilizar las opciones de confirmación de entrega y lectura, cuando sea necesario

33.9 Con respecto a la autofirma en el correo (Ejemplo: Nombre, Cargo, Teléfono, Anexo), ésta debe ser breve e informativa, no debiendo ocupar más de 3 líneas. No incluir la dirección de correo en la firma.

33.10 Todo correo electrónico externo no solicitado y/o recibido de fuentes desconocidas deberá inmediatamente eliminarse en forma definitiva del recipiente de correos recibidos por medidas de seguridad.

33.11 El sistema de correo verificará, previo al envío o recepción del cualquier mensaje, la existencia o no de algún virus informático, código malicioso o información prohibida. En caso de detectar alguna anomalía

al respecto, el sistema de correo automáticamente registrará el evento ocurrido, para su control y manejo por el administrador del sistema.

33.12 El envío de información de uso interno y confidencial a través del correo electrónico deberá realizarse teniendo en cuenta la Política de seguridad la información.

33.13 Todo usuario del sistema de correo electrónico en coordinación con el área de informática, deberá configurar un mensaje automático de respuesta por vacaciones en su cuenta de correo, un dia antes del inicio de sus vacaciones.

33.14 El administrador del sistema de correo electrónico deberá mantener la privacidad, confidencial y seguridad de la información almacenada en el servidor de correo electrónico y sólo podrá acceder o hacer de conocimiento de la unidad orgánica que la solicite (Ejemplo: Oficina de Auditoria, Sanciones, Ética y Transparencia, etc) previa solicitud por escrito de la instancia inmediata superior en coordinación con el área de Informática.

Artículo 34°.- Política de Controles Criptográficos

34.1 El área de Informática a través de sus áreas relacionadas debe implementar sistemas de cifrado con el fin de evitar la interceptación de la información electrónica.

34.2 El uso de algoritmos de cifrado propietarios no esta permitido para ningún propósito, a menos que sea revisado por el respectivo personal técnico de las áreas relacionadas al área de Informática.

34.3 La información de uso interno y confidencial debe ser cifrada antes de ser transmitida en especial cuando se utilizan equipos de informática móvil fuera de las instalaciones de la SUNARP (por ejemplo: computadoras portátiles, PDA's, etc). Asimismo, sólo el personal del área de Informática implementará las facilidades técnicas necesarias.

Artículo 35°.- Política de Transmisión de Información

35.1 La transmisión de la información se realizará de acuerdo con la directiva "Establecimiento de Niveles de Confidencialidad y Gestión de Activos" y con la politica "Intercambio de información por Voz, fax y/o Video".

35.2 Los usuarios podrán transmitir información de uso interno y confidencial considerando los aspectos los aspectos señalados en la directiva "Establecimiento de Niveles de Confidencialidad y Gestión de Activos" y en la Política para el intercambio de información por voz, fax y/o video.

35.3 Los usuarios debidamente autorizados por las instancias correspondientes de la SUNARP, para transmitir información confidencial a través del correo electrónico, deben enviar dicha información adjunta en un formato de archivo de tipo seguro (se recomienda utilizar el formato de archivo del tipo PDF), así mismo el área de Informática a través de sus instancias implementará las facilidades técnicas necesarias para proteger la información (cifrado de datos) enviada por el servicio de correo electrónico.

Artículo 36°.- Política de Acceso a Páginas Web Especiales

36.1 El acceso a Páginas Web Especiales constituye un mecanismo en el cual se brinda acceso temporal o permanente a un determinado sitio de Internet, con el propósito de facilitar la labor de un usuario, la cual debe estar debidamente sustentada y autorizada por el jefe inmediato superior.

36.2 La verificación del requerimiento de acceso y su posterior aprobación es responsabilidad del Responsable de Seguridad de la Información (Oficial de Seguridad de la información) en coordinación con el área de Informática y Unidad Orgánica solicitante.

36.3 Todo sitio web será administrado por el filtro de contenidos de acceso web, que a su vez los clasificará por tipo de contenido y por tipo de usuario. Dependiendo del tipo de usuario que intente acceder a un determinado sitio web se tendrá distintos tipos de acceso y opciones de navegación.

36.4 El área de informática debe crear los perfiles para el acceso a internet de acuerdo a los requerimientos de seguridad y de las unidades orgánicas.

Artículo 37°.- Política de Acceso a entornos Web

37.1 Considérese como Entornos Web a aquellos entornos administrados por la SUNARP los cuales ofrecen servicios web como la Intranet, el Portal Institucional y el acceso a Internet.

37.2 El acceso a la Intranet, al Portal Institucional y a Internet debe ser sólo para fines relacionados con la actividad laboral propia y con la plena conciencia del uso que se le da.

37.3 Los usuarios no deberán utilizar estos servicios con fines ilícitos, lesivos de derechos y libertades de terceros, o que puedan perjudicar, dañar o impedir por cualquier forma, el acceso a los mismos, en perjuicio de la SUNARP o de terceros.

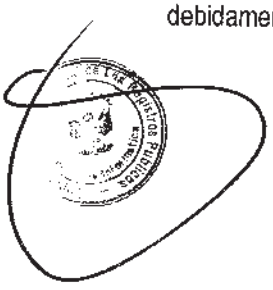
37.4 En ningún caso el usuario podrá utilizar los servicios de entornos web para promocionar, vender, contratar, divulgar publicidad o información propia o de terceras personas sin autorización previa de una instancia superior.

37.5 Los usuarios no deberán realizar acciones que impidan o dificulten el acceso a entornos web a través de virus informáticos, código, software, programa informático o de telecomunicaciones que puedan provocar daños o alteraciones no autorizadas a los contenidos, programas o sistemas accesibles a través éstos servicios.

37.6 Los usuarios no deben descargar o abrir archivos provenientes de Internet u otras redes externas sin tener activo y actualizado el software antivirus.

37.7 Se encuentra prohibida la descarga de archivos de música, video, juegos y otros de tipo entretenimiento debido a que el canal de comunicación de Internet es sólo para fines laborales, salvo excepciones debidamente justificadas y autorizadas por la Unidad Orgánica y ejecutada por el área de Informática.

37.8 Debido a la saturación que ocasiona el ejecutar los programas de Radio por Internet, tanto musicales como Noticiosas, el uso de estas funcionalidades se encuentra restringido, salvo excepciones debidamente justificadas y autorizadas por el área de Informática.



37.9 La publicación de información en el portal institucional y en la intranet se realiza de acuerdo con lo señalado en los documentos aprobados por la Institución. Asimismo, la Gerencia de Imagen Institucional y Relaciones Públicas será responsable de la actualización de los sistemas publicados en el portal web de la institución.

CAPÍTULO IX. DESARROLLO, ADQUISICIÓN Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Artículo 38°.- Objetivo
Definir lineamientos y pautas para el desarrollo, adquisición y mantenimiento de sistemas de información, que permitan proteger la información de agentes no autorizados.

Artículo 39°.- Política de Planificación y Aceptación de Sistemas

39.1 Los requerimientos de nuevos sistemas así como sus actualizaciones debe ser invocada por las áreas usuarias, a través de un procedimiento formal.

39.2 El área de Informática debe definir y comunicar el plazo de la implementación a los plazos de entrega del requerimiento solicitado por el área usuaria.

39.3 El área de informática, a través del personal asignado para el análisis, diseño y desarrollo de sistemas, debe hacer uso de los estándares y buenas prácticas que garantice la disponibilidad, accesibilidad e integridad de la información.

39.4 La aceptación del software se hará efectiva por el Área Usuaria, previo análisis y pruebas efectuadas por el personal del área de Informática.

39.5 Únicamente se utilizará software certificado o en su defecto software previamente revisado y aprobado, por el área de Informática.

39.6 La aceptación y uso de los sistemas no exonera, de responsabilidad alguna sobre el gestor de seguridad, para efectuar pruebas o diagnósticos a la seguridad de los mismos.

39.7 El software diseñado y desarrollado internamente deberá ser analizado y aprobado, por el personal de seguridad de la información de la institución.

39.8 Es tarea de desarrolladores el realizar pruebas de validación de entradas, en cuanto a:

- Valores fuera de rango.
- Caracteres inválidos, en los campos de datos.
- Datos incompletos.
- Datos con longitud excedente o valor fuera de rango.
- Datos no autorizados o inconsistentes.
- Procedimientos operativos de validación de errores
- Procedimientos operativos para validación de caracteres.
- Procedimientos operativos para validación de la integridad de los datos.
- Procedimientos operativos para validación e integridad de las salidas.

39.9 Toda prueba de las aplicaciones o sistemas en un entorno de producción, se deberá hacer teniendo en cuenta las medidas de protección de los archivos reales.

39.10 Cualquier prueba sobre los sistemas, del ámbito a la que esta se refiera deberá ser documentada y cualquier documento o archivo que haya sido necesario para su ejecución deberá ser borrado de los registros y dispositivos físicos, mediante tratamiento electrónico.

Artículo 40°.- Política de Protección contra software malicioso

40.1 Se deberá adquirir y utilizar software únicamente de fuentes confiables y aprobadas por el área de Informática.

40.2 Los servidores, al igual que las estaciones de trabajo, tendrán instalado y configurado correctamente software antivirus actualizable y activada la protección en tiempo real.

Artículo 41°.- Política de Mantenimiento de Sistemas

41.1 El mantenimiento de las aplicaciones y software de sistemas es de exclusiva responsabilidad del área de informática.

41.2 El personal del área de Informática llevará un registro global del mantenimiento efectuado sobre los sistemas y cambios realizados desde su instalación.

CAPÍTULO X. CONTINUIDAD DE LAS OPERACIONES

Artículo 42°.- Objetivo
Establecer los niveles aceptables de operatividad y disponibilidad de los servicios que brinda la Institución a los usuarios finales/clientes.

Artículo 43°.- Política de Definir, Revisar y Actualizar el Plan de Continuidad de Negocios.

43.1 Implementar y mantener un proceso de gestión para el desarrollo y el mantenimiento de la continuidad del Negocio de la SUNARP que trate los requerimientos en la seguridad de información necesarios para la continuidad del negocio.

43.2 Todo personal que labore en la SUNARP bajo cualquier modalidad de contrato debe cumplir con los roles y responsabilidades asignadas en el proceso de Continuidad de Negocio.

43.3 Revisar y de ser necesario actualizar el Plan de Continuidad de Negocios.

43.4 Ejecutar periódicamente el Plan de Pruebas.

CAPÍTULO XI. MANEJO DE INCIDENCIAS Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN

Artículo 44°.- Objetivo
Establecer pautas que permitan administrar adecuadamente las incidencias y debilidades de seguridad de información presentadas en los sistemas de información, minimizando sus ocurrencias e impacto sobre los proceso del negocio de la SUNARP.

Artículo 45°.- Política de Respuesta ante Incidencias y debilidades

45.1 El área de informática a través de Soporte Técnico brindará servicio a los usuarios ante el desconocimiento y/o problemas con el uso de las herramientas informáticas como: File Server, Correo, Cambio de contraseñas, entre otros.

45.2 Todo trabajador que labore, preste o reciba servicios en la SUNARP (personal que labora en la SUNARP, proveedores y su personal e Instituciones con las que la SUNARP firma Convenios de Colaboración Interinstitucional y su personal) deberá comunicar al Responsable de la Seguridad de la Información (Oficial de Seguridad de la Información), cualquier incidente o debilidad de la seguridad de la información.

45.3 El responsable del analizar, evaluar, escalar y comunicar los resultados es el Responsable de la Seguridad de la Información (Oficial de Seguridad de la Información), de acuerdo a los lineamientos establecidos en la Directiva de Gestión de Incidentes de Seguridad.

45.4 En caso el personal de la SUNARP, de los proveedores o de las Instituciones con las que la SUNARP firma Convenios de Colaboración Interinstitucional resultarán responsables en las investigaciones, serán sancionados de acuerdo con lo señalado en el Reglamento Interno de Trabajo, contratos y convenios firmados.