RESOLUCION N° 21-2013

DRA. ANDREA BRASALES JIMENEZ

REGISTRADORA DE LA PROPIEDAD DEL CANTON CUENCA

CONSIDERANDO

Que, el Art. 1 de la Ley del Sistema Nacional de Registro de Datos Públicos manifiesta que "La presente ley crea y regula el sistema de registro de datos públicos y su acceso, en entidades públicas o privadas que administren dichas bases o registros. El objeto de la ley es: garantizar la seguridad jurídica, organizar, regular, sistematizar e interconectar la información, así como: la eficacia y eficiencia de su manejo, su publicidad, transparencia, acceso e implementación de nuevas tecnologías".

Que, el Art. 4 de la ley Ibidem manifiesta que "Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo".

Que, el Art. 15 de la Ley del Sistema Nacional de Registro de Datos Públicos manifiesta que "Los registros, llevarán la información de modo digitalizado, con soporte físico, en la forma determinada por la presente ley y en la normativa pertinente para cada registro, en lo que respecta a: 2.Registro de la Propiedad: Llevará su registro bajo el sistema de información cronológica, personal y real;".

Que, el Art. 10 de la Ley Orgánica de transparencia y Acceso a la información Publica establece que "Es responsabilidad de las instituciones públicas, personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley, crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción...".

Que, el Art. 23 de la Ley del Sistema Nacional de Registro de Datos Públicos manifiesta que "El sistema informático tiene como objetivo la tecnificación y modernización de los registros, empleando tecnologías de información, bases de datos y lenguajes informáticos estandarizados, protocolos de intercambio de datos seguros, que permitan un manejo de la información adecuado que reciba, capture, archive,

codifique, proteja, intercambie, reproduzca, verifique, certifique o procese de manera tecnológica la información de los datos registrados...".

En uso de las atribuciones conferidas por la Ley

RESUELVE

1.- Aprobar el Manual de Políticas de Seguridad de la Información del Registro de la Propiedad del Cantón Cuenca.

2.- Solicitar a la Dirección de Desarrollo Institucional y Talento Humano se proceda a sociabilizar el presente documento.

La presente Resolución entrara en vigencia a partir de su suscripción.

Cuenca, 09 de julio de 2013.

REGISTRO DE LA PROPIEDAD

DRA. ANDREA BRASALES JIMENEZ

REGISTRADORA DE LA PROPIEDAD DEL CANTON CUENCA

Registro de la Propiedad

REGISTRO DE LA PROPIEDAD DEL CANTÓN CUENCA

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Fecha	Versión	Descripción	Autor
2013-05-20	1.0	Elaboración del BORRADOR	Claudio Crespo Merchán

Contenido

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Introducción

En la actualidad, las instituciones para realizar sus actividades, cada vez son más dependientes de los sistemas automáticos y de las tecnologías de la información. Se ha vuelto crítico la disponibilidad de estos elementos, ya que resultaría complicado funcionar sin el soporte informático. Los procedimientos manuales de contingencia, sólo serían prácticos por un período corto.

De darse un siniestro, la paralización prolongada de los servicios de TIC's puede llevar a las instituciones a situaciones de pérdidas de imagen y financieras significativas, lo que conllevaría a una merma parcial o total de los servicios que presta. Por lo tanto, la capacidad que tengan los centros informáticos para recuperarse de los efectos de un desastre dentro de un periodo predeterminado debe ser un elemento crucial en un plan de seguridad para una organización.

El Registro de la Propiedad del Cantón Cuenca, es una Institución Adscrita al Gobierno Autónomo Descentralizado Municipal del Cantón Cuenca, con características de independencia Registral y Administrativa, ha sido creada en el año 2011 y es que en el último cuarto de año inicia sus actividades, soportado en una infraestructura informática débil y sin planes certeros de estrategias.

Para el año 2012, se plantea dentro del Plan Operativo Anual, un proyecto de fortalecimiento de la infraestructura informática, apuntando a la seguridad del centro de cómputo y a la seguridad lógica de las instalaciones. De este plan, dentro del área de TIC's, la institución cuenta con algunos controles de seguridad y de recuperación de ciertos recursos de TIC's, pero sin haber realizado un previo análisis de riesgos y sin contar con un proceso formal de prevención y recuperación de desastres (Plan de Contingencia). Por este motivo se ha visto la necesidad de diseñar un Plan de Contingencia de TIC´s como parte del Programa de Modernización de la Institución.

La administración de los recursos de la institución busca asegurar y salvaguardar el entorno tecnológico, para lo cual es de suma importancia emplear un conjunto de mecanismos reguladores de las funciones y actividades desarrolladas por cada uno de los miembros de la institución.

El Registro de la Propiedad del Cantón Cuenca, se encuentra estructurada de la siguiente manera:

1.1 FUNCION DIRECTIVA

Se encuentra integrada por el Registrador de la Propiedad. No tiene órgano regulador superior establecido en la Ordenanza.

Coordina su actuación con La Dirección Nacional de Registro de Datos Públicos, perteneciente a la Función Ejecutiva dentro del Ministerio de Telecomunicaciones y Sociedad de la Información, en cuanto a la normativa Registral; y , al Gobierno Autónomo Descentralizado Municipal del Cantón Cuenca, en cuanto a lo administrativo.

1.2 FUNCION EJECUTIVA

Representada por el Registrador de la Propiedad, quien es nombrado por el Alcalde del Gobierno Autónomo Descentralizado del Cantón Cuenca, fruto de un concurso de oposición y méritos regulados por la Ley de datos públicos.

1.3 FUNCION ADMINISTRATIVA

Integrada por las siguientes dependencias: Dirección Administrativa - Financiera, y, Dirección de Desarrollo Institucional y Talento Humano.

1.4 FUNCION OPERATIVA

Integrada por la Dirección de Operaciones Registrales,

2 Definiciones

2.1 Seguridad Organizacional

Dentro de esta definición, se establece el marco formal de seguridad que debe sustentar la Institución, incluyendo servicios o contrataciones externas a la infraestructura de seguridad, integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias para contestación a circunstancias especiales a la seguridad.

2.2 Seguridad Lógica

Establece e integra los mecanismos y guías técnicas-administrativas, que permitan monitorear y conocer el acceso a los activos de información, que incluye los procedimientos para la administración de los usuarios, definición de las responsabilidades de los diferentes actores en el sistema, definición de los perfiles de seguridad de los usuarios, control de acceso a las aplicaciones y documentación, que van desde el control de cambios en la configuración de los equipos y sistemas, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.

2.3 Seguridad Física

Determina los requerimientos mínimos que se deben satisfacer en cuanto a seguridad perimetral, de forma que se puedan determinar controles en el

manejo del hardware, cambios en la información y control de los ingreso a las distintas áreas con base en la importancia de los activos.

2.4 Seguridad Legal

Integra los requerimientos de seguridad que deben cumplir todos los empleados, proveedores y usuarios de la red institucional bajo la reglamentación de la normativa interna de políticas y manuales de procedimientos de la Institución.

Por la existencia de un número significativo de amenazas y riesgos, que la infraestructura de red y recursos informáticos de una organización deben estar protegidos bajo un esquema de seguridad que reduzca los niveles de vulnerabilidad y permita una eficiente administración del riesgo. Para ello, resulta importante establecer políticas de seguridad, las cuales van desde la evaluación, el diseño de procedimientos de operación y control para establecer los niveles de protección de los recursos.

2.5 Administración de la Seguridad

La administración de la seguridad informática se basa en un sistema de gestión que comprende la estructura de la organización, las políticas institucionales, los procedimientos de seguridad y control, los procesos y los recursos necesarios para implementar la Administración de la Seguridad de la Información (SGSI).

Un sistema de gestión de la seguridad se implanta de acuerdo a estándares internacionales de seguridad como la ISO 27001 basada en el código de buenas prácticas y objetivos de control de la ISO 27002, el cual se centra en la preservación de las características de confidencialidad, integridad y disponibilidad.

3 Definición de Normas y Políticas de Seguridad

3.1 Normas de Seguridad

Las normas de seguridad son un conjunto de reglas, recomendaciones y controles con el propósito de dar respaldo a las políticas de seguridad y a los objetivos desarrollados por éstas, a través de funciones, delegación de responsabilidades y otras técnicas, con un objetivo claro y acorde a las necesidades de seguridad establecidas para el entorno administrativo y tecnológico de la institución.

Las normas y políticas de seguridad están basadas en estándares internacionales que garantizan las mejores prácticas. Las principales son las siguientes:

ISO 27000, vocabulario y definiciones (terminología para el resto de estándares de la serie).

ISO 27001, especificación del sistema de gestión de la seguridad de la información (SGSI). Esta norma será certificable bajo los esquemas nacionales de cada país.

ISO 27002, que describe el Código de buenas prácticas para la gestión de la seguridad de la información.

ISO 27003, que contendrá una guía de implementación.

ISO 27004, estándar relacionado con las métricas y medidas en materia de seguridad para evaluar la efectividad del sistema de gestión de la seguridad de la información.

ISO 27005, que proporcionará el estándar base para la gestión del riesgo de la seguridad en sistemas de información.

3.2 Políticas de Seguridad

Constituyen un marco formal de actuación, en relación con los recursos y servicios informáticos de la organización. Estas a su vez establecen las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños, sin importar el origen de estos.

3.2.1 Elementos de una Política de Seguridad Informática

Una PSI debe orientar las decisiones que se toman en relación con la seguridad. Por tanto, requiere de una disposición por parte de cada uno de los miembros de la institución para lograr una visión conjunta de lo que se considera importante.

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

Las Políticas de Seguridad de la Información implantan los medios de organización en relación con la seguridad. Deben establecer un lenguaje común sin tecnicismos y términos legales que compliquen una comprensión clara de las mismas, sin sacrificar su precisión y formalidad.

Por otra parte, la política debe asignar la autoridad responsable para que las cosas ocurran, el marco de competencia para implantación de los correctivos y sus actuaciones, con la autoridad que permita ejecutar y sancionar de ser el caso.

3.3 Las Políticas de Seguridad Informática como base de la Administración de la Seguridad Integral

El agregado de lineamientos que una organización debe seguir para asegurar la confiabilidad de sus sistemas son "Las políticas de seguridad informática". Por tanto, es importante instituir un proceso continuo y retroalimentado que observe el empoderamiento, los métodos, el monitoreo de cumplimiento y la renovación, aceptación de las reglas, que logren aceptación total.

Las políticas por sí mismas no garantizan la seguridad de la Institución. Ellas deben responder a intereses y necesidades organizacionales.

3.3.1 La seguridad tiene varios estratos:

- Marco jurídico adecuado.
- Medidas técnicas y administrativas, políticas y procedimientos, auditoría de seguridad.

3.3.2 Control de la Seguridad

Cada vez más, los administradores observan el impacto significativo que la información puede tener en el éxito de una institución. La dirección espera un alto entendimiento de la técnica aplicada en TIC´s y de la posibilidad de que sea aprovechada con éxito, para que:

- Garantice el logro de sus objetivos
- Tenga suficiente flexibilidad para aprender y adaptarse
- Administre los riesgos que enfrenta
- Reconozca de forma apropiada las oportunidades.

Para garantizar los puntos antes indicados, es necesaria la implementación de procesos de control dentro del gobierno de tecnologías de información y comunicación por lo tanto: control se define como "las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos".

Por lo tanto, el sistema empresarial de controles internos impacta en la tecnología de información y comunicación en tres niveles:

- Al nivel de Dirección, se reglan los objetivos de negocio, se instauran políticas y se toman decisiones para administrar los recursos empresariales.
- Al nivel de procesos de negocio, se aplican controles para actividades específicas. La mayoría de los procesos de negocio están automatizados, sin embargo, algunos controles permanecen como procedimientos manuales.
- Para soportar los procesos, TIC´s proporciona servicios, por lo general de forma compartida, por varios procesos operacionales, y mucha de la infraestructura de TIC´s provee un servicio común. La operación formal de estos controles es necesaria para que dé confiabilidad.

3.4 Análisis de riesgos

El análisis de riesgos permite determinar qué tiene la Institución y estimar lo que podría pasar si ocurrieran fenómenos naturales o humanos contrarios a un comportamiento normal cotidiano.

3.4.1 Elementos:

- Activos, los elementos del sistema de información que aportan valor a la Organización
- Amenazas, sucesos que les pueden afectar a los activos causando un perjuicio a la Organización
- Salvaguardas, elementos de defensa desplegados para que aquellas amenazas no causen o mermen daños.
- El impacto: lo que podría pasar
- El riesgo: lo que probablemente pase

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento.

3.5 Gestión de riesgos

Administración que permite constituir la defensa prudente, para enfrentar las emergencias, subsistir a los incidentes y continuar operando en las mejores condiciones; logrando reducir el riesgo a un nivel residual que la organización asume.

3.6 Análisis de riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo y sirve para:

- Determinar los activos relevantes para la Organización, su interrelación y su valor.
- Determinar a qué amenazas están expuestos aquellos activos
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo

- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de una amenaza.

4 POLITICAS DE SEGURIDAD

4.1 Seguridad Organizacional

4.1.1 Política de Seguridad

Establece un marco de referencia para el manejo de los servicios informáticos así como la normativa para la designación de un equipo de seguridad al interior de la misma.

Artículo 1. Los servicios informáticos del Registro de la Propiedad son de exclusivo uso institucional y para gestiones administrativas, cualquier cambio en la normativa de uso de los mismos, será expresa y adecuada como política de seguridad en este documento. El incumplimiento de la presente política será objeto de sanciones administrativas sin perjuicio de las acciones civiles o penales que pueda llevar a cabo la institución contra el infractor.

Artículo 2. La Administración nombrará un Comité de seguridad, que dé seguimiento al cumplimiento de la normativa y propicie el entorno necesario para crear un sistema de gestión de la seguridad de la información, el cual tendrá entre sus funciones:

a) Velar por la seguridad de los activos informáticos
b) Aplicación de sanciones.
c) Elaboración de planes de seguridad.
d) Capacitación de usuarios en temas de seguridad.
e) Gestionar y coordinar esfuerzos, por crear un plan de contingencia, que dé sustento o solución, a problemas de seguridad dentro de la institución.
f) Informar sobre problemas de seguridad al Registrador.
g) Poner especial atención a los usuarios de la red institucional sobre sugerencias o quejas con respecto al funcionamiento de los activos de información.

El comité de seguridad estará integrado por los siguientes miembros:

a) Registrador de la Propiedad
b) Director Administrativo Financiero
c) Delegado de Seguridad, entre los Funcionarios de Informática, nombrado por el Registrador.

Artículo 3. El personal de cada unidad organizativa es el único responsable de las actividades procedentes de sus acciones.

Artículo 4. El Administrador de la Infraestructura de Sistemas es el encargado de mantener en buen estado los activos comunes.

Artículo 5. Todo usuario, gozará de total reserva sobre su información, o la información que provenga de sus acciones, salvo en casos, en que esté involucrado en actos ilícitos o contraproducentes para la seguridad institucional, sus servicios.

Artículo 6. Los usuarios tendrán acceso a Internet, cuando cumplan los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones de uso de la red.

Artículo 7. Las actividades administrativas tienen prioridad, sobre otro uso autorizado en la red.

4.1.2 Política de Excepciones de Responsabilidad

Norma excepciones al cumplimiento de una determinada política institucional.

Artículo 8. Los usuarios que por disposición de sus superiores realicen acciones que perjudiquen a otros usuarios o la información que estos procesan, deberán mantener dicha disposición por escrito.

Artículo 9. Algunos usuarios pueden estar exentos de responsabilidad, o de seguir algunas de las políticas enumeradas en este documento, debido a la responsabilidad de su cargo, o a situaciones no programadas. Estas excepciones deberán ser solicitadas formalmente y aprobadas por el comité de seguridad, con la documentación necesaria para el caso, siendo el Registrador de la Propiedad, quien dé por sentada su aprobación final.

4.1.3 Política de Responsabilidad por los Activos

Norma la responsabilidad que tienen los diferentes departamentos de la Institución en el control y cuidado de los activos institucionales.

Artículo 10. Cada departamento, tendrá un responsable por el/los activo/s crítico/s o de mayor importancia para la el departamento, cuando estos no hayan estado asignados a un funcionario en particular.

Artículo 11. La persona responsable de los bienes, velará por la salvaguarda de los activos físicos.

Artículo 12. El administrador de Sistemas será el responsable de la seguridad de la información almacenada en esos recursos.

4.1.4 Política de Clasificación de la Información

Norma la identificación los diferentes tipos de información con los que cuenta la Institución.

Artículo 13. De forma individual, los departamentos de la Institución, son responsables, de clasificar de acuerdo al nivel de importancia, la información que en ella se procese.

Artículo 14. Se tomarán como base, los siguientes criterios, como niveles de importancia, para clasificar la información:

a) Pública

b) Interna

c) Confidencial

Artículo 15. Los activos de información de mayor importancia para la institución deberán clasificarse por su nivel de exposición o vulnerabilidad.

4.1.5 Política de Seguridad Ligada al Personal

Norma el uso de la información por parte del personal que labora en la Institución.

Artículo 16. Se entregará al funcionario, toda la documentación necesaria para ejercer sus labores dentro de la institución, en el momento en que se dé por establecido su documento contractual laboral.

Artículo 17. El nombramiento o el contrato de trabajo deberán complementar un acuerdo de no divulgación y confidencialidad, donde el empleado se compromete a mantener en secreto información sensible de la organización.

Artículo 18. Una vez terminado el trabajo y antes de dar por terminada la relación laboral, el funcionario deberá restituir toda la información entregada por parte de la Institución.

Artículo 19. La información procesada, manipulada o almacenada por el empleado es propiedad exclusiva de la Institución.

Artículo 20. La Institución no se hace responsable por daños causados provenientes de sus funcionarios a la información o activos de procesamiento, propiedad de terceros y/o daños efectuados desde sus instalaciones a equipos informáticos externos.

4.1.6 Política de Capacitación de Usuarios

Norma sobre la importancia de la seguridad.

Artículo 21. Los usuarios de los servicios informáticos institucionales, serán capacitados en cuestiones de seguridad de la información, según sea el área operativa y en función de las actividades que se desarrollan.

Artículo 22. Se deben tomar todas las medidas de seguridad necesarias, antes de realizar una capacitación a personal ajeno o propio de la institución, siempre y cuando se vea implicada la utilización de los servicios o se exponga material de importancia considerable para la institución.

4.1.7 Política de Respuesta a Incidentes o Anomalías de Seguridad

Norma el respaldo de la información institucional.

Artículo 23. Se realizarán respaldos de la información, diariamente, para los activos de mayor importancia o críticos, un respaldo semanal que se utilizará en caso de fallas y un tercer respaldo efectuado mensualmente, el cual deberá ser guardado y evitar su utilización a menos que sea estrictamente necesaria.

Artículo 24. El Comité de Seguridad en conjunto con la Administración de Informática, diseñarán e implantarán un plan de continuidad del servicio, acorde con las técnicas estándares, para lo cual se basará en la disponibilidad presupuestaria y la afectación que pueda soportar ante una interrupción del servicio.

Artículo 25. El encargado de Infraestructura de Sistemas deberá elaborar un documento donde deba explicar los pasos que se deberán seguir en situaciones contraproducentes a la seguridad y explicarlo detalladamente en una reunión ante el personal de respuesta a incidentes.

Artículo 26. El Comité de Seguridad en acción conjunta con la Administración de Informática, diseñarán e implementarán un plan de contingencia y recuperación de desastres de acuerdo a técnicas estándares que garantice la continuidad del servicio.

4.2 Seguridad Lógica

4.2.1 Política de Control de Accesos

Norma la utilización de la información perteneciente a la Institución.

Artículo 27. El Administrador de Sistemas proporcionará toda la documentación necesaria para agilizar la utilización de los sistemas, referente a formularios, guías, controles, otros.

Artículo 28. Cualquier petición de información, servicio o acción proveniente de un determinado usuario o departamento, se deberá efectuar siguiendo los canales de gestión formalmente establecidos por la institución, para realizar dicha acción; no dar seguimiento a esta política implica:

a) Negar por completo la ejecución de la acción o servicio.

b) Un informe completo dirigido al comité de seguridad, el mismo que será realizado por el Administrador de Sistemas con copia al departamento al cual solicita el servicio.
c) Sanciones aplicables por el Registrador, previamente discutidas con el comité de seguridad.

4.2.2 Política de Administración del Acceso de Usuarios

Norma el acceso de los usuarios a la red institucional.

Artículo 29. El sistema de control de contraseñas será administrado centralmente por un delegado de la unidad y será parte de las políticas de administración de red.

Artículo 30. Son usuarios de los servicios informáticos institucionales los servidores públicos operativos, administrativos, y toda aquella persona, que tenga contacto directo como empleado y utilice los servicios de la red institucional.

Artículo 31. Se asignará una cuenta de acceso a los sistemas de la intranet, a todo, siempre y cuando se identifique previamente el objetivo de su uso o permisos explícitos a los que este accederá, junto a la información personal del usuario.

Artículo 32. Los servidores públicos de la Institución, son usuarios limitados, estos tendrán acceso únicamente a los servicios de Internet y recursos compartidos, cualquier cambio sobre los servicios a los que estos tengan acceso, será motivo de revisión y modificación de esta política, adecuándose a las nuevas especificaciones.

Artículo 33. Se consideran usuarios externos o terceros, cualquier entidad o persona natural, que tenga una relación con la institución fuera del ámbito de empleado y siempre que tenga una vinculación con los servicios de la red institucional.

Artículo 34. El acceso a la red por parte de terceros es estrictamente restrictivo y permisible únicamente mediante firma impresa y documentación de aceptación de confidencialidad hacia la institución y comprometido con el uso exclusivo del servicio para el que le fue provisto el acceso.

Artículo 35. No se proporcionará el servicio solicitado por un usuario o departamento, sin antes haberse completado todos los procedimientos de autorización necesarios para su ejecución.

Artículo 36. Se creará una cuenta temporal del usuario, en caso de olvido o extravío de información de la cuenta personal, para brindarse al usuario que lo necesite, siempre y cuando se muestre un documento de autorización.

Artículo 37. La longitud mínima de caracteres permisibles en una contraseña se establece en 8 caracteres, los cuales tendrán una combinación alfanumérica, incluida en estos caracteres especiales.

Artículo 38. La longitud máxima de caracteres permisibles en una contraseña se establece en 12 caracteres, siendo esta una combinación de Mayúsculas y minúsculas.

4.2.3 Política de Responsabilidades del Usuario

Norma las responsabilidades de los usuarios sobre el uso de los activos informáticos de la Institución

Artículo 39. El usuario es responsable exclusivo de mantener a salvo su contraseña.

Artículo 40. El usuario será responsable del uso que haga de su cuenta de acceso a los sistemas o servicios.

Artículo 41. Se debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas, a menos que ésta se guardada en un lugar seguro.

Artículo 42. El usuario es responsable de eliminar cualquier rastro de documentos proporcionados por el Administrador de Sistemas, que contenga información que pueda facilitar a un tercero la obtención de la información de su cuenta de usuario.

Artículo 43. El usuario es responsable de evitar la práctica de establecer contraseñas relacionadas con alguna característica de su persona o relacionado con su vida o la de sus parientes.

Artículo 44. El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en él, mediante una herramienta de bloqueo protegida por una contraseña, el cual deberá activarse en el preciso momento en que el usuario deba ausentarse.

Artículo 45. Cualquier usuario que encuentre un hueco o falla de seguridad en los sistemas informáticos de la institución, está obligado a reportarlo al Administrador de Sistemas.

Artículo 46. Los usuarios son responsables de guardar sus trabajos en elementos de respaldo, siempre y cuando hayan sido autorizados por el administrador de Informática, y así evitar cualquier pérdida de información valiosa.

4.2.4 Política de Uso de Correo Electrónico

Norma el uso del servicio de correo electrónico.

Artículo 47. El servicio de correo electrónico, es un servicio gratuito, y no se puede garantizar su confiabilidad, se debe hacer uso de él, acatando todas las disposiciones de seguridad diseñadas para su utilización y evitar el uso o introducción de software malicioso a la red institucional.

Artículo 48. El correo electrónico es de uso exclusivo, para los empleados de la Institución.

Artículo 49. Todo uso indebido del servicio de correo electrónico, será motivo de suspensión temporal de su cuenta de correo o según sea necesario la eliminación total de la cuenta dentro del sistema.

Artículo 50. El usuario será responsable de la información que sea enviada con su cuenta.

Artículo 51. El Comité de Seguridad, se reservará el derecho de monitorear las cuentas de usuarios, que presenten un comportamiento sospechoso para la seguridad de la red institucional.

Artículo 52. El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para distribuir de forma ilegal licencias de software o reproducir información sin conocimiento del autor.

4.2.5 Política de Seguridad en Acceso de Terceros

Norma el acceso de terceras personas a la red institucional.

Artículo 53. El acceso de terceros será concedido siempre y cuando se cumplan con los requisitos de seguridad establecidos en el contrato de trabajo o asociación para el servicio, el cual deberá estar firmado por las entidades involucradas en el mismo.

Artículo 54. Todo usuario externo, estará facultado a utilizar única y exclusivamente el servicio que le fue asignado, y acatar las responsabilidades que devengan de la utilización del mismo.

Artículo 55. Los servicios accedidos por terceros acataran las disposiciones generales de acceso a servicios por el personal interno de la institución, además de los requisitos expuestos en su contrato con el Registro de la Propiedad del Cantón Cuenca.

4.2.6 Política de Control de Acceso a la Red

Norma el acceso de los usuarios a la red institucional.

Artículo56. El acceso a la red interna, se permitirá siempre y cuando se cumpla con los requisitos de seguridad necesarios, y éste será permitido mediante un mecanismo de autenticación.

Artículo 57. Se debe eliminar cualquier acceso a la red sin previa autenticación o validación del usuario o el equipo implicado en el proceso.

Artículo 58. Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, será motivo de verificación y tendrá como resultado directo la realización de una auditoria de seguridad.

Artículo 59. El Administrador de sistemas deberá emplear dispositivos de red para el bloqueo, enrutamiento, o el filtrado de tráfico evitando el acceso o flujo de información, no autorizada hacia la red interna o desde la red interna hacia el exterior.

Artículo 60. Los accesos a la red interna o local desde una red externa de la institución o extranet, se harán mediante un mecanismo de autenticación seguro y el tráfico entre ambas redes o sistemas será cifrado con una encriptación de mínimo 128 bits.

Artículo 61. Se registrara todo acceso a los dispositivos de red, mediante archivos de registro o Log, de los dispositivos que provean estos accesos.

Artículo 62. Se efectuara una revisión de Log de los dispositivos de acceso a la red en un tiempo máximo de 48 horas.

4.2.7 Política de Control de Acceso al Sistema Operativo

Norma las configuraciones básicas del sistema operativo en los equipos de la Institución.

Artículo 63. Se deshabilitarán las cuentas creadas por ciertas aplicaciones con privilegios de sistema, evitando que estas corran sus servicios con libertades nocivos para la seguridad del sistema.

Artículo 64. Al terminar una sesión de trabajo en las estaciones, los operadores o cualquier otro usuario, evitara dejar encendido el equipo, evitando proporcionar un entorno de utilización de la estación de trabajo.

Artículo 65. El acceso a la configuración del sistema operativo de los servidores, es únicamente permitido al usuario administrador.

Artículo 66. Los administradores de servicios, tendrán acceso único a los módulos de configuración de las respectivas aplicaciones que tienen bajo su responsabilidad.

Artículo 67. Todo servicio provisto o instalado en los servidores, correrá o será ejecutado bajo cuentas restrictivas, en ningún momento se obviaran situaciones de servicios corriendo con cuentas administrativas, estos privilegios tendrán que ser eliminados o configurados correctamente.

4.2.8 Política de Control de Acceso a las Aplicaciones

Norma la configuración de los sistemas que se ejecutan sobre los equipos de la Institución.

Artículo 68. Las aplicaciones deberán estar correctamente diseñadas, con funciones de acceso específicas para cada usuario del entorno operativo de la aplicación.

Artículo 69. Se deberá definir y estructurar el nivel de permisos sobre las aplicaciones, de acuerdo al nivel de ejecución o criticidad de las aplicaciones o archivos, y haciendo especial énfasis en los derechos de escritura, lectura, modificación, ejecución o borrado de información.

Artículo 70. Se deberán efectuar revisiones o pruebas minuciosas sobre las aplicaciones, de forma aleatoria, sobre distintas fases, antes de ponerlas en un entorno operativo real, con el objetivo de evitar redundancias en las salidas de información u otras anomalías.

Artículo 71. Las salidas de información, de las aplicaciones, en un entorno de red, deberán ser documentadas, y especificar la terminal por la que deberá ejecutarse exclusivamente la salida de información.

Artículo 72. Se deberá llevar un registro mediante Log de aplicaciones, sobre las actividades de los usuarios en cuanto a accesos, errores de conexión, horas de conexión, intentos fallidos, terminal desde donde conecta, entre otros, de manera que proporcionen información relevante y revisable posteriormente.

4.2.9 Política de Monitoreo del Acceso y Uso del Sistema

Norma el registro del uso de las aplicaciones informáticas de la Institución.

Artículo 73. Se registrará y archivará toda actividad, procedente del uso de las aplicaciones, sistemas de información y uso de la red, mediante archivos de Log o bitácoras de sistemas.

Artículo 74. Los archivos de Log, almacenarán nombres de usuarios, nivel de privilegios, IP de terminal, fecha y hora de acceso o utilización, actividad desarrollada, aplicación implicada en el proceso, intentos de conexión fallidos o acertados, archivos a los que se tuvo acceso, entre otros.

Artículo 75. Se efectuará una copia automática de los archivos de Log, y se conducirá o enviara hacia otra terminal o servidor, evitando se guarde la copia localmente donde se produce.

4.2.10 Política de Responsabilidades y Procedimientos Operativos

Norma los procedimientos operativos que deben llevar a cabo los administradores de las aplicaciones y servicios que se encuentran en ejecución en la Institución.

Artículo 76. El personal administrador de algún servicio, es el responsable absoluto por mantener en óptimo funcionamiento ése, coordinar esfuerzos con el Administrador de Sistemas, para fomentar una cultura de administración segura y servicios óptimos.

Artículo 77. Las configuraciones y puesta en marcha de servicios, son normadas por el Comité de Seguridad.

Artículo 78. El personal responsable de los servicios, llevará archivos de registro de fallas de seguridad del sistema, revisara, estos archivos de forma frecuente y en especial después de ocurrida una falla.

4.2.11 Política de Planificación y Aceptación de Sistemas

Norma el proceso de aceptación de software adquirido o provisto por terceros.

Artículo79. El Personal asignado en el área de planificación, efectuarán todo el proceso propio de la proyección, desarrollo, adquisición, comparación y adaptación del software necesario para la Institución.

Artículo 80. La aceptación del software se hará efectiva por la Dirección de la institución que es beneficiaria de sus servicios, previo análisis y pruebas efectuadas por el personal de informática.

Artículo 81. Únicamente se utilizará software certificado o en su defecto software previamente revisado y aprobado, por personal calificado en el área de seguridad.

Artículo 82. La aceptación y uso de los sistemas no exonera, de responsabilidad alguna sobre el Administrador de Sistemas, para efectuar pruebas o diagnósticos a la seguridad de los mismos.

Artículo 83. El software de desarrollo propio, deberá ser analizado y aprobado, por el Administrador de Sistemas, antes de su implementación.

Artículo 84. Es tarea de programadores el realizar pruebas de validación de entradas, en cuanto a:

a. Valores fuera de rango.
b. Caracteres inválidos, en los campos de datos.
c. Datos incompletos.
d. Datos con longitud excedente o valor fuera de rango.
e. Datos no autorizados o inconsistentes.
f. Procedimientos operativos de validación de errores
g. Procedimientos operativos para validación de caracteres.
h. Procedimientos operativos para validación de la integridad de los datos.
i. Procedimientos operativos para validación e integridad de las salidas.

Artículo 85. Toda prueba de las aplicaciones o sistemas, se deberá hacer teniendo en cuenta las medidas de protección de los archivos de producción reales.

Artículo 86. 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 dispositivos físicos, mediante tratamiento electrónico.

4.2.12 Política de Protección Contra Software Malicioso

Norma el uso de software para prevenir el uso de programas maliciosos.

Artículo 87. Se adquirirá y utilizará software únicamente de fuentes confiables.

Artículo 88. En caso de ser necesaria la adquisición de software de fuentes no confiables, este se adquirirá en código fuente.

Artículo 89. Los servidores, al igual que las estaciones de trabajo, tendrán instalado y configurado correctamente software antivirus actualizable y activada la protección en tiempo real.

4.2.13 Política de Mantenimiento

Norma el mantenimiento de las aplicaciones que se ejecutan en los equipos de la Institución.

Artículo 90. El mantenimiento de las aplicaciones y software de sistemas es de exclusiva responsabilidad del personal del Centro de Cómputo, o del personal de soporte técnico.

Artículo 91. El cambio de archivos de sistema, no es permitido, sin una justificación aceptable y verificable por el gestor de seguridad.

Artículo 92. Se llevará un registro global del mantenimiento efectuado sobre los equipos y cambios realizados desde su instalación.

4.2.14 Política de Manejo de Seguridad y Medios de Almacenamiento

Norma el manejo de los medios de almacenamiento y de respaldos de la información institucional.

Artículo 93. Los medios de almacenamiento o copias de seguridad del sistema de archivos, o información de la institución, serán etiquetados de acuerdo a la información que almacenan u objetivo que suponga su uso, detallando o haciendo alusión a su contenido.

Artículo 94. Los medios de almacenamiento con información crítica o copias de respaldo deberán ser manipulados única y exclusivamente por el personal encargado de hacer los respaldos y el personal encargado de su salvaguarda.

Artículo 95. Todo medio de almacenamiento con información crítica será guardado bajo llave en una caja especial a la cual tendrá acceso únicamente, el Administrador de Sistemas o el Director, esta caja no debería ser removible, una segunda copia será resguardada por un tercero, entidad financiera o afín.

Artículo 96. Se llevará un control, en el que se especifiquen los medios de almacenamiento en los que se debe guardar información y su uso.

4.3 Seguridad Física

4.3.1 Política de Seguridad de los Equipos

Norma la seguridad física de los equipos informáticos de la Institución.

Artículo 97. El cableado de red, se instalará físicamente separado de cualquier otro tipo de cables, llámese a estos de corriente o energía eléctrica, para evitar interferencias.

Artículo 98. Los servidores, sin importar al grupo al que estos pertenezcan, con problemas de hardware, deberán ser reparados localmente, de no cumplirse lo anterior, deberán ser retirados sus medios de almacenamiento.

Artículo 99. Los equipos o activos críticos de información y proceso, deberán ubicarse en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por el Administrador de Sistemas y las personas responsables por esos activos, quienes deberán poseer su debida identificación.

4.3.2 Política de Controles Generales

Establece los parámetros de controles generales sobre los activos pertenecientes a la Institución.

Artículo 100. Las estaciones o terminales de trabajo, con procesamientos críticos no deben de contar con medios de almacenamientos extraíbles, que puedan facilitar el robo o manipulación de la información por terceros o personal que no deba tener acceso a esta información.

Artículo 101. En ningún momento se deberá dejar información sensible de robo, manipulación o acceso visual, sin importar el medio en el que esta se encuentre, de forma que pueda ser alcanzada por terceros o personas que no deban tener acceso a esta información.

Artículo 102. Deberá llevarse un control exhaustivo del mantenimiento preventivo y otro para el mantenimiento correctivo que se les haga a los equipos.

Artículo 103. Toda oficina o área de trabajo debe poseer entre sus inventarios, herramientas auxiliares (extintores, alarmas contra incendios, lámpara de

emergencia), necesarias para salvaguardar los recursos tecnológicos y la información, en concordancia con las políticas de Seguridad y Salud Ocupacional de la Institución.

Artículo 104. Toda visita a las oficinas de tratamiento de datos críticos e información (Centro de Cómputo, sala de servidores entre otros) deberá ser registrada mediante un formulario de accesos a las salas de procesamiento crítico, para posteriores análisis del mismo.

Artículo 105. La sala o cuarto de servidores, deberá estar separada de las oficinas administrativas de la unidad de informática o cualquier otra unidad, departamento o sala de recepción del personal, mediante una división en la unidad de informática, recubierta de material aislante o protegido contra el fuego, Esta sala deberá ser utilizada únicamente por las estaciones prestadoras de servicios y/o dispositivos a fines.

Artículo 106. El suministro de energía eléctrica debe hacerse a través de un circuito exclusivo para los equipos de cómputo, o en su defecto el circuito que se utilice no debe tener conectados equipos que demandan grandes cantidades de energía.

Artículo 107. El suministro de energía eléctrica debe estar debidamente polarizado, no siendo conveniente la utilización de polarizaciones locales de tomas de corriente, sino que debe existir una red de polarización.

Artículo 108. Las instalaciones de las áreas de trabajo deben contar con una adecuada instalación eléctrica, y proveer del suministro de energía mediante una estación de alimentación ininterrumpida o UPS para poder proteger la información.

Artículo 109. Las salas o instalaciones físicas de procesamiento de información deberán poseer información en carteles, sobre accesos, alimentos o cualquier otra actividad contraria a la seguridad de la misma o de la información que ahí se procesa.

4.4 Seguridad Legal

4.4.1 Política de Licenciamiento de Software

Norma la utilización de software propietario que se ejecuta en la Institución.

Artículo 110. La Institución, se reserva el derecho de respaldo, a cualquier miembro facultativo miembro de las áreas administrativas, ante cualquier asunto legal relacionado a infracciones a las leyes de copyright o piratería de software.

Artículo 111. Todo el software comercial que utilice la Institución, deberá estar legalmente registrado, en los contratos de arrendamiento de software con sus respectivas licencias.

Artículo 112. La adquisición de software por parte de personal que labore en la institución, no expresa el consentimiento de la institución, la instalación del mismo, no garantiza responsabilidad alguna para la Institución, por ende la institución no se hace responsable de las actividades de sus empleados.

Artículo 113. Tanto el software comercial como el software libre son propiedad intelectual exclusiva de sus desarrolladores, la Institución respeta la propiedad intelectual y se rige por el contrato de licencia de sus autores.

Artículo 114. El software comercial licenciado a la Institución, es propiedad exclusiva de la institución, la misma se reserva el derecho de reproducción de éste, sin el permiso de sus autores, respetando el esquema de cero piratería y/o distribución a terceros.

Artículo 115. En caso de transferencia de software comercial a terceros, se harán las gestiones necesarias para su efecto y se acataran las medidas de licenciamiento relacionadas con la propiedad intelectual.

Artículo 116. Las responsabilidades inherentes al licenciamiento de software libre son responsabilidad absoluta de la Institución.

Artículo 117. Cualquier cambio en la política de utilización de software comercial o software libre, se hará documentado y en base a las disposiciones de la respectiva licencia.

Artículo 118. El software desarrollado internamente, por el personal que labora en la institución es propiedad exclusiva del Registro de la Propiedad del Cantón Cuenca.

Artículo 119. La adquisición del software libre o comercial deberá ser gestionada con las autoridades competentes y acatando sus disposiciones legales, en ningún momento se obtendrá software de forma fraudulenta.

Artículo 120. Los contratos con terceros, en la gestión o prestación de un servicio, deberán especificar, las medidas necesarias de seguridad, nivel de prestación del servicio, y/o el personal involucrado en tal proceso.

4.4.2 Política de Revisión de las Políticas de Seguridad y Cumplimiento Técnico

Norma la revisión y cumplimiento de las políticas de seguridad establecidas para la Institución.

Artículo 121. Toda violación a las políticas de licenciamiento de software, será motivo de sanciones aplicables al personal que incurra en la violación.

Artículo 122. El documento de seguridad será elaborado y actualizado por el Administrador de Sistemas, junto al Comité de Seguridad, su aprobación y puesta en ejecución será responsabilidad del Registrador.

Artículo 123. Cualquier violación a la seguridad por parte del personal que labora, para la Institución, así como terceros que tengan relación o alguna especie de contrato con la institución se harán acreedores a sanciones aplicables de ley.

4.4.3 Política de Consideraciones Sobre Auditorías de Sistemas

Norma el proceso de auditoria de sistemas y de seguridad que se realicen en la Institución.

Artículo 124. Se debe efectuar una auditoria de seguridad a los sistemas de acceso a la red, enmarcada en pruebas de acceso tanto internas como externas, desarrolladas por personal técnico especializado o en su defecto personal capacitado en el área de seguridad.

Artículo 125. Toda auditoria a los sistemas, estará debidamente aprobada, y tendrá el sello y firma de la Dirección.

Artículo 126. Cualquier acción que amerite la ejecución de una auditoria a los sistemas informáticos deberá ser documentada y establecida su aplicabilidad y objetivos de la misma, así como razones para su ejecución, personal involucrada en la misma y sistemas implicados.

Artículo 127. La auditoría no deberá modificar en ningún momento el sistema de archivos de los sistemas implicados, en caso de haber necesidad de modificar algunos, se deberá hacer un respaldo formal del sistema o sus archivos.

Artículo 128. Las herramientas utilizadas para la auditoria deberán estar separadas de los sistemas de producción y en ningún momento estas se quedaran al alcance de personal ajeno a la elaboración de la auditoria.

4.5 Seguridad de los Documentos de información en medios tradicionales.

4.5.1 Política de Manejo de Secciones de Archivo y Biblioteca.

Artículo 129. Los espacios destinados para la custodia de los documentos, deben contar con las condiciones adecuadas de limpieza y protección. De manera que cada área administrativa, lugar de trabajo y sala de archivos debe disponer de un espacio adecuado para la custodia de la información, minimizando los riesgos de deterioro.

Artículo 130. La conservación, recuperación, seguridad y consulta de los documentos, en los documentos de gestión de las áreas administrativas y Registrales, independientemente de su forma o soporte, es responsabilidad de sus funcionarios. Por lo tanto, deben acoger los procedimientos y directrices establecidas por la Institución para la gestión documental.

Artículo 131. Todo documento generado por las áreas en cumplimiento de sus funciones, una vez que ha cumplido su trámite o disminuido su consulta, debe ser transferido al Área de Archivo, incluyendo los documentos para eliminación. Por ningún motivo deben estar represados en las oficinas.

Artículo 132. La identificación y descripción de los documentos debe estar acorde con las codificaciones de las series documentales.

Artículo 133. Es responsabilidad de cada Director de área, mantener actualizado el procedimiento, de manera que, a través de los Protocolos Registrales y archivos se controle el manejo y modificación de los asientos registrales.

Artículo 134. Cuando un servidor se retire o cambie de cargo en el Registro de la Propiedad del cantón Cuenca, debe entregar inventario (utilice el formato de transferencia documental) de sus documentos físicos y digitales a su Jefe inmediato, o en caso de que la información haya terminado su tiempo de gestión debe hacer transferencia documental al Archivo Central.

Artículo 135. Los usuarios que solicitan documentos en calidad de préstamo al Área de Archivo Registral, son responsables de la integridad, seguridad y devolución de la información suministrada.

Artículo 136. Se capacitará en materia de manejo de archivos y seguridad de los mismos a los encargados de archivo y biblioteca.

Artículo 137. Se deberá informar al Comité de seguridad de cualquier falta a la Política de Seguridad, que pueda poner en riesgo los activos bajo su responsabilidad.

Artículo 138. Se deberá proponer las medidas de mitigación adecuadas.

Artículo 139. Los documentos deberán estar organizados y la información accesible para su uso, en instalaciones adecuadas y bajo dirección de un funcionario de la misma repartición, nombrado especialmente para tal cometido, el cual se denominará "encargado de archivos".

Artículo 140. Ante el cese de funciones de un funcionario del Área de Archivo, se debe confeccionar un acta de entrega o de traspaso de la documentación asociada a la gestión del funcionario que se retira.

4.5.2 Política de Manejo de Biblioteca Registral

Norma la utilización de la biblioteca registral de la Institución.

Artículo 141. El Registrador de la Propiedad, nombrará un encargado de la Biblioteca Central del Registro, en donde se contará con todos los libros y documentos en medios tradicionales, de forma clasificada e inventariada.

Artículo 142. Se velará por el ordenamiento, protección, uso y resguardo del Archivo, de conformidad a la normativa vigente.

Artículo 143. Se asegurará que la información reciba un nivel de protección apropiado.

Artículo 144. Se clasificará la información en términos de su valor, requerimientos legales, sensibilidad y grado crítico para el Servicio.

Artículo 145. Se implementará los procedimientos adecuados para el etiquetado y manejo de la información de acuerdo a la normativa vigente.

Artículo 146. Se definirá procedimientos de manejo seguro que incluyan procesamiento, almacenamiento, transmisión, desclasificación y destrucción.

Artículo 147. Se definirá los procedimientos de la cadena de custodia y el registro de cualquier incidente de seguridad relevante.

4.5.3 Política de Manejo de Archivo de Oficina

Artículo 148. El Director de cada área, será el encargado del Archivo de Oficina, pudiendo delegar esta función a un delegado de su confianza; archivo en donde se contará con todos los libros y documentos en medios tradicionales, de forma clasificada e inventariada.

Artículo 149. El Encargado del Archivo de Oficina tendrá por función velar por el ordenamiento, protección, uso y resguardo del Archivo de Oficina, de conformidad a la normativa vigente.

Artículo 150. Se documentará y actualizará periódicamente la clasificación de datos efectuada.

Artículo 151. Se velará por la seguridad de sus datos, procurando la correcta aplicación de mecanismos orientados a la mitigación de riesgos.

4.5.4 Política de Manejo de Archivo del Personal.

Artículo 152. Se velará por el correcto uso, resguardo y protección de los Activos de Información de los funcionarios del Registro de la Propiedad, como por ejemplo, calificaciones, anotaciones, expedientes que posean los funcionarios etc.

Artículo 153. Se realizará inducción a los Funcionarios nuevos respecto de la Política General de Seguridad del Servicio, incluidas normas y procedimientos asociados.