POLÍTICA DE SEGURIDAD INFORMÁTICA

Contenido

Exposición de motivos

I. Introducción

II. Políticas de seguridad: II.1

Equipo

a) De la instalación de equipo de cómputo

b) Para el mantenimiento de equipo de cómputo

c) De la actualización del equipo

d) De la reubicación del equipo de cómputo

II.2 Control de accesos

a) Del acceso a áreas críticas

b) Del control de acceso al equipo de cómputo c) Del control de acceso local a la red

d) De control de acceso remoto

e) De acceso a los sistemas administrativos
f) Del WWW

II.3. Utilización de recursos de la red. Software

a) De la adquisición de software

b) De la instalación de software

c) De la actualización del software

d) De la auditoría de software instalado

e) Del software propiedad de la institución

f) Sobre el uso de software académico

g) De la propiedad intelectual

II.5 Supervisión y evaluación

III. Generales

IV. Sanciones

V. Recomendaciones

EXPOSICIÓN DE MOTIVOS

Ante el esquema de globalización que las tecnologías de la información han originado principalmente por el uso masivo y universal de la internet y sus tecnologías, las instituciones se ven inmersas en ambientes agresivos donde el delinquir, sabotear, robar se convierte en retos para delincuentes informáticos universales conocidos como Hackers, Crackers, etc., es decir en transgresores.

Conforme las tecnologías se han esparcido, la severidad y frecuencia las han transformado en un continuo riesgo, que obliga a las entidades a crear medidas de emergencia y políticas definitivas para contrarrestar estos ataques y transgresiones.

En nuestro país no existe una sola institución que no se haya visto sujeta a los ataques en sus instalaciones, tanto desde el interior como del exterior, basta decir que cuando en el centro estamos sujetos a un ataque un grupo de gente se involucran y están pendientes de éste, tratando de contrarrestar y anular estas amenazas reales.

Después del diagnóstico que se llevó a cabo, se observó la carencia de un inventario detallado de los equipos que se encuentran en la corporación, lo cual hace difícil su administración.

La carencia de recursos humanos involucrados en seguridad, la escasa concientización, la falta de visión y las limitantes económicas han retrasado el plan de seguridad que se requiere en la entidad.

El objetivo principal de la SUBAREA DE SISTEMAS E INFORMATICA es brindar a los usuarios los recursos informáticos con la cantidad y calidad que demandan, esto es, que tengamos continuidad en el servicio los 365 días del año confiable. Así, la cantidad de recursos de cómputo y de telecomunicaciones con que cuenta el Centro son de consideración y se requiere que se protejan para garantizar su buen funcionamiento.

La seguridad de las instituciones en muchos de los países se ha convertido en cuestión de seguridad nacional, por ello contar con un documento de políticas de seguridad es imprescindible, y se debe plasmar mecanismos confiables que con base en la política institucional proteja los activos del Centro.

Así pues, ante este panorama surge el siguiente proyecto de políticas rectoras que harán que la Dirección de Telemática pueda disponer de los ejes de proyección que en materia de seguridad la Institución requiere.

RESUMEN

El presente es una propuesta de las políticas de seguridad que en materia de informática y de comunicaciones digitales de la SUBAREA DE SISTEMAS E INFORMATICA de CORPOCESAR, ha elaborado, para normar a la institución.

Algunas acciones que por la naturaleza extraordinaria tuvieron que ser llevadas a la práctica como son: los inventarios y su control, se mencionan, así como todos los aspectos que representan un riesgo o las acciones donde se ve involucrada y que compete a las tecnologías de la información; se han contemplado también las políticas que reflejan la visión de la actual administración respecto a la problemática de seguridad informática institucional.

La propuesta ha sido detenidamente planteada, analizada y revisada a fin de no contravenir con las garantías básicas del individuo, y no pretende ser una camisa de fuerza, y más bien muestra una buena forma de operar el sistema con seguridad, respetando en todo momento estatutos y reglamentos vigentes de la corporación.

I. INTRODUCCIÓN

Los requerimientos de seguridad que involucran las tecnologías de la información, en pocos años han cobrado un gran auge, y más aún con las de carácter globalizador como los son la de Internet y en particular la relacionada con el Web, la visión de nuevos horizontes explorando más allá de las fronteras naturales, situación que ha llevado la aparición de nuevas amenazas en los sistemas computarizados.

Llevado a que muchas organizaciones gubernamentales y no gubernamentales internacionales desarrollen políticas que norman el uso adecuado de estas destrezas tecnológicas y recomendaciones para aprovechar estas ventajas, y evitar su uso indebido, ocasionando problemas en los bienes y servicios de las entidades.

De esta manera, las políticas de seguridad en informática de CORPOCESAR emergen como el instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permiten al Centro cumplir con su misión.

El proponer esta política de seguridad requiere un alto compromiso con la institución, agudeza técnica para establecer fallas y deficiencias, constancia para renovar y actualizar dicha política en función del ambiente dinámico que nos rodea.

II. POLÍTICAS DE SEGURIDAD

La SUBAREA DE SISTEMAS E INFORMATICA actualmente está conformado por dos (2) funcionarios los cuales compelen distintas funciones referentes a el soporte y mantenimiento de la plataforma tecnológica, desarrollo de sistemas de información, administración de bases de datos, gestión de recursos de tecnología y administración de la red; dado a esta razón ha sido necesario emitir políticas particulares para el conjunto de recursos y facilidades informáticas, de la infraestructura de telecomunicaciones y servicios asociados a ellos, provistos por la SUBAREA DE SISTEMAS E INFORMATICA. Así pues este apartado contiene una clasificación de estas políticas, y son:

II.1 EQUIPOS

De la Instalación de Equipo de Cómputo.

1. Todo el equipo de cómputo (computadoras, estaciones de trabajo, servidores, y equipo accesorio), que esté o sea conectado a la red de CORPOCESAR, o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe sujetarse a las normas y procedimientos de instalación que emite el departamento de SUBAREA DE SISTEMAS E INFORMATICA.

2. La SUBAREA DE SISTEMAS E INFORMATICA en coordinación con el área de LOGÍSTICA deberá tener un registro de todos los equipos propiedad de la corporación.

3. El equipo de la institución que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en un área que cumpla con los requerimientos de: seguridad física, las condiciones ambientales, la alimentación eléctrica y la normatividad para el acceso de equipos que la SUBAREA DE SISTEMAS E INFORMATICA IMPLANTE.

4. Los funcionarios de la SUBAREA DE SISTEMAS E INFORMATICA debe dar cumplimiento a las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos en su ubicación, de adjudicación, sistema y misión.

5. La protección física de los equipos corresponde a quienes en un principio se les asigna, y corresponde notificar los movimientos en caso de que existan, a las autoridades correspondientes (departamento de Mantenimiento, departamento de Cómputo, departamento de Control Patrimonial, y otros de competencia).

Del Mantenimiento de Equipo de Cómputo.

1. La SUBAREA DE SISTEMAS E INFORMATICA, corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar. Para tal fin debe emitir las normas y procedimientos respectivos.

2. En el caso de los equipos atendidos por terceros la SUBAREA DE SISTEMAS E INFORMATICA deberá coordinar y velar por el cuidado y preservación del mismo.

3. Los responsables de las áreas de Cómputo de un departamento pueden otorgar mantenimiento preventivo y correctivo, a partir del momento en que sean autorizados por la SUBAREA DE SISTEMAS E INFORMATICA.

4. Corresponde a la SUBAREA DE SISTEMAS E INFORMATICA debe dar a conocer las listas de las personas, que puedan tener acceso a los equipos y brindar los servicios de mantenimiento básico, a excepción de los atendidos por terceros.

5. Por motivos de normatividad interna CORPOCESAR comunica queda que estrictamente prohibido dar mantenimiento a equipos de cómputo que no sea propiedad de la institución.

De la actualización del equipo.

1. Todo el equipo de cómputo (computadoras personales, estaciones de trabajo, servidores y demás relacionados), y los de telecomunicaciones que sean propiedad del CORPOCESAR debe procurarse sea actualizado tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

De la reubicación del equipo de cómputo.

1. La reubicación del equipo de cómputo se realizará satisfaciendo las normas y procedimientos que la SUBAREA DE SISTEMAS E INFORMATICA emita para ello.

2. En caso de existir personal técnico de apoyo, éste notificará de los cambios tanto físicos como de software que realice, dando aviso a la SUBAREA DE SISTEMAS E INFORMATICA y al área de LOGÍSTICA notificando también los cambios de los equipos para adjuntarlos al inventario.

3. El equipo de cómputo a reubicar sea de o bien externo se hará únicamente bajo la autorización del responsable contando el lugar a donde se hará la ubicación con los medios necesarios para la instalación del equipo.

II.2 DEL CONTROL DE ACCESOS

Del Acceso a Áreas Críticas.

1. El acceso de personal se llevará acabo de acuerdo a las normas y procedimientos que dicta la SUBAREA DE SISTEMAS E INFORMATICA.

   En concordancia con la política de la institución y debido a la naturaleza de estas áreas se llevará un registro permanente del tráfico de personal, sin excepción.

2. La SUBAREA DE SISTEMAS E INFORMATICA deberá proveer de la infraestructura de seguridad requerida con base en los requerimientos específicos de cada área.

3. Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las autoridades superiores de la institución.

Del control de acceso al equipo de cómputo.

1. Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.

2. Las áreas donde se tiene equipo de propósito general cuya misión es crítica estarán sujetas a los requerimientos que la SUBAREA DE SISTEMAS E INFORMATICA emita.
3. Las áreas de cómputo de los departamentos donde se encuentre equipo cuyo

propósito reúna características de imprescindible y de misión crítica, deberán sujetarse también a las normas que establezca la SUBAREA DE SISTEMAS E INFORMATICA.

4. Los accesos a las áreas de críticas deberán de ser clasificados de acuerdo a las normas que dicte la SUBAREA DE SISTEMAS E INFORMATICA de común acuerdo con su comité de seguridad informática.

5. Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, la Dirección de la SUBAREA DE SISTEMAS E INFORMATICA tiene la facultad de acceder a cualquier equipo de cómputo que no estén bajo su supervisión.

Del control de acceso local a la red.

1. La SUBAREA DE SISTEMAS E INFORMATICA es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.

2. La SUBAREA DE SISTEMAS E INFORMATICA es la responsable de difundir el reglamento la SUBAREA DE SISTEMAS E INFORMATICA para el uso de la red y de procurar su cumplimiento.

3. Dado el carácter unipersonal del acceso a la Red de CORPOCESAR, la verificará el uso responsable, de acuerdo al Reglamento para el uso de la red.

4. El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos, equipo de supercómputo centralizado y distribuido, etc.) conectado a la red es administrado por la SUBAREA DE SISTEMAS E INFORMATICA.

5. Todo el equipo de cómputo que esté o sea conectado a la Red de CORPOCESAR, o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe de sujetarse a los procedimientos de acceso que emite la SUBAREA DE SISTEMAS E INFORMATICA.

De control de acceso remoto.

1. La SUBAREA DE SISTEMAS E INFORMATICA es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.

2. Para el caso especial de los recursos de SERVIDORES a terceros deberán ser autorizados por la DIRECCIÓN GENERAL o por la COORDINACION SUBAREA ADMINISTRATIVA .

3. El usuario de estos servicios deberá sujetarse al Reglamento de uso de la Red de CORPOCESAR y en concordancia con los lineamientos generales de uso de Internet.

4. El acceso remoto que realicen personas ajenas a la institución deberá cumplir las normas que emite la oficina de SUBAREA DE SISTEMAS E INFORMATICA.

De acceso a los sistemas administrativos.

1. Tendrá acceso a los sistemas administrativos solo el personal de CORPOCESAR o persona que tenga la autorización por la DIRECCIÓN GENERAL DE LA ENTIDAD.

2. El manejo de información administrativa que se considere de uso restringido deberá ser cifrado con el objeto de garantizar su integridad.

3. Los servidores de bases de datos administrativos son dedicados, por lo que se prohíben los accesos de cualquiera, excepto para el personal de la SUBAREA DE SISTEMAS E INFORMATICA.

4. El control de acceso a cada sistema de información de la Dirección Administrativa será determinado por la unidad responsable de generar y procesar los datos involucrados.

Del WWW y Servidor Web.

1. En concordancia con la LEY 1273 y de común acuerdo con las políticas generales de informática, la COORDINACION SUBAREA ADMINISTRATIVA es el responsable de instalar y administrar el o los servidor(es) WWW. Es decir, sólo se permiten servidores de páginas autorizados por, la SUBAREA DE SISTEMAS E INFORMATICA.

2. La SUBAREA DE SISTEMAS E INFORMATICA deberá emitir las normas y los requerimientos para la instalación de servidores de páginas locales, de bases de datos, del uso de la Intranet institucional, así como las especificaciones para que el acceso a estos sea seguro.

3. Los accesos a las páginas de Web a través de los navegadores deben sujetarse a las normas que previamente se manifiestan en el Reglamento de acceso a la red de CORPOCESAR.

4. A los responsables de los servidores de Web corresponde la verificación de

respaldo y protección.

5. Toda la programación involucrada en la tecnología Web deberá estar de acuerdo con las normas y procedimientos que la SUBAREA DE SISTEMAS E INFORMATICA emita.

6. El material que aparezca en la página de Internet de CORPOCESAR deberá ser probado por la SUBAREA DE SISTEMAS E INFORMATICA, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).

7. En concordancia con la libertad de investigación, se acepta que en la red del CORPOCESAR conectada a Internet pueda ponerse información individual sin autorización (siempre y cuando no contravenga las disposiciones que se aplican a las instituciones gubernamentales paraestatales).

8. Con referencia a la seguridad y protección de las páginas, así como al diseño de las mismas deberá referirse a las consideraciones de diseño de páginas electrónicas establecidas por la SUBAREA DE SISTEMAS E INFORMATICA.

9. La SUBAREA DE SISTEMAS E INFORMATICA tiene la facultad de llevar a cabo la revisión periódica de los accesos a nuestros servicios de información, y conservar información del tráfico.

II.3 DE UTILIZACIÓN DE LOS RECURSOS DE LA RED

1. Los recursos disponibles a través de la Red de CORPOCESAR serán de uso exclusivo para asuntos relacionados con las actividades de la entidad.

2. La SUBAREA DE SISTEMAS E INFORMATICA es la responsable de emitir y dar seguimiento al Reglamento para el uso de la Red.

3. La SUBAREA DE SISTEMAS E INFORMATICA debe propiciar el uso de las tecnologías de la información con el fin de contribuir con las directrices económicas y ecológicas de la institución.

II.4 DEL SOFTWARE

De la adquisición de software.

1. En concordancia con la política de la institución, el Comité de Informática y la SUBAREA DE SISTEMAS E INFORMATICA son los organismos oficiales de la entidad para establecer los mecanismos de procuración de sistemas informáticos.

2. Del presupuesto de los proyectos que se otorga a las diferentes áreas de CORPOCESAR una cantidad deberá ser aplicada para la adquisición de sistemas de información licenciados o el desarrollo de sistemas de información a la medida.

3. De acuerdo con el MINISTERIO DE LAS TIC, la Dirección General en conjunto con el Comité de Informática y la SUBAREA DE SISTEMAS E INFORMATICA, propiciará la adquisición de licencias de sitio, licencias flotantes, licencias por empleado y de licencias en cantidad, para obtener economías de escala y de acorde al plan de austeridad del gobierno de la república.

4. Corresponderá a la SUBAREA DE SISTEMAS E INFORMATICA emitir las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.

5. De acuerdo a los objetivos globales de la SUBAREA DE SISTEMAS E INFORMATICA deberá propiciar la adquisición y asesoramiento en cuanto a software de vanguardia.

6. En cuanto a la paquetería sin costo deberá respetarse la propiedad intelectual intrínseca del autor.

7. La SUBAREA DE SISTEMAS E INFORMATICA promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

8. La SUBAREA DE SISTEMAS E INFORMATICA deberá promover el uso de sistemas programáticos que redunden en la independencia de la institución con los proveedores.

De la instalación de software.

1. Corresponde a la SUBAREA DE SISTEMAS E INFORMATICA emitir las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.

2. En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y de acorde a la propiedad intelectual.

3. Los departamentos de Cómputo y de Informática son los responsables de brindar asesoría y supervisión para la instalación de software informático, asimismo la SUBAREA DE SISTEMAS E INFORMATICA para el software de telecomunicaciones.

4. La instalación de software que desde el punto de vista de la SUBAREA DE SISTEMAS E INFORMATICA pudiera poner en riesgo los recursos de la institución no está permitida.

5. Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, y otros que se apliquen).

6. La protección lógica de los sistemas corresponde a quienes en un principio se les asigna y les compete notificar cualquier movimiento al departamento de Cómputo.

De la actualización del software.

1. La adquisición y actualización de software para equipo especializado de cómputo y de telecomunicaciones se llevará a cabo de acuerdo a la calendarización que anualmente sea propuesta por la SUBAREA DE SISTEMAS E INFORMATICA.

2. Corresponde a la SUBAREA DE SISTEMAS E INFORMATICA autorizar cualquier adquisición y actualización del software.

3. Las actualizaciones del software de uso común o más generalizado se llevarán a cabo de acuerdo al plan de actualización desarrollado por la SUBAREA DE SISTEMAS E INFORMATICA.

De la auditoría de software instalado.

1. El área de CONTROL INTERNO de CORPOCESAR es el responsable de realizar revisiones periódicas para asegurar que sólo programación con licencia esté instalada en las computadoras de la institución.

2. El área de CONTROL INTERNO y el comité de seguridad informática propiciará la conformación de un grupo especializado en auditoría de sistemas de cómputo y sistemas de información.

3. Corresponderá al grupo especializado dictar las normas, procedimientos y calendarios de auditoría.

Del software propiedad de la institución.

1. Toda la programática adquirida por la institución sea por compra, donación o cesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera.

2. La SUBAREA DE SISTEMAS E INFORMATICA en coordinación con la Subdirección administrativa y financiera deberá tener un registro de todos los paquetes de programación.

3. Todos los sistemas programáticos (programas, bases de datos, sistemas operativos, interfaces) desarrollados con o a través de los recursos de CORPOCESAR se mantendrán como propiedad de la institución respetando la propiedad intelectual del mismo.

4. Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservar.

5. Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución deben estar resguardados.

6. Corresponderá a la SUBAREA DE SISTEMAS E INFORMATICA promover y difundir los mecanismos de respaldo y salvaguarda de los datos y de los sistemas programáticos.

7. La SUBAREA DE SISTEMAS E INFORMATICA en conjunto con la COORDINACION SUBAREA ADMINISTRATIVA propiciará la gestión de patentes y derechos de creación de software de propiedad de la institución.

8. La SUBAREA DE SISTEMAS E INFORMATICA administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política informática.

De la propiedad intelectual.

1. Corresponde a la SUBAREA DE SISTEMAS E INFORMATICA, procurar que todo el software instalado en CORPOCESAR esté de acuerdo a la ley de propiedad intelectual a que dé lugar.

II.5 De supervisión y evaluación

1. Las auditorías de cada actividad donde se involucren aspectos de seguridad lógica y física deberán realizarse periódicamente y deberá sujetarse al calendario que establezca la SUBAREA DE SISTEMAS E INFORMATICA y/o el grupo especializado de seguridad.

2. Para efectos de que la institución disponga de una red con alto grado de confiabilidad, será necesario que se realice un monitoreo constante sobre todos y cada uno de los servicios que las tecnologías de la Internet e Intranet disponen.

3. Los sistemas considerados críticos, deberán estar bajo monitoreo permanente.

III. GENERALES.

1. Cada uno de los procesos deberá emitir los planes de contingencia que correspondan a las actividades críticas que realicen.

2. Debido al carácter confidencial de la información, el personal de la SUBAREA DE SISTEMAS E INFORMATICA deberá de conducirse de acuerdo a los códigos de ética profesional y normas y procedimientos establecidos.

IV. SANCIONES.

Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la SUBDIRECCIÓN ADMINISTRATIVA Y FINANCIERA.

Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.

Corresponderá al Comité de Informática hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de la institución.

Todas las acciones en las que se comprometa la seguridad de la Red de CORPOCESAR y que no estén previstas en esta política, deberán ser revisadas por la Dirección General para dictar una resolución sujetándose al estado de derecho.

En cuanto a los daños a la infraestructura tecnológica, Interceptación ilegítima de sistema informático o red de telecomunicación, Suplantación de sitios Web para capturar datos personales, Acceso abusivo a un sistema informático y de más delitos informáticos se aplicara la ley 1273, incurriendo a las sanciones que aplica.

V.
RECOMENDACIONES

Se tendrá que convocar un COMITÉ DE SEGURIDAD INFORMÁTICA a nivel de la alta gerencia, la cual provea soluciones informáticas y tecnológicas, promoviendo la preservación de la arquitectura tecnológica de la entidad y la información vital de la misma.

Para el óptimo funcionamiento De la SUBAREA DE SISTEMAS E INFORMATICA recomiendo conformar tres procesos los cuales velaran por el óptimo funcionamiento de la infraestructura tecnológica de la entidad. Estos procesos estarán distribuidos de la siguiente manera:

- Proceso de soporte y mantenimiento.
- Proceso de administración de redes.
- Proceso de Informática, investigación y desarrollo

Se recomienda implementar planes de contingencia para todos los procesos concernientes a seguridad informática y continuidad del negocio.