Políticas de Seguridad

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 Crakers, 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 involucra y está pendiente de éste, tratando de contrarrestar y anular estas amenazas.

Nuestra carencia de recursos humanos involucrados en seguridad, la escasa concientización y las limitantes económicas han retrasado el plan rector de seguridad que se requiere.

El objetivo principal de la Unidad de Telecomunicaciones y Sistemas 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 debe de 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 Unidad de Telecomunicaciones y Sistemas 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 Unidad de Telecomunicaciones y Sistemas del CIMAV, ha elaborado, para normar a la institución en estos rubros.

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 Institución.

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 globalizado 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 del CIMAV 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 Unidad de Telecomunicaciones y Sistemas está conformada por 3 departamentos de servicio. Los departamentos son Desarrollo de Sistemas, Cómputo, y Redes, estos se encargan de brindar servicio directo al usuario, por el ámbito de competencia que tiene cada uno de ellos en materia de informática, desde el equipamiento, instalación, alteración, cambio de lugar, programación, etc. Por lo que ha sido necesario emitir políticas particulares para la Red-CIMAV, que es el nombre de un conjunto de recursos y facilidades informáticas, de la infraestructura de telecomunicaciones y servicios asociados a ellos, provistos por la Unidad de Telecomunicaciones y Sistemas. Así pues este apartado contiene una clasificación de estas políticas, y son:

Del equipo

De la instalación de equipo de cómputo.

1. Todo el equipo de cómputo (computadoras, estaciones de trabajo, supercomputadoras, y equipo accesorio), que esté o sea conectado a la Red-CIMAV, o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe de sujetarse a las normas y procedimientos de instalación que emite el departamento de Redes de la Unidad de Telecomunicaciones y Sistemas.
2. La Unidad de Telecomunicaciones y Sistemas en coordinación con el departamento de Control Patrimonial deberá tener un registro de todos los equipos propiedad del CIMAV.
3. El equipo de la institución que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en una área que cumpla con los requerimientos de: seguridad física, las condiciones ambientales, la alimentación eléctrica, su acceso que la Unidad de Telecomunicaciones y Sistemas tiene establecido en su normatividad de este tipo.
4. Los responsables de las áreas de apoyo interno de los departamentos deberán en conjunción con el departamento de Redes dar cabal cumplimiento con 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, Unidad de Telecomunicaciones y Sistemas, departamento de Control Patrimonial, y otros de competencia).

Del mantenimiento de equipo de cómputo.

1. Al departamento de Redes de la Unidad de Telecomunicaciones y Sistemas, 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.
2. Corresponde al departamento de Redes 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.
3. Por motivos de normatividad expedidos por la SECODAM queda estrictamente prohibido dar mantenimiento a equipo de cómputo que no es propiedad de la institución.

De la actualización del equipo.

1. Todo el equipo de cómputo (computadoras personales, estaciones de trabajo, supercomputadora y demás relacionados), y los de telecomunicaciones que sean propiedad del CIMAV 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. En caso de existir personal técnico de apoyo de los departamentos académicos, éste notificará de los cambios tanto físicos como de software de red que realice al departamento de Redes, y en su caso si cambiará de responsable (el equipo) al departamento de Control Patrimonial de la Subdirección de Recursos Materiales y Servicios. Notificando también los cambios de equipo inventariado (cambio de monitores, de impresoras etc.).
2. El equipo de cómputo a reubicar sea del CIMAV 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.

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 Unidad de Telecomunicaciones y Sistemas.
2. 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.
3. La Unidad de Telecomunicaciones y Sistemas deberá proveer de la infraestructura de seguridad requerida con base en los requerimientos específicos de cada área.
4. 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 Unidad de Telecomunicaciones y Sistemas 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 Unidad de Telecomunicaciones y Sistemas.
4. Los accesos a las áreas de críticas deberán de ser clasificados de acuerdo a las normas que dicte la Unidad de Telecomunicaciones y Sistemas de común acuerdo con su comité de Cómputo Asesor.
5. Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, la Unidad de Telecomunicaciones y Sistemas tiene la facultad de acceder a cualquier equipo de cómputo que no este bajo su supervisión.

Del control de acceso local a la red.

1. El departamento de Cómputo de la Unidad de Telecomunicaciones y Sistemas es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.
2. La Unidad de Telecomunicaciones y Sistemas es la responsable de difundir el Reglamento para el Uso de la Red y de procurar su cumplimiento.
3. Dado el carácter unipersonal del acceso a la Red-CIMAV, el departamento de Cómputo 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, etc.) conectado a la red es administrado por la Unidad de Telecomunicaciones y Sistemas.
5. Todo el equipo de cómputo que esté o sea conectado a la Red-CIMAV, 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 Unidad de Telecomunicaciones y Sistemas.

De control de acceso remoto.

1. La Unidad de Telecomunicaciones y Sistemas 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 supercómputo a terceros deberán ser autorizados por la Dirección General.
3. El usuario de estos servicios deberá sujetarse al Reglamento de uso de la Red-CIMAV 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 Unidad de Telecomunicaciones y Sistemas.

Del acceso a los sistemas administrativos.

1. Tendrá acceso a los sistemas administrativos solo el personal del CIMAV que es titular de una cuenta o bien tenga la autorización del responsable si se trata de personal de apoyo administrativo o técnico.
2. El manejo de información administrativa que se considere de uso restringido deberá ser cifrada con el objeto de garantizar su integridad.
3. Tendrá acceso al sistema de información de la División de Estudios de Posgrado sólo aquellos usuarios de Red-CIMAV o externos autorizados por dicha División.
4. La instalación y uso de los sistemas de información se rigen por el reglamento de uso de la Red-CIMAV.
5. Los servidores de bases de datos administrativos son dedicados, por lo que se prohíben los accesos de cualquiera, excepto para el personal de la Unidad de Telecomunicaciones y Sistemas.
6. 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.

1. En concordancia con la legislación federal y de común acuerdo con las políticas generales de informática, la Unidad de Telecomunicaciones y Sistemas a través del departamento de Redes es el responsable de instalar y administrar el o los servidor(es) WWW. Es decir, sólo se permiten servidores de páginas autorizados por la Unidad de Telecomunicaciones y Sistemas.
2. 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-CIMAV.
3. A los responsables de los servidores de Web corresponde la verificación de respaldo y protección adecuada.
4. Toda la programación involucrada en la tecnología Web deberá estar de acuerdo con las normas y procedimientos que la Unidad de Telecomunicaciones y Sistemas emita.
5. El material que aparezca en la página de Internet del CIMAV deberá ser aprobado por la Unidad de Telecomunicaciones y Sistemas, respetando la ley de propiedad intelectual (derechos de autor, créditos, permisos y protección, como los que se aplican a cualquier material impreso).
6. En concordancia con la libertad de investigación, se acepta que en la red del CIMAV conectada a Internet pueda ponerse información individual sin autorización (siempre y cuando no contravenga las disposiciones que se aplican a las instituciones gubernamentales paraestatales), pero deberá llevar el enunciado siguiente: "Las expresiones, opiniones o comentarios que aquí aparecen pertenecen al autor individual y no necesariamente al CIMAV"; y deberá siempre responder a un comportamiento profesional y ético.
7. 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 Unidad de Telecomunicaciones y Sistemas.
8. La Unidad de Telecomunicaciones y Sistemas tiene la facultad de llevar a cabo la revisión periódica de los accesos a nuestros servicios de información, y conservar información del tráfico.

De utilización de los recursos de la red

1. Los recursos disponibles a través de la Red-CIMAV serán de uso exclusivo para asuntos relacionados con las actividades sustantivas del centro.
2. La Unidad de Telecomunicaciones y Sistemas es la responsable de emitir y dar seguimiento al Reglamento para el uso de la Red.
3. De acuerdo con las disposiciones de la SECODAM, corresponde a la Unidad de Telecomunicaciones y Sistemas administrar, mantener y actualizar la infraestructura de la Red-CIMAV.
4. La Unidad de Telecomunicaciones y Sistemas debe propiciar el uso de las tecnologías de la información con el fin de contribuir con las directrices económicas de la institución.

Del Software

De la adquisición de software.

1. Del presupuesto de los proyectos que se otorga a las diferentes áreas del CIMAV una cantidad deberá ser aplicada para la adquisición de programas con licencia.
2. De acuerdo con el Programa Nacional de Informática, la Dirección General en conjunto con el Comité de Cómputo Asesor y la Unidad de Telecomunicaciones y Sistemas, 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.
3. Corresponderá a la Unidad de Telecomunicaciones y Sistemas emitir las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.
4. De acuerdo a los objetivos globales de la Unidad de Telecomunicaciones y Sistemas se deberá propiciar la adquisición y asesoramiento en cuanto a software de vanguardia.
5. En cuanto a la paquetería sin costo deberá respetarse la propiedad intelectual intrínseca del autor.
6. La Unidad de Telecomunicaciones y Sistemas promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.
7. La Unidad de Telecomunicaciones y Sistemas 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 Unidad de Telecomunicaciones y Sistemas 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. La Unidad de Telecomunicaciones y Sistemas es la responsable de brindar asesoría y supervisión para la instalación de software informático, asimismo el departamento de Redes para el software de telecomunicaciones.
4. La instalación de software que desde el punto de vista de la Unidad de Telecomunicaciones y Sistemas 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 a la Unidad de Telecomunicaciones y Sistemas.

De la actualización del software.

1. Corresponde a la Unidad de Telecomunicaciones y Sistemas autorizar cualquier adquisición y actualización del software.
2. Las actualizaciones del software de uso común o más generalizado se llevarán a cabo de acuerdo al plan de actualización desarrollado por la Unidad de Telecomunicaciones y Sistemas.

De la auditoria de software instalado.

1. La Unidad de Telecomunicaciones y Sistemas del CIMAV es la responsable de realizar revisiones periódicas para asegurar que sólo programación con licencia esté instalada en las computadoras de la institución.
2. La Unidad de Telecomunicaciones y Sistemas propiciará la conformación de un grupo especializado en auditoria de sistemas de cómputo y sistemas de información.
3. Corresponderá al grupo especializado dictar las normas, procedimientos y calendarios de auditoria.

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 Unidad de Telecomunicaciones y Sistemas en coordinación con el departamento de Control Patrimonial deberá tener un registro de todos los paquetes de programación propiedad del CIMAV.
3. Todos los sistemas programáticos (programas, bases de datos, sistemas operativos, interfases) desarrollados con o a través de los recursos del CIMAV 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 preservarse.
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 Unidad de Telecomunicaciones y Sistemas promover y difundir los mecanismos de respaldo y salvaguarda de los datos y de los sistemas programáticos.
7. La Unidad de Telecomunicaciones y Sistemas en conjunto con la Dirección de Vinculación propiciará la gestión de patentes y derechos de creación de software propiedad de la institución.
8. La Unidad de Telecomunicaciones y Sistemas administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política informática.

Sobre el uso de software académico.

1. Cualquier software que requiera ser instalado para trabajar sobre la Red-CIMAV deberá ser evaluado por la Unidad de Telecomunicaciones y Sistemas.
2. Todo el software propiedad de la institución deberá ser usado exclusivamente para asuntos relacionados con las actividades del Centro.

De la propiedad intelectual.

1. Corresponde a la Unidad de Telecomunicaciones y Sistemas procurar que todo el software instalado en la Red-CIMAV esté de acuerdo a la ley de propiedad intelectual a que dé lugar.

De supervisión y evaluación

1. Las auditorias de cada actividad donde se involucren aspectos de seguridad lógica y física deberán realizarse periódicamente y deberá sujetarse al calendario que establezca la Unidad de Telecomunicaciones y Sistemas 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 departamentos deberán de 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 Unidad de Telecomunicaciones y Sistemas deberá de conducirse de acuerdo a los códigos de ética profesional y normas y procedimientos establecidos.

IV. Sanciones.

1. Cualquier violación a las políticas y normas de seguridad deberá ser sancionada de acuerdo al reglamento emitido por la Unidad de Telecomunicaciones y Sistemas.
2. 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.
3. Corresponderá al Comité de Cómputo Asesor hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de la institución.
4. Todas las acciones en las que se comprometa la seguridad de la Red-CIMAV y que no estén previstas en esta política, deberán ser revisadas por la Dirección General y la Unidad de Telecomunicaciones y Sistemas para dictar una resolución sujetándose al estado de derecho.

V. Referencias

Cano, Heimy J. (1998). Pautas y Recomendaciones para Elaborar Políticas de Seguridad Informática (PSI). Universidad de los Andes, Colombia.

Organisation for Economic Cooperation and Development (OEDC) Guidelines for Security of Information Systems. 1992.

Swanson, et al. (1996) National Institute of Standard and Technology (NIST). General Principles for Information Systems Security Policies.

VI. Notas

Esta política de seguridad deberá seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, desarrollo de nuevos servicios, entre otros.

El documento que contiene la política de seguridad deber ser difundido a todo el personal involucrado en la definición de estas políticas.

VII. Glosario.

Departamento de Cómputo.

Es la entidad encargada del buen uso de las tecnologías de la computación, organización y optimización de los recursos computacionales de la institución.

Departamento de Redes.

Es la entidad encargada de desarrollar el plan estrategico de conectividad del centro (CIMAV) que favoresca la prestación de servicios eficientes, eficaces y de utilidad en la transmisión de datos, voz y video para apoyar efectivamente los requerimientos del usuario.

Departamento de Desarrollo de Sistemas.

Es la entidad encargada de ofrecer sistemas de información administrativa integral permitiendo en forma oportuna satisfacer necesidades de información, como apoyo en el desarrollo de las actividades propias del centro.

Bases de Datos.

Es un conjunto de datos interrelacionados y un conjunto de programas para accesarlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápida.

WWW (World Wide Web).

Es una convergencia de conceptos computacionales para presentar y enlazar información que se encuentra dispersa a través de Internet en una forma accesible. Sistema avanzado para navegar a través de Internet.

Area Crítica.

Es el área física donde se encuentra instalado el equipo de cómputo y telecomunicaciones que requiere de cuidados especiales y son indispensables para el funcionamiento continuo de los sistemas de comunicación del centro.

Equipo de Telecomunicaciones.

Todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.

Equipo de Cómputo.

Dispositivo con la capacidad de aceptar y procesar información en base a programas establecidos o instrucciones previas, teniendo la oportunidad de conectarse a una red de equipos o computadoras para compartir datos y recursos, entregando resultados mediante despliegues visuales, impresos o audibles.

SECODAM - Secretaria de Contraloría y Desarrollo Administrativo.

IP - Internet Protocol.

Parte de la familia de protocolos TCP/IP, que describe el software que supervisa las direcciones de nodo Internet, encamina mensajes salientes y reconoce los mensajes entrantes.

Dirección de INTERNET.

Identificador único de 32 bits para una computadora principal TCP/IP en una RED. También llamada dirección IP. Las direcciones IP están normalmente impresas en una forma decimal de puntos, tal como 148.223.46.100 **Auditoría.**

Llevar a cabo una inspección y examen independiente de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y procedimientos operativos, y para recomendar cualquier cambio que se estime necesario.

Control de Acceso.

1. Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria.
2. Una característica o técnica en un sistema de comunicaciones para permitir o negar el uso de algunos componentes o algunas de sus funciones.