UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN INGENIERÍA

FACULTAD DE INGENIERÍA

IMPLEMENTACIÓN DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE ISO-17799 PLATAFORMA BSD

T E S I S

QUE PARA OPTAR POR EL GRADO DE

MAESTRA EN INGENIERÍA ELECTRÍCA

P R E S E N T A:

JULIA JANET BERNUY SÁNCHEZ

DIRECTOR DE TESIS

DR. JULIO SOLANO GONZÁLEZ

CODIRECTOR DE TESIS

ING. RICARDO VILLARREAL MARTÍNEZ

MÉXICO. D.F. 2008

AGRADECIMIENTOS

A Dios por la vida.

A ti padre (q.e.p.d), porque siempre estas conmigo.

A mi madre y hermanos por su apoyo y comprensión.

A mi esposo por gran amor y apoyo.

Y a mi país aunque haya grandes distancias seguirán dándome fuerzas para seguir adelante.

A mis amigos por su apoyo y amistad.

Gracias

Índice

Capitulo 3: Plataforma BSD

Capitulo 4: Revisión de seguridad de la información en el IIMAS

Capitulo 5: Controles Específicos Propuestos

“La seguridad no es un producto, es un proceso”

INTRODUCCIÓN

El desarrollo de las redes, sistemas y en general cualquier tecnología de la información conlleva a una creciente preocupación por la seguridad de los mismos y en la medida que se aseguren se proporcionará protección para el buen funcionamiento de la información.

La información, hoy en día es uno de los activos más importantes para cualquier organización, requiere de sistemas que garanticen su resguardo sobre posibles amenazas para minimizar los daños que éstas puedan ocasionar a la organización, así como dar oportunidad a la continuidad de las actividades de la misma.

Como se sabe, por cualquier red circula diariamente todo tipo de datos, entre ellos muchos se podrían catalogar como confidenciales (nóminas, expedientes, presupuestos) o como privados (correo electrónico, proyectos de investigación, artículos a punto de ser publicados), etc.

A fin de lograr una mayor protección de la información surge la necesidad de definir procesos y controles para resguardarla, para lo cual existen estándares. **ISO 17799[**[1]**]** nació como respuesta a dicha necesidad, este estándar es una compilación de recomendaciones para las prácticas de seguridad que toda organización puede aplicar sin importar el tamaño de la empresa u organización. Tiene su origen en BSI [[2]] (BS7799), más adelante la ISO hace una revisión y la publica como ISO/IEC 17799:2000.[[3]]

Se considera necesario que cualquier organización mantenga los servicios, sistemas y productos de su red en óptimas condiciones, además de proteger la información siguiendo buenas prácticas y a través de estándares internacionales como ISO 17799, para esto se llevo a cabo un caso de estudio en la presente tesis dirigido al Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas (IIMAS) de la UNAM para evaluar los niveles de seguridad de su información basándose en el estándar y a través de este dar seguimiento a la confiabilidad y calidad en la seguridad de la información, de ahí que el objetivo del presente trabajo es: diseñar, desarrollar y proponer un esquema de seguridad de la información, conjuntamente con las políticas de seguridad, para así mantener la integridad, confidencialidad y disponibilidad de información que se genere en el Instituto, además de una revisión de seguridad con el fin de evaluar si cumple con las recomendaciones y mecanismos de seguridad que menciona dicho estándar.

De esta manera se contribuye a que la comunidad del IIMAS pueda contar con lineamientos y herramientas de apoyo a la seguridad de la información de los desarrollos tecnológicos, resultado de sus proyectos de investigación y en general la información de todos sus usuarios.

El contenido del presente trabajo de tesis se describe a continuación. En el **capítulo 1**, se definen conceptos como integridad, disponibilidad y confidencialidad, riesgos, amenazas, vulnerabilidad y otros términos relacionados con la seguridad de la

información, de igual forma se describen otros estándares internacionales relacionados con el manejo de la información como ITIL*, CoBIT* y NIST*.

Como referencia del capítulo anterior sobre diversos estándares, en el **capítulo 2**, se describe la historia y desarrollo del ISO 17799, su origen en BSI, la evolución, revisión y actualización con la ISO, beneficios del estándar, los pasos necesarios para obtener la certificación mediante la implementación del ISMS[4], así también de la familia de estándares internacionales ISO 27000.

A partir de los lineamientos del estándar se debe determinar el valor de la información manejada en la organización y su sensibilidad, es decir, identificar qué tan importante es la información que se maneja, bien por procesos de la organización o por necesidad de compartir datos; luego identificar las amenazas en las aplicaciones y, lo más importante será tratar de cuantificar los daños que pueden causar en caso de que las amenazas ocurran, para todo esto se realizó un análisis de riesgos en el **capítulo 3**, y una Revisión de la Administración de la Seguridad de la Información (véase Apéndice A)de los 11 dominios que se encuentran definidos en el ISO 17799.

El estándar en relación a la tecnología describe que aspectos se deben tomar en cuenta pero no sobre qué producto o plataforma se debe utilizar. En el **capítulo 4** se explica y describe sobre la tecnología BSD y en específico el sistema operativo OpenBSD el porqué se considera un sistema robusto respecto a la seguridad, sus características y fortalezas que apoyaron al desarrollo del control *seguridad en los servicios de red* del siguiente capítulo.

Una vez definido la plataforma y conceptos respecto a las tecnologías que se utilizaron, se desarrollaron dos controles específicos de los 133 que precisa el ISO: *Documento de Política de seguridad de la información y Seguridad en los servicios de red* en el **capítulo 5**. Del primer control se diseñó y propuso un documento con las Políticas Generales de la Información (véase Apéndice B) a partir del análisis de riesgos como parte de la gestión de seguridad en el Instituto. A su vez se analizó la infraestructura de red y se propuso un esquema de seguridad con elementos como un firewall, Proxy, IDS, etc. como parte del segundo control.

Al final del presente caso de estudio se concluyó acerca de la revisión de la gestión seguridad de la información en el Instituto a partir del análisis de riesgos, el cumplimiento de los dos controles desarrollados, además de las ventajas y desventajas del estándar.

Las contribuciones más importantes de este trabajo fueron la revisión de los procesos y actividades que realiza el Instituto a través de un análisis de riesgos, se identificó los recursos, así como amenazas y debilidades las cuales servirán como punto de partida para la elaboración de Políticas Generales de Seguridad de la Información (véase Apéndice B) además se planteó un esquema de seguridad de la red (véase Capítulo 5) que apoyaron la implementación de seguridad siguiendo el estándar internacional ISO 17799. Cabe señalar que el presente trabajo de tesis es una propuesta de la gestión de seguridad de la información en el Instituto y no un proyecto del mismo.

[1] ISO 17799 Código de buenas prácticas en Gestión de la Seguridad de la Información. .
[2] BSI (British Standards Institution) Instituto Nacional de Normas del Reino Unido.
http ://www.bsiamericas.com
IEC (International Electrotechnical Commission) Comisión Electrotécnica Internacional.
[3] ISO (International Organization for Standardization) Organización Internacional para la Estandarización
IEC (International Electrotechnical Commission) Comisión Electrotécnica Internacional.
[4] ISMS (Information Security Management System)
* ITIL (**I**nformation **T**echnology **I**nfraestructure **L**ibrary)
*COBIT (**C**ontrol **Ob**jectives for **I**nformation and Related **T**echnology).
*NIST (**N**ational **I**nstitute of **S**tandards and **T**echnology).

CAPÍTULO 1

ANTECEDENTES

1.1 Introducción.

El crecimiento actual en las tecnologías de la información está ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en formas no imaginadas, creando amenazas informáticas que implican un incremento en el riesgo de la información de las organización y que se puede traducir en pérdidas económicas.

El tema de la seguridad de la información comprende a las organizaciones de todos los tamaños y/o sectores con un problema común, su vulnerabilidad, toda la información en todas las áreas, ya sea almacenado electrónicamente, transmitida por correo, presentada en imágenes o expuestas en una conversación están en riesgo de una cantidad de amenazas. La seguridad de la información ya no es simplemente un asunto para administradores de tecnologías de la información (IT), una simple violación de seguridad, podría costar pérdidas económicas y daños irreparables a la imagen y reputación de la organización. Para llevar a cabo una gestión de seguridad de la información se debe establecer un programa a través de un estándar que puede ser conceptualizado como la definición clara de un modelo, criterio, regla de medida o de los requisitos mínimos aceptables para la operación de procesos específicos. Un Sistema de Administración de Seguridad de la Información basado en ISO 17799 proveerá un programa de trabajo para iniciar, implementar, mantener y administrar la seguridad de la información dentro de cualquier organización.[1]

1.2 Seguridad de la Información.

Para definir la **Seguridad de la Información** es necesario precisar los tipos de información que maneja una organización. En la actualidad las organizaciones se enfrentan cada vez con más riesgos procedentes de una amplia variedad de fuentes que pueden impactar a sus sistemas de información, poniendo en peligro la continuidad de éstas.[2]

De acuerdo a lo anterior, la Seguridad de la Información es un conjunto de medidas técnicas, organizativas y legales, que permiten a una organización preservar la confidencialidad, integridad y disponibilidad de la información. Estos tres conceptos se definen como:

La **integridad** de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal o procesos autorizados, dicha modificación debe ser registrada para controles o revisiones posteriores.[*]

Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que acceden de forma no autorizada al sistema.

La **disponibilidad**es la capacidad que tiene la información de estar siempre utilizable para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria. [*]

La **confidencialidad** de la información se refiere a que el contenido de un documento o mensaje sólo debe ser conocido y/ leído por las personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño (por ejemplo: los planes de desarrollo de un producto que se "filtran" a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes). [*]

El **control** sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma. [*]

La **autenticidad** permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad permite asegurar el origen de la información, validando el emisor de la misma, el receptor o ambos inclusive, para evitar suplantación de identidades. [*]

Adicionalmente pueden considerarse otros aspectos, relacionados con los anteriores conceptos, pero que incorporan algunos aspectos particulares:

- **Protección a la Réplica**: mediante la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario.
- **No repudio**: se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.
- **Consistencia**: poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.
- **Aislamiento**: este aspecto, íntimamente relacionado con la confidencialidad, permite regular el acceso a la información, impidiendo que personas no autorizadas hagan uso del mismo.
- **Auditoría**: es la capacidad de determinar qué acciones o procesos se están llevando a cabo con la información, así como quién y cuándo las realiza.

1.3 Amenazas para la seguridad de la Información.

Una amenaza tiene el potencial de causar un incidente no deseado, el cual puede generar daño al sistema, la organización y a los activos.

Las amenazas pueden ser analizadas en tres momentos: antes del ataque, durante y después del mismo, existen diversos tipos de amenazas como las naturales, humanas y que a su vez generan otras, como se muestra en la figura 1.1.

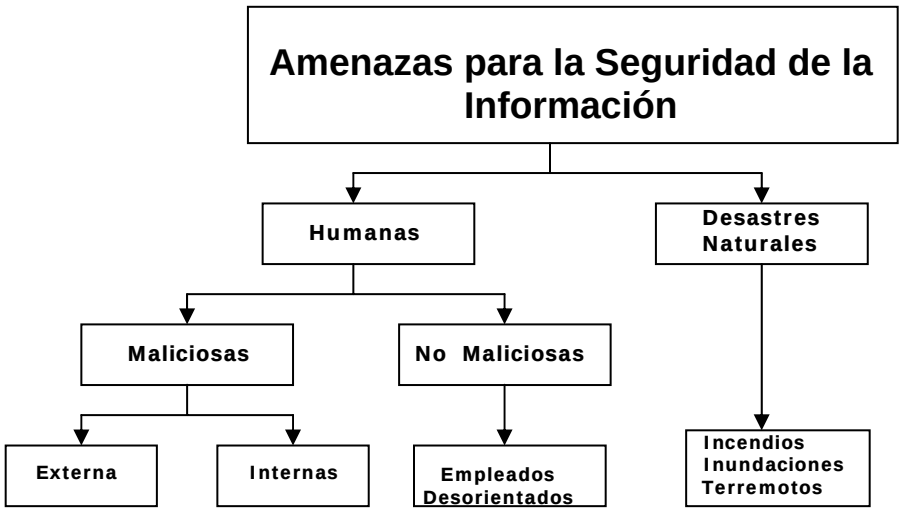

Figura 1.1. Amenazas para la seguridad de la Información.

Los mecanismos que conforman políticas para garantizar la seguridad de los sistemas de información son:

a) La prevención (antes): mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión previene la divulgación no autorizada.
b) La detección (durante): mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de monitoreo.
c) La recuperación (después): mecanismos que se aplican, cuando la violación al sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo recuperación desde las copias de seguridad (backup) realizadas.

1.4 Análisis de riesgos.

Cualquier organización está expuesta a eventos que impacten de manera negativa su funcionamiento. La incertidumbre de no conocer o entender dichos eventos lleva a la organización a la exposición de riesgos y amenazas, por lo cuál se requiere administrar esa incertidumbre y que no es una tarea fácil de realizar debido entre otras cosas a los recursos limitados, los cambios que realizan la organización, etc. Se pueden presentar un amplio panorama de riesgos y vulnerabilidades difíciles de controlar. Para esto existen herramientas y metodologías que apoyan a entender y minimizar estas amenazas y el impacto que puede tener en la organización.[3]

1.4.1 Riesgo.

El riesgo se puede definir como la combinación de la probabilidad de un suceso y sus consecuencias (Guía ISO/CEI 73). En cualquier tipo de organización existe un potencial de sucesos y consecuencias que constituyen oportunidades para conseguir beneficios (lado positivo) o amenazas (lado negativo). Los riesgos a los que afronta una organización pueden resultar de factores tanto internos como externos.

La Organización Internacional por la Normalización (ISO) define riesgo tecnológico (Guías para la gestión de la seguridad de TI /TEC TR 13335-1, 1996) como:

"*La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos, generándole perdidas o daños*".

1.4.2 Amenaza.

Una amenaza tiene el potencial de causar un evento no deseado, el cual puede generar daño a los sistemas de información, la organización y a los activos. El daño puede ocurrir por un ataque directo o indirecto a la información, pueden originarse de fuentes accidentales o de manera deliberada. Comúnmente se consideran como amenazas a las fallas, a los ingresos no autorizados, a los virus, uso inadecuado de software, los desastres ambientales como terremotos o inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones, etc. Las amenazas pueden ser de carácter físico o lógico, como una inundación en el primer caso, o un acceso no autorizado a una base de datos en el segundo caso.
Por medio de una "lluvia de ideas" se pueden detectar las amenazas accidentales o deliberadas y estimar su posibilidad de ocurrencia.[4]

Las amenazas que puede afectar a la seguridad se pueden clasificar en tres categorías:

- Naturales.
- Accidentales y
- Deliberadas.

1.4.2.1 Amenazas Naturales.

Las amenazas naturales, incluyen principalmente, cambios naturales, que pueden afectar el desempeño y funcionamiento de los sistemas de información que se manejan en la organización.

1.4.2.2 Amenazas Accidentales.

Las amenazas catalogadas dentro de las accidentales son las más comunes:

a) Si un usuario teclea su login y una contraseña incorrecta, no debería tener acceso al sistema, se determina como ERROR DE USUARIO.
b) Si un administrador tiene su sesión abierta y olvidó salir del sistema, cualquier otro usuario con acceso físico a la máquina podría hacer modificaciones causando entonces ERRORES DE LOS ADMINISTRADORES.
c) EN LAS INSTALACIONES Y CONFIGURACIONES: Si el administrador modifica los archivos de inicialización de ciertos servicios y no activo los mecanismos de seguridad debidos, lo que resultó finalmente es un servicio sin seguridad; o bien, denominado ERROR ADMINISTRATIVO.

d) Si hay una transferencia cuyos datos deberían estar encriptados y no lo están causará DATOS MAL PREPARADOS.
e) Si las impresoras están mal direccionadas y un documento confidencial fue enviado por error a una impresora que no debería, causará ERRORES DE SALIDA.
f) Si el sistema de archivos se daño y una contraseña fue borrada o cambiada por otra causará ERRORES EN EL SISTEMA.
g) ERRORES EN LAS COMUNICACIONES que fácilmente podría violar la confidencialidad de los datos, si se presentará un problema electromagnético.
h) Mal uso de medios móviles como discos compactos, puede causar ERROR DE USO.

1.4.2.3 Amenazas Deliberadas.

Las amenazas deliberadas tanto activas como pasivas son peligrosas para toda la organización. Las activas incluyen accesos no autorizados, modificaciones no autorizadas, sabotaje, etc. las cuales siempre o casi siempre involucran un "cracker".

Las amenazas pasivas son de naturaleza mucho más técnica y dentro de estas encontramos; problemas electromagnéticos que pueden dañar la información sobre la red, ruptura del cableado e información mal protegida o disponible sin ningún tipo de control (por olvido, error, etc.). Véase tabla 1.2.

ELEMENTO DE RED	AMENAZA
Sistema Operativo de red	Acceso no autorizado. Modificación no autorizada. Negación de un servicio. Robo de información. Instalación de programas peligrosos.
Switches Access Point Ruteadores	Acceso no autorizado. Modificaciones de la configuración que causan negación de servicios y/o acceso a recursos.
Servidores Estaciones de trabajo	Acceso físico a los servidores sin autorización. Robo o destrucción de información. Acceso no autorizado y modificación

Tabla 1.1 Amenazas pasivas

1.4.3 Vulnerabilidades.

Las vulnerabilidades son ciertas condiciones que se presentan en los entornos de los activos y que facilitan que las amenazas se materialicen y conduzcan a esos activos a ser vulnerables. Mediante el uso de las debilidades o defectos existentes es que las amenazas logran materializarse, o sea, las amenazas siempre están presentes, pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto.
Estas vulnerabilidades son de naturaleza variada. Por ejemplo: falta de conocimiento del usuario, uso de tecnología no revisada, inadecuada transmisión por redes públicas, etc.

Una vulnerabilidad común es contar con antivirus no actualizado, la cual permitirá al virus actuar y ocasionar daños. Si el antivirus estuviese actualizado la amenaza (virus) si bien potencialmente seguiría existiendo no podría materializarse.

Definir específicamente cuál es la vulnerabilidad a las amenazas identificadas y el grado de riesgo, se controlará planteando soluciones mediante mecanismos de seguridad y/o medidas para contrarrestar las fallas que implican enormes riesgos, todo esto para evitar la ejecución de las principales amenazas dados los riesgos.

1.4.4 Probabilidad.

Establecer la probabilidad de ocurrencia puede realizarse de manera cuantitativa o cualitativa, pero siempre considerando que la medida no debe contemplar la existencia de ninguna acción ligera, o sea, debe considerarse en cada caso qué posibilidades existen de que la amenaza se presente independientemente del hecho que sea o no contrarrestada.
Existen amenazas, como por ejemplo incendios, para las cuales hay información suficiente (manuales, capacitación, compañías de seguros y otros datos) para establecer con objetividad su probabilidad de ocurrencia. Otras amenazas presentan mayor dificultad en establecer cuantitativamente la probabilidad. Por ejemplo, el acceso no autorizado a datos; donde se hacen estimaciones sobre la base de experiencias.

1.4.5 Impacto.

El impacto son las consecuencias de la ocurrencia de las distintas amenazas y que son siempre negativas. Las pérdidas generadas pueden ser financieras, no financieras, de corto plazo o de largo plazo. Se puede establecer que las más comunes son: la pérdida de dinero, la pérdida de confianza, la reducción de la eficiencia y la pérdida de oportunidades de negocio, entre otras.

1.5 Estándares relacionados con seguridad.

Además del ISO 17799 (véase Capítulo 2), existen otros estándares internacionales aplicables a la seguridad de la información y que se describen brevemente a continuación:

1.5.1 ITIL (Information Technology Infraestructure Library).

ITIL es un estándar que proporciona una guía en la parte administración de servicios de TI (Tecnologías de la Información). Desarrollado en la década de los 80’s, actualmente se ha actualizado con prácticas modernas para la administración de Tecnologías de Información. [5]

Tiene un marco de referencia aceptado a nivel mundial, además proporciona un conjunto de prácticas hechas por la OGC (Office Government Commerce) del Gobierno Británico, se puede aplicar a todo tipo de organizaciones independientemente de su tamaño o su tecnología, debido a que se ha desarrollado tomando en cuenta que estas organizaciones son dependientes de las tecnologías de la información. Por lo cual necesitan cumplir ciertos lineamientos para lograr sus objetivos.

1.5.1.1. Marco de referencia de ITIL.

La figura 1.2, muestra el esquema diseñado por la OGC se observa la relación de cada módulo con el negocio y la tecnología. Los módulos de la perspectiva del negocio se alinean más cerca con el negocio, así como el módulo de la administración de la infraestructura con la tecnología. La prestación de servicios de las TI y el soporte a los servicios de las TI son la parte principal del esquema.

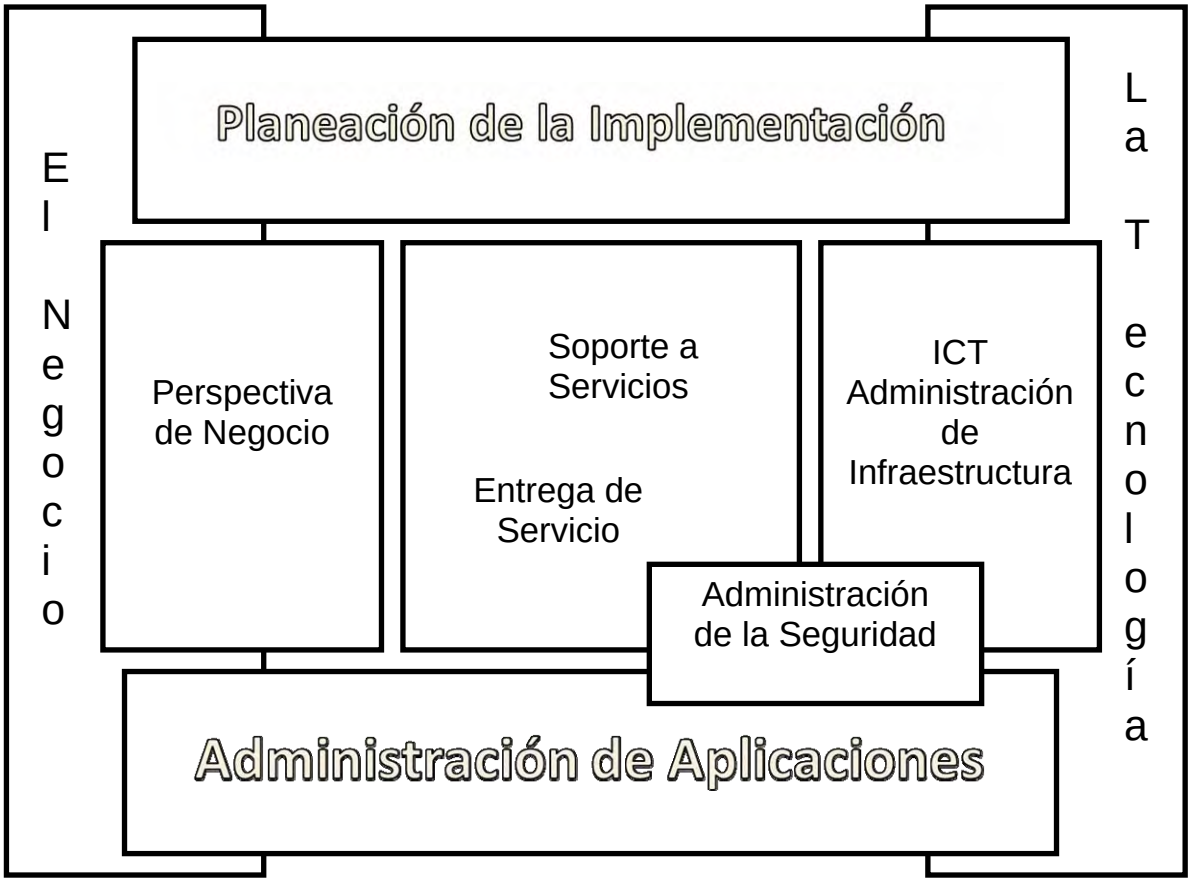

Figura 1.2 ITIL Framework

Estos módulos constituyen la base de ITIL. En la versión 3 ha mejorado la estructura y un nuevo alcance, el contenido y sus relaciones entre ellos, a continuación se describen brevemente:

Entrega de servicios (Service Delivery): cubre los procesos requeridos para la planeación y entrega de servicios de TI de calidad, además, visualiza los procesos de largo plazo asociado con mejorar la calidad en los servicios entregados. Lo compone: la administración de los niveles de servicio, la administración financiera de los servicios de las TI, administración de la continuidad de los servicios de las TI y administración de la disponibilidad.

Soporte de servicios (Service Support): describe los procesos asociados y necesarios para cumplir con los objetivos, continuidad y calidad de los servicios de tecnologías de información.

Administración de Infraestructura (ICTIM: Information Communication Technology-Infraestructure Management): cubre todos los aspectos de la administración de la infraestructura de las ICT, identifica los requerimientos del negocio, análisis de los procesos, prueba, instalación, desarrollo, operación y la optimización en curso de los componentes del ICT y servicios IT.

Planeación de la implementación (Planning to implement Service Management): Provee los elementos a considerar para planear la administración de los servicios de las ICT. Examina y detalla los requerimientos dependiendo de las necesidades de la organización o del negocio en aspectos de TI para cumplir sus objetivos.

Administración de Aplicaciones (Application Management): describe cómo administrar las aplicaciones de negocios, desde la identificación de necesidades, planeación y desarrollo, mejorando así los procesos de la administración del servicio dentro de una organización.

Perspectivas de negocios (The Business Perspective): propone sugerencias y una guía a la gerencia para entender cómo pueden contribuir en el diseño, arquitectura y elementos esenciales para definir la infraestructura de Tecnologías de Información de negocio.

Administración de la seguridad (Security Management): detalla el proceso de planeación y administración a un nivel definido de seguridad identificado en los acuerdos de niveles de servicio de las TI, incluyendo todos los aspectos asociados con incidentes de la seguridad. También incluye una evaluación, administración de riesgos y vulnerabilidades además de la implementación de medidas necesarias.

1.5.2. CObIT (**C**ontrol **Ob**jectives for **I**nformation and related **T**echnology).

CObIT (Objetivos de control de información y Tecnologías relacionadas), es un modelo desarrollado por la Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI). Desde sus inicios en 1996 CObIT determina, con el respaldo de las principales normas técnicas internacionales, un conjunto de mejores prácticas para la seguridad, la calidad, la eficacia y la eficiencia en TI que son necesarias para alinearse con el negocio, identificar riesgos, entregar valor al negocio, gestionar recursos y medir el desempeño, el cumplimiento de metas y el nivel de madurez de los procesos de la organización.[6]

La orientación a negocios es el tema principal de CObIT. Está diseñado no sólo para ser utilizado por usuarios y auditores, también para los propietarios de los procesos de negocio a través de una lista de verificación detallada. En forma incremental, las prácticas de negocio requieren de una mayor delegación y otorgamiento de autoridad de los dueños de procesos para que estos posean total responsabilidad de todos los aspectos relacionados con dichos procesos de negocio. Esto incluye proporcionar controles adecuados. El Marco

Referencial de CObIT proporciona herramientas al propietario de procesos de negocio que le facilitan el cumplimiento de esta responsabilidad.

CobIT, es un conjunto de 34 Objetivos de Control de alto nivel, uno para cada proceso de TI, agrupados en cuatro dominios: planeación y organización, adquisición e implementación, entrega (de servicio) y monitoreo[5].

Esta estructura cubre todos los aspectos de información y de la tecnología que la soporta; dirigiendo estos 34 Objetivos de Control de alto nivel, el propietario de proceso de negocio podrá asegurar que se proporciona un sistema de control adecuado para el ambiente de tecnología de información. Adicionalmente, correspondiendo a cada uno de los 34 objetivos de control de alto nivel, existe una guía de auditoría o de aseguramiento que permite la revisión de los procesos de TI contra los 302 objetivos detallados de control recomendados por CObIT para proporcionar a la gerencia la certeza de su cumplimiento y/o una recomendación para su mejora. CObIT contiene un conjunto de herramientas de implementación que proporciona lecciones aprendidas por empresas que rápida y exitosamente aplicaron CObIT en sus ambientes de trabajo.

En la Figura 1.3 se muestra el Marco Referencial CObIT que otorga especial importancia al impacto sobre los recursos de TI, así como a los requerimientos de negocios en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad que deben ser satisfechos. Además, proporciona definiciones para los requerimientos de negocio que son derivados de objetivos de control superiores en lo referente a calidad, seguridad y reportes en tanto se relacionen con Tecnología de Información.

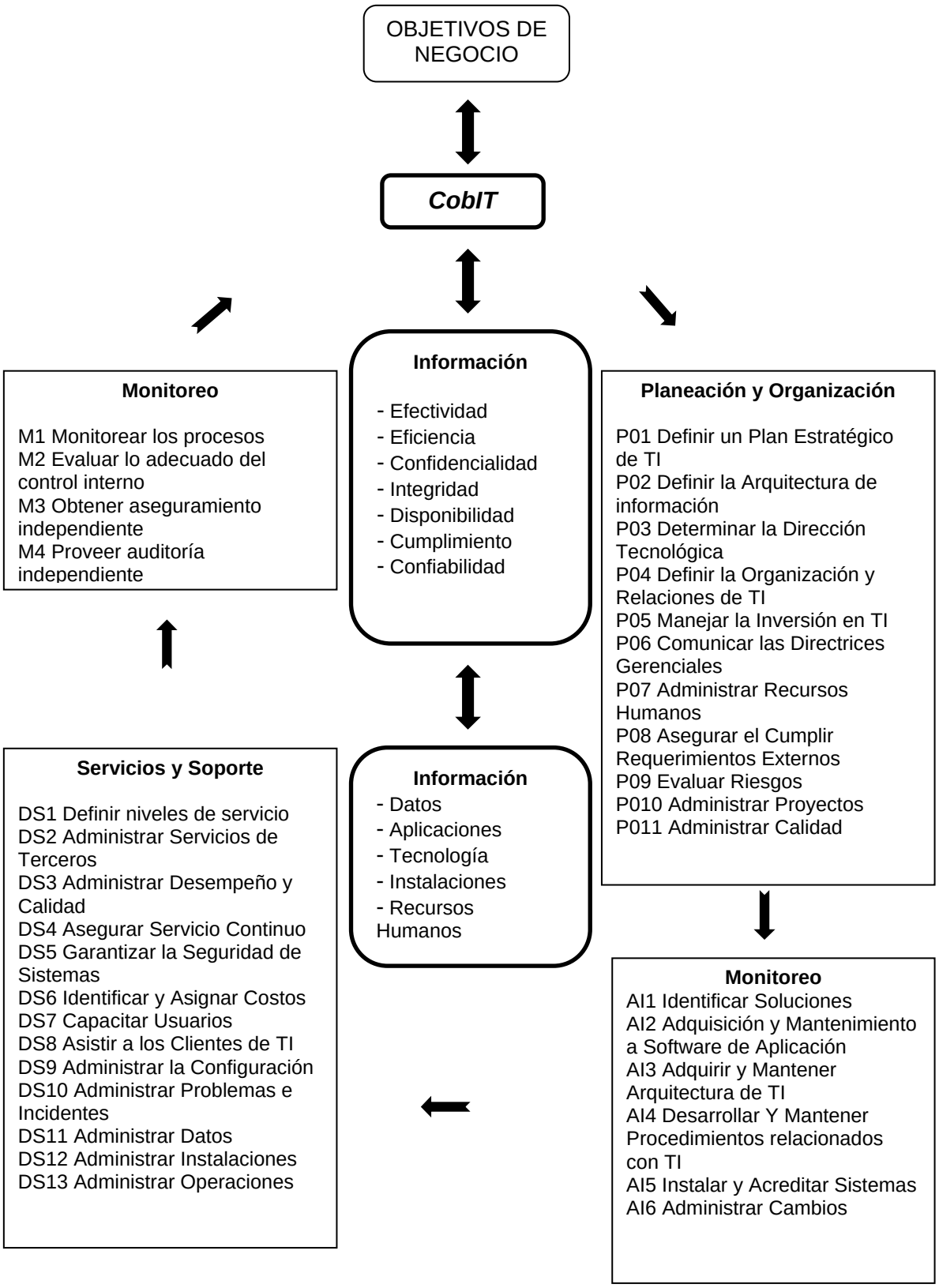

Figura 1.3 CoBIT

1.5.3 NIST Serie 800 (National Institute of Standards and Technology).

El Instituto Nacional de Estándares y Tecnología, es un organismo federal no regulador que forma parte de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos.[7]

La misión del NIST consiste en elaborar y promover patrones de medición, normas y tecnología con el fin de realzar la productividad, facilitar el comercio y mejorar la calidad de vida.

NIST viene editando, a lo largo de los últimos años, manuales dedicados a diferentes aspectos de la seguridad, estos documentos se engloban dentro de la Serie 800 de los publicados por esta Organización y agencias gubernamentales disponibles para su descarga. Estas guías y directrices son documentos muy elaborados y de reconocido prestigio, que cubren múltiples aspectos relacionados con la seguridad de la información y que pueden servir de apoyo a la hora de desarrollar políticas, procedimientos y controles. A continuación (véase tabla 1.2) se mencionan algunas de las publicaciones que ha realizado el NIST en relación a diversos temas relacionados con la seguridad de la información:

Serie	Descripción
SP 800-53	Controles recomendados de la seguridad para los sistemas de información federales.
SP 800-53A	Guía para determinar los controles de la seguridad en sistemas de información federales

Serie	Descripción
SP 800-86	Guía con técnicas forenses para incidentes de seguridad
SP 800-83	Guía para la prevención de incidentes de Malware
SP 800-81	Guía para seguridad en un servidor de nombres (DNS).

Serie	Descripción
SP 800-95	Guía de los servicios seguros en el WEB
SP 800-94	Guía de detección de intrusos y sistemas de prevención
SP 800-92	Guía para administración de la seguridad (registros)

Serie	Descripción
SP 800-98	Publicación especial 800-98, dirección del bosquejo para asegurar sistemas de la identificación de la radiofrecuencia (RFID).
SP 800-97	Publicación especial 800-97, guía del bosquejo a IEEE 802.11i: Redes robustas de la seguridad
SP 800-96	Pautas de la interoperabilidad de las tarjetas lectoras.

Serie	Descripción
SP 800-103	Publicación especial 800-103 del bosquejo de las credenciales de la identidad, parte I: Fondo y formulación.
SP 800-101	Publicación especial 800-101, pautas del bosquejo en el “Cell Phone Forensics”.
SP 800-100	Manual de la seguridad de la información: Una guía para los administradores.

Tabla 1.2 NIST Serie 800

1.6 Conclusiones.

Con lo anteriormente expuesto, se deduce la importancia del tema de seguridad de la información para cualquier organización, conocer y comprender los conceptos básicos: confidencialidad, disponibilidad y confiabilidad y si cualquiera de ellos se ve afectada podrá causar eventos que puedan dañar a la organización.

Además de las posibles amenazas sean naturales, accidentales o provocados que pueden dañar la información; identificar riesgos, vulnerabilidades y el impacto que pueden causar en caso de que se produzcan, es por esto que se mencionan los mecanismos para garantizar su seguridad.

Se concluye con la descripción de otros estándares internacionales relacionados con la seguridad de la información como: CoBIT, ITIL, NIST 800, algunos relacionados con la tecnología de la información y guías para evaluar la seguridad en una organización.

En el siguiente capítulo se define el estándar ISO 17799, se describe los dominios y controles y qué se debe desarrollar para obtener una certificación internacional.

[1] Draft BS 7799-2:2005 (ISO/IEC FDIS 27001:2005) Information Technology. Security Techniques. Information Security Management Systems.

[2] ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. Argentina. 1997.

[*] Security in Computing, Charles P Fleeger, Hardcover Edition Prentice Hall, 2002

[3] Practical UNIX and Internet Security, Second Edition, Simson Garfinkel, Gene Spafford, Second Edition April 1996, USA, O’Really, 2003.

[4] Peltier, Thomas R., Information Security Risk Analysis, Aurebach Publications, 2001

[5] OGC ITIL. (2002) "Best Practice for Security Management" (2da. edición) Londres, Inglaterra: TSO (The Stationery Office).

[6] http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/

[7] http://csrc.nist.gov/publications/PubsSPs.html

CAPÍTULO 2

ISO 17799: 2005 / 27000

2.1 Introducción.

La **información** es un activo vital para la continuidad y desarrollo de cualquier organización pero el funcionamiento de controles y procedimientos de seguridad se realiza frecuentemente sin un criterio común establecido, en torno a la compra de productos técnicos y sin considerar toda la información esencial que se debe proteger. Gastos extraordinarios, juicios legales por incumplimiento de obligaciones contractuales o responsabilidades individuales, incluido el cese de las actividades, son algunas de las consecuencias más extremas.

La Organización Internacional de Estandarización (ISO)[i], a través de las normas recogidas en ISO/IEC 17799, establece una implementación efectiva de la seguridad de la información organizacional.

Este capítulo describe el estándar internacional ISO 17799, su evolución a la nueva familia de estándares 27000 y específicamente la norma 27001, además de su importancia para cualquier organización que desee planear e implementar una gestión de seguridad de la información orientada a una futura certificación dentro de estos estándares.

Un estándar es una publicación que reúne el trabajo realizado por comités de usuarios, organizaciones, áreas de gobiernos y consumidores, que contiene especificaciones técnicas y mejores prácticas basadas en la experiencia, con el objetivo de ser utilizada como guía o definición para ciertas necesidades por la sociedad o la tecnología.

Actualmente en México el tema de la certificación en aspectos de seguridad de la información no se le ha dado la debida atención, tal vez porque todavía no se toma con la seriedad que se merece. Pero es importante mencionar que si las organizaciones desean interrelacionar sistemas, clientes, productos, etc. y quieren competir en el mercado deberá ser obligatorio obtener una certificación.

2.2 Historia.

British Standard Institution [ii] (BSI) es una organización que desde hace más de cien años ha realizado estudios con la finalidad de establecer normas y estándares de alta calidad.

La norma BS7799 fue desarrollada a principios del año 1995 como respuesta a las peticiones de la industria y gobierno para crear una estructura común de seguridad de la información, el objetivo era preparar a cualquier organización sobre la gestión de la seguridad.[**]

El estándar BS 7799 Parte 1 es oficialmente publicada y la Parte 2 en 1998. La primera parte de la norma (BS7799-1) es una guía de buenas prácticas, sin ser un modelo a seguir para certificarse. La segunda parte (BS7799-2) con la que se audita y certifica a aquellas organizaciones que desarrollen un SGSI (Sistema de Gestión de Seguridad de

la Información) según un modelo conocido como PDCA (Plan-Do-Check-Act) que se definirá más adelante en está investigación.

La Organización Internacional para la Estandarización (ISO) comienza a interesarse en los trabajos publicados por el Instituto inglés. El estándar Internacional ISO/IEC [iii] adoptó el BS7799 bajo la supervisión del grupo de trabajo "Tecnologías de la información", del Comité Técnico de la unión de la ISO/IEC.

En diciembre del 2000, la ISO incorpora la primera parte de la norma BS 7799, denominada como ISO/IEC 17799:2000. En septiembre del 2002, realiza una revisión de la segunda parte de la norma BS 7799 con el fin de enlazarla con otras normas de gestión tales como ISO 9001:2006[iv] e ISO 14001: 1996[v], así como con los principios de la Organización de Cooperación y de Desarrollos Económicos (OCDE).

La norma ISO/IEC 17799 es redactada y publicada en dos partes:

1) ISO / IEC 17799 Parte 1: Es una guía de recomendaciones de buenas prácticas para la gestión de la seguridad de la información. Contiene consejos y recomendaciones que permite garantizar la seguridad de la información de la organización, además cubre otras áreas y funciones que puedan afectar dicha información.
2) BS 17799 Parte 2: Contiene la guía relativa para la implementación de un sistema de gestión de la seguridad de la Información que propone recomendaciones con el fin de establecer un marco para la gestión de la información denominada Information Security Management System (ISMS). Es el documento que sirve de guía de evaluación para la certificación

En resumen y para entender este punto hay que tener presente que la ISO 17799 deriva de la norma británica BS 7799 y de hecho es prácticamente igual a la primera parte de la misma. La norma británica tiene dos partes y justamente en la segunda parte (BS-7799-2) se contempla la Implementación de un Sistema de gestión de seguridad. Recientemente (octubre del 2005) se liberó la ISO 27001 en base a la BS 7799-2. En consecuencia, todas las consideraciones referidas a la BS 7799-2 se aplican ahora a la ISO 27001 (véase figura 2.1.).

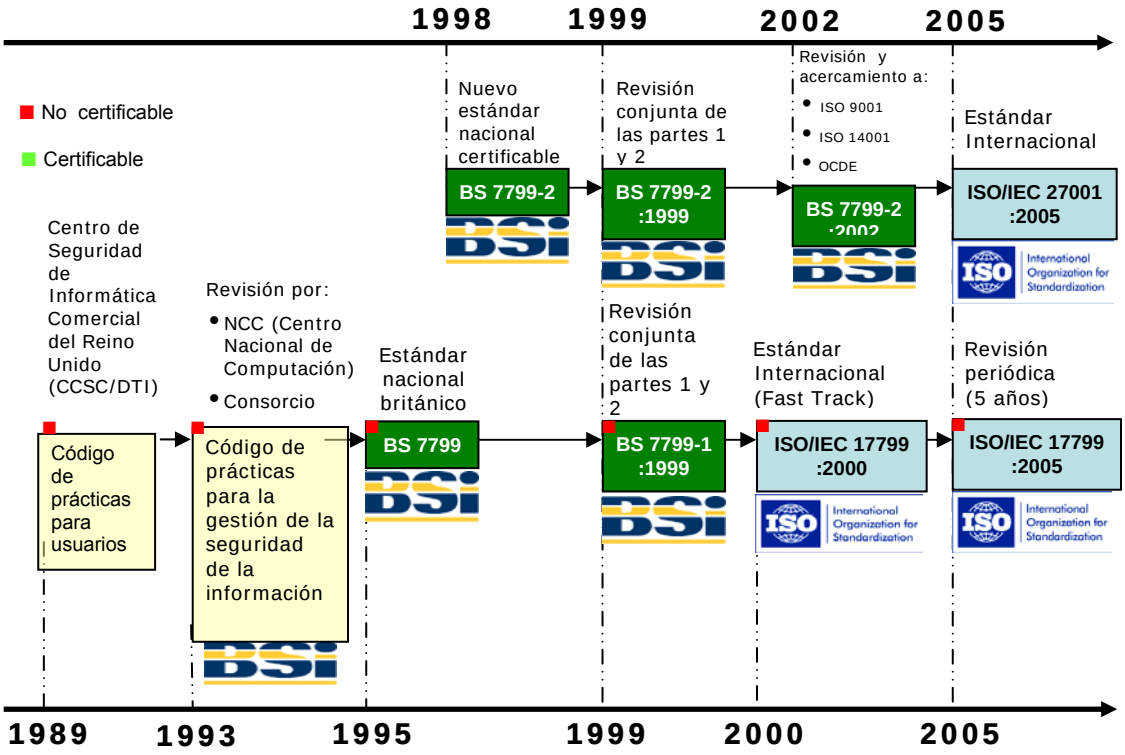

Figura 2.1. Historia y desarrollo del estándar.

2.3 Familia ISO 27000.

Actualmente el ISO/IEC JTC/SC27 está desarrollando una familia de Estándares Internacionales para Sistemas de Gestión de la Seguridad de la Información, que incluye requerimientos, gestión del riesgo, guías de métodos y/o medidas, vocabulario y mejoras continuas. La serie de estándares 27000 ha sido reservada específicamente por la ISO para las materias de seguridad de la información. Esto por supuesto, alinea con un número de otros estándares, incluyendo ISO 9000 e ISO 14001.

Entre el conjunto de estándares que se encuentran en la familia 27000 son:

- **ISO 27000**: Definiciones y vocabulario que se emplean en todas las series 27000.
- **ISO 27001**: Estándar principal para la especificación de un Security System Management System (ISMS) y substituye al BS7799-2[*]
- **ISO 27002**: Este es el nuevo estándar del existente ISO 17799:2005.[vi]
- **ISO 27003**: Este estándar será una guía para la aplicación de un ISMS e información acerca del uso del modelo PDCA. Probable publicación para el 2008.[*]
- **ISO 27004**: Estándar que especificará las técnicas para determinar la eficiencia y efectividad en el funcionamiento de un SGSI. Probablemente se publicará en el 2008.[*]
- **ISO 27005**: Estándar que surge para la gestión de los riesgos de la seguridad de la información. Será publicado a inicios del 2008.[*]
- **ISO 27006**: Publicada en el 2007, su función será especificar el proceso de acreditación de entidades de certificación.[*]

2.4 Diferencias BS7799 / ISO 17799.

BS7799	ISO 17799
Fue desarrollado en el Reino Unido por British Standards	Fue desarrollado por varias organizaciones Internacionales, entre ellas la Comisión Electrotécnica Internacional (International Electrotechnical Commission IEC).
Es conocido como BS7799:2000 dividido en dos partes: BS7799-1:2000 BS7799-2:2002	ISO 17799:2000 → ISO 17799:2005
La parte de certificación está en la BS7799-2	Se encuentra dentro de la familia de estándares 27000 ISO 17799:2005 -→ ISO 27002[vii] ISO 27001 es equivalente al BS7799-2

Figura 2.2: BS7799 – ISO 17799

La figura 2.2 muestra un cuadro comparativo entre BS 7799 respecto a ISO 17799.

ISO 17799: Son ***recomendaciones*** sobre el uso de 133 controles específicos de seguridad según 11 dominios. No establece requisitos que al cumplirse pudieran certificarse.
Las 11 áreas o dominios son:

1. **Política de seguridad** - Proporciona a la alta dirección el apoyo para la seguridad de la información.
2. **Organización de la Seguridad de la Información** - Apoya a administrar la seguridad de la información dentro de la organización.
3. **Gestión de activos** – Ayuda en la identificación y protección de activos.
4. **Seguridad en recursos humanos** - para reducir los riesgos de error humano, robo, fraude o mal uso de las instalaciones y equipo.
5. **Seguridad física y ambiental** - para prevenir accesos no autorizados, daños e interferencia a las instalaciones de la organización y a la información.
6. **Gestión de comunicaciones y operaciones** - para asegurar la operación correcta y segura de las instalaciones de procesamiento de la información.
7. **Control de accesos** - para controlar el acceso a la información.
8. **Adquisición, desarrollo y mantenimiento de sistemas** - para asegurar que se introduzca la seguridad a los sistemas de información.
9. **Gestión de incidentes de seguridad de la información** – asegurar acontecimientos y debilidades de la seguridad de la información de la organización.
10. **Gestión de continuidad del negocio** - para contrarrestar las interrupciones a las actividades y proteger procesos críticos contra los efectos causados por fallas mayores o desastres.
11. **Conformidad** - para evitar infracciones a las leyes criminales y civiles, obligaciones contractuales, y cualquier otro requisito de seguridad.

En la figura 2.3. se muestran los once dominios que cubre la ISO 17799, además de que cada una es independiente y estructurado alrededor de aspectos administrativos, lógicos y físicos, se observa como una pirámide ya que según el eje de orientación descendente, inicia desde el punto más alto de una organización hasta el nivel operativo.

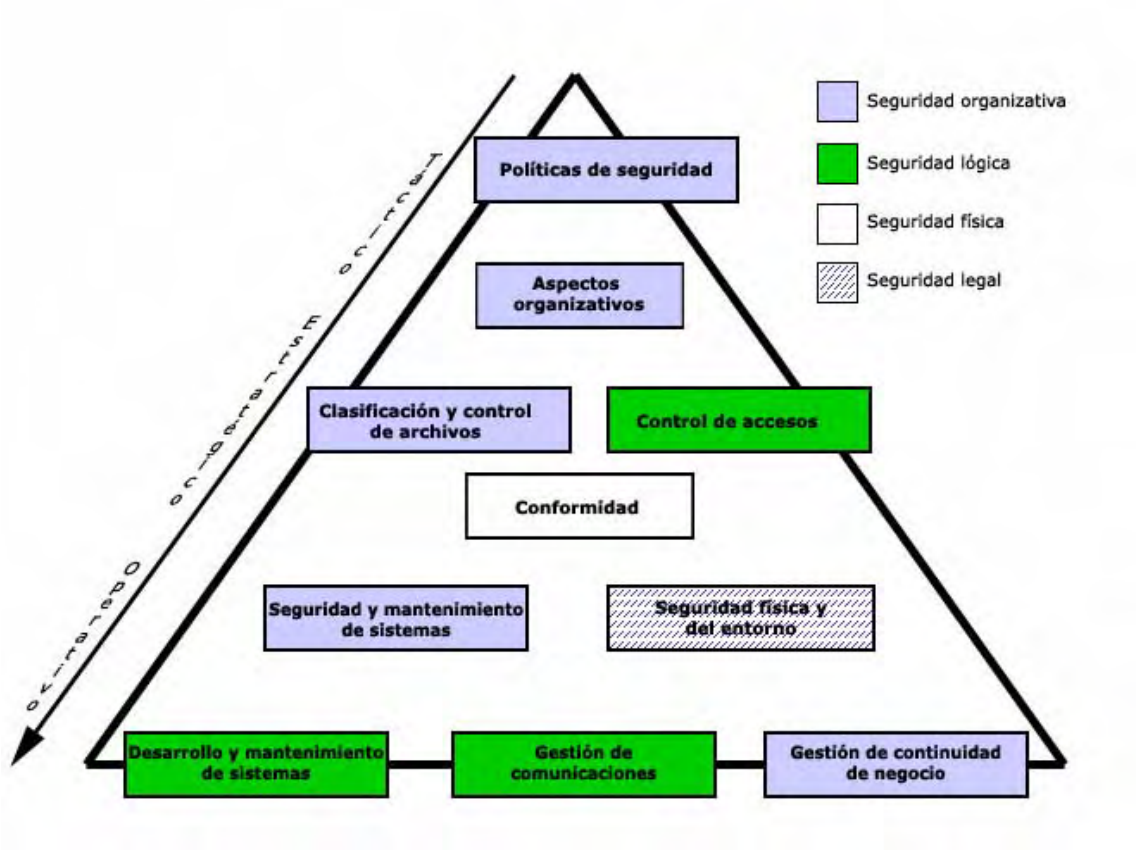

Figura 2.3.- Esquema que muestra los once controles del ISO/IEC 17799

2.5 - ¿A quién va dirigida ISO/IEC 17799:2005?

ISO 17799 puede ser utilizado por cualquier tipo de organización o compañía privada o pública. Si la organización utiliza sistemas internos o externos que poseen información confidencial, si depende de estos sistemas para el funcionamiento normal de sus operaciones o si simplemente desea probar su nivel de seguridad de la información apegándose a una norma reconocida, ésta puede ser la norma ISO/IEC 17799.

Tipo de empresa	Tamaño	Objetivo principal	Utilización de la norma
Pequeña empresa u organismo	Inferior a 200 empleados	Sensibilizar a la Dirección de la seguridad de la información	La norma ISO/IEC 17799 contiene los temas de seguridad que deben tratarse como base de la Gestión.
Empresa media (centralizada o descentralizada)	Inferior a 1000 empleados	Crear una cultura de seguridad global compatible	La norma contiene las prácticas necesarias para constituir la seguridad de la información
Empresa muy grande	Superior a 1000 Empleados	Obtener una certificación de seguridad	Utilización del ISO para crear un documento referencial e integral de seguridad interna

Cuadro 2.1. Tipos de empresas que pueden utilizar la norma.

Cabe señalar que el IIMAS cae en el tipo de empresa pequeña por las características mencionadas en cuadro 2.1., además por los objetivos de la misma, siendo una dependencia académica en donde el ISO 17799 es un punto de partida para la seguridad de la Información.

2.6 Beneficios de la norma.

El hecho de implantar seguridad a través de un estándar o de obtener la certificación no garantiza el 100% de la seguridad de la información. No obstante la adopción del estándar internacional proporciona ventajas que cualquier organización debe tomar en cuenta.

En el siguiente cuadro (**véase cuadro 2.2**) se muestra los diversos aspectos y beneficios al implementar el estándar.

Aspecto organizacional • La certificación permite garantizar y demostrar la eficacia de los esfuerzos desarrollados para asegurar la información en todos sus niveles. • Permite establecer una metodología de la gestión de la seguridad de la información clara y estructurada. • Las auditorias externas ayudarán a identificar las debilidades de los sistemas de información y las mejoras que se pueden realizar. • El sistema se puede integrar con otras normas (ISO 9001, ISO 14001, etc.) • La organización obtendrá una imagen internacional y un elemento diferenciador de su competencia.	**Aspecto funcional** • Tener un mejor conocimiento de los sistemas de información, sus fallas y los medios de protección. • Garantiza también una mejor disponibilidad de los activos y de la información que existe en la organización. • Reduce el riesgo de pérdida, robo o corrupción de la información. • Revisa continuamente los controles y los riesgos. • Ofrece continuidad a las operaciones criticas de la organización tras algún incidente de seguridad
Aspecto comercial • Existe la confianza de los socios, los accionistas y usuarios al constatar la importancia que la organización concede a la seguridad de la información. • Algunas licitaciones internacionales ya comienzan a pedir una gestión ISO 17799.	**Aspecto financiero** • Reducción de los costos vinculados a los incidentes y posibilidad de disminución de las primas de seguro.
Aspecto humano • Mejora la sensibilización del personal a la seguridad y a sus responsabilidades en la organización. • Además proporcionará confianza y reglas claras al personal de la organización.	

Cuadro 2.2. Aspectos que se benefician en la implementación del estándar

2.7 ISO 27001.

ISO 27001 es una norma internacional que no se orienta a aspectos tecnológicos o de infraestructura, sino que su propósito principal se define como "organizar la seguridad de la información" es por esto que se compone de varias etapas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI o ISMS (Information Security Management System)"[θ]

Esta norma al igual que el BS 7799-2 es certificable. Esto significa que la organización que tenga implantado un SGSI podrá solicitar una auditoria a una entidad certificadora acreditada y en caso de aprobar exitosamente obtendrá la certificación del sistema.

El SGSI debe ser una decisión estratégica de cualquier organización que inicia de sus necesidades, objetivos, requerimientos de seguridad, procedimientos y estructura de la organización.

Está conformada por:

- **Introducción:** generalidades e introducción al método PDCA.
- **Campo de aplicación:** se especifica el objetivo, la aplicación y el tratamiento de exclusiones.
- **Referencias normativas:** otras normas que sirven de referencia.
- **Términos y definiciones:** breve descripción de los términos más usados en la norma.
- **Sistema de gestión de seguridad de la información:** cómo establecer, implementar, monitorizar, revisar, mantener y mejorar el ISMS; requerimientos de documentación y su control.
- **Responsabilidades de la Dirección:** en cuanto a compromiso con el ISMS, provisión de recursos y formación y concienciación del personal.
- **Auditorias internas del ISMS:** realizar las auditorias internas de control.
- **Revisión del ISMS por la Dirección:** cómo gestionar el proceso de revisión constante del ISMS.
- **Mejora de ISMS:** mejora continua y acciones preventivas.
- **Resumen de controles:** anexo que enumera los objetivos de control y controles que se encuentran detallados en la norma ISO 17799.
- **Relación con los Principios de la OCDE:** correspondencia entre los apartados de la ISO 27001 y los principios de buen gobierno de la OCDE.
- **Correspondencia con otras normas:** tabla de correspondencia de puntos con ISO 9001 y 14001.

2.7.1 PDCA (Plan-Do-Check-Act).

Este estándar internacional maneja también el modelo "*Plan-Do-Check-Act*" PDCA[π] (véase figura 2.4.) el cual es aplicado al SGSI, y se describe a continuación:

Figura 2.4. Modelo PDCA

- **Plan** (Establecer el SGSI): Significa establecer al SGSI, los objetivos, procesos, procedimientos, los riesgos y mejoras para la seguridad de la información, según las políticas y objetivos de la organización.
- **Do** (Implementar y operar el SGSI): Se refiere a la forma en que se debe operar e implementar las políticas, controles, procesos y procedimientos.
- **Check** (Revisar el SGSI): Analizar y ajustar los procesos con relación a la política del SGSI, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.
- **Act** (Mejorar el SGSI): Realizar las acciones preventivas y correctivas, para lograr la mejora continua del SGSI.

2.8 Implementación del ISMS.

El proyecto de gestión de la seguridad de la información debe establecer previamente, de forma clara y documentada, el compromiso de los directivos de la organización de un SGSI (Sistema de Gestión de la Seguridad de la Información). Además de otras fases que más adelante se describirán, las cuales permitirán, además de lograr la certificación, llevar a varias acciones según ISO 27001 que apoya y mejora los procesos con base en los objetivos de la organización.[ϕ]

ISO 27001 exige que se cumplan los siguientes puntos:

Inicio del Proyecto

1.- Apoyo y compromiso de la principal autoridad de la organización.
Una de las partes iniciales del proyecto es contar con el apoyo total de la Dirección de la Organización. Ya que el cambio y concienciación de la norma deberá de iniciar desde ese punto, además del compromiso para poder impulsar el proyecto.
2.- Planear fechas y asignar responsables de las fases del proyecto. El tiempo y esfuerzo que se le dé a está fase aumentará los efectos positivos de las demás etapas.

Planeación

1.- Definir el alcance del SGSI: según el modelo organizativo, definir los límites del marco de dirección de seguridad de la información.
2.- Definir las políticas de seguridad: que incluya el marco general y los objetivos de seguridad de la información de la organización.
3.- Levantar un Inventario de activos que se vean afectados por la seguridad de la información.
4.- Identificar amenazas y vulnerabilidades a los activos del inventario.
5.- Análisis de riesgos: evaluar el daño resultante de un incidente de seguridad

Selección de controles
1.- Definir plan de tratamiento de riesgos, que identifique las acciones, sus responsables y las prioridades en la gestión de los riesgos de seguridad de la información.

Implementación
1.- Implantar un plan de tratamiento de riesgos, con la meta de alcanzar los objetivos de control identificados.
2.- Implementar los controles, todos los que se determinaron en la fase anterior.
3.- Formación y concienciación de todo el personal en lo relativo a la seguridad de la información.
4.- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.
5.- Gestionar todos los recursos asignados al SGSI.

Monitorización
1.- Revisar el SGSI para determinar si el alcance definido sigue siendo el adecuado, identificar mejoras al proceso, identificar nuevas vulnerabilidades, revisar cambios organizativos y modificar procedimientos.
2.- Realizar auditorias internas del SGSI: para determinar la efectividad y detectar posibles no conformidades.

Mejora continua
1.- Implantar mejoras: poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.
2.- Acciones correctivas: para solucionar inconformidades detectadas.
3.- Acciones preventivas: para prevenir potenciales inconformidades.

La documentación en las medidas para llevar a cabo el SGSI deberá incluir:
- Política y objetivos de seguridad.
- Alcance del ISMS.
- Procedimientos y controles que apoyan el SGSI.
- Descripción de la metodología de evaluación del riesgo.
- Informe resultante de la evaluación del riesgo.
- Plan de tratamiento de riesgos.
- Procedimientos de planificación, manejo y control de los procesos de seguridad de la información y de medición de la eficacia de los controles.
- Registros.
- Procedimiento de gestión de toda la documentación del SGSI.

2.9 Aspectos a considerar.

Aunque se realicen todos los pasos mencionados para obtener los objetivos del proyecto, hay aspectos claves y fundamentales que se deben considerar:

- Compromiso y apoyo de la Dirección de la organización.
- Compromiso del usuario y formación.
- Compromiso de mejoramiento continúo.
- Establecimiento de políticas y normas.
- Organización y comunicación.
- Integración del SGSI en la organización.

Algunos de los factores que nos pueden llevar a un buen logro al implantar este sistema son:

- La concienciación del personal o empleados de la organización por la seguridad.
- Realización de comités de dirección con descubrimiento continuo de "No conformidades" o acciones de mejora.
- Creación de un sistema de gestión de incidencias que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).
- La seguridad absoluta no existe, se trata de reducir el riesgo a niveles mínimos o que no afecten a la función de la organización
- La seguridad es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.
- La seguridad debe ser inherente a los procesos de información y del negocio.

Como todo proyecto existen riesgos latentes que se pueden presentar como son:
- Exceso de tiempos de implementación (Costos).
- Temor ante el cambio (Resistencia).
- Discrepancia en la Dirección.
- Planes de formación inadecuados.
- Calendario de revisiones que no se puedan cumplir.
- Definición poco clara del alcance.
- Exceso de medidas técnicas en la formación y concienciación.
- Falta de comunicación del progreso del proyecto con el personal de la organización.

2.10 Organizaciones certificadas.

Actualmente existen 3,309 organizaciones certificadas en ISO 27001 y BS7799-2 en el mundo. En ISO 27001 son 933, que incluyen 432 actualizaciones desde BS 7799-2 y 501 nuevas certificaciones.

Japón es el país con más organizaciones certificadas 1,907, el Reino Unido con 319 y la India con 269. En la tabla 2.1 se pueden observar el número de organizaciones en Latinoamérica incluyendo a México que han obtenido la certificación.

País	Número de Organización Certificadas
Brasil	19
México	12
Argentina	3
Colombia	2
Perú	2
Uruguay	1

Tabla 2.1 Países latinoamericanos con certificaciones.

Esta información con fecha de abril del 2007 se puede obtener mes a mes de forma detallada por países y empresas en International Register of ISMS Certificates.[vii]

2.11 Conclusiones.

En este capítulo se ha mostrado la importancia de la seguridad en los sistemas de información y la necesidad que tienen las organizaciones de alinear la seguridad a estándares internacionales y mantener así protegido uno de los más importantes activos para cualquier organización, **la información**.

Además se ha descrito los trabajos que ha realizado el ISO en el diseño de estándares internacionales a través de comités para determinadas actividades técnicas.

Así mismo, se describió el estándar de seguridad de la información ISO 17799, que se remonta a principios de los 90's y que publicó el Departamento de Comercio e Industria del Reino Unido como BS7799, en el 2000, el ISO lo publicó como un estándar internacional denominado ISO/IEC 17799. El estándar establece algunas definiciones, como por ejemplo, el concepto de seguridad informática, ¿por qué es necesaria la seguridad informática?, ¿cómo establecer los requerimientos de seguridad?, evaluación de riesgos, etc. Respecto de la seguridad de la información, la define como la preservación de las siguientes características o atributos de la misma: **confidencialidad, disponibilidad e integridad.**

Igualmente se definió los 133 controles específicos que sugiere el estándar para la gestión de seguridad de la información y que abarcan las políticas, prácticas y procedimientos.

Una vez que la organización tiene perfectamente implantadas las medidas necesarias para la administración de la seguridad es cuando podrá empezar el proceso de certificación a través del modelo PDCA, y cumplir los lineamientos que solicita el estándar, que únicamente podrá ser realizado por entidades que posean el reconocimiento y que después de realizar la pertinente auditoria podrán considerar que tienen correctamente seguros sus sistemas.

El siguiente capítulo aborda el tema sobre la tecnología BSD y en particular el sistema operativo OpenBSD, como la plataforma que se propuso utilizar para el caso de estudio, además con la definición de algunos conceptos básicos antes de iniciar el proyecto de gestión de seguridad.

---

[i] La Organización Internacional de Normalización ISO es un organismo, cuyo objetivo primordial es promover el desarrollo de la normalización y actividades relacionadas en el mundo, con la finalidad de facilitar el intercambio internacional tanto de bienes como de servicios http://www.iso.org

[ii] BSI (British Standard Institution) Más información: http://www.bsi-global.com

[**] The History of ISO 17799 and BS7799 http://www.pc-history.org/17799.htm

[iii] Comisión Electrotécnica Internacional.- http://www.iec.ch/

[iv] Norma de Administración de la Calidad. – http://www.iso.org

[v] Norma internacional de Sistemas de Gestión Medioambiental (EMS).- http://www.iso.org

[*] http://www.27000.org

[vi] http://www.27000.org

[θ] http://www.iso27000.es

[π] http://www.iso.org/iso/understand_the_basics

[ϕ] http://www.iso.org/iso/

[vii] http://www.iso27001certificates.com/

PLATAFORMA BSD

3.1 Introducción.

Actualmente la seguridad informática ha crecido exponencialmente debido al flujo de información a través de las redes; todo esto implica que es necesario utilizar herramientas que permitan trabajar mejor, pero manteniendo toda la seguridad necesaria. En este entorno donde la plataforma BSD y en especifico el sistema operativo OpenBSD cumple sus funciones mejor que cualquier otra alternativa, la presente investigación se enfocó en desarrollar y cumplir los lineamientos y especificaciones de ISO 17799 bajo dicha plataforma.

OpenBSD, es considerado como el sistema operativo más seguro del mundo de software libre y en especial, porque es una solución recomendable para el uso de firewalls, además de mi experiencia personal en su uso, a continuación se mencionan algunas características:

- Sistema operativo seguro por defecto.
- Un sistema proactivo.
- Contiene un firewall robusto, completo, auditable (packet filter), etc.

Cabe señalar que esta plataforma apoya al dominio del ISO 17799: "Gestión de Comunicaciones y Operaciones" y al control especifico 10.6.2 *Seguridad en los servicios de red,* del siguiente capítulo.

3.2 Antecedentes.

OpenBSD es un sistema operativo libre de tipo Unix. Fue desarrollado por la Universidad de Berkeley en California. Esta rama, conocida como BSD , era una rama del Unix original creado en 1969 en los laboratorios Bell, distribuido por la Universidad de Berkeley en California, que introdujo un elevado número de mejoras al sistema operativo Unix en general, como el nuevo sistema de memoria virtual, la creación de sockets o la implementación del protocolo TCP/IP, entre otras.

El sistema operativo OpenBSD incluye emulación de binarios para la mayoría de los programas de los sistemas SVR4 (Solaris), FreeBSD, Linux, BSD/OS, SunOS y HP-UX.

3.3 Distribución BSD.

La entidad que más aportó a Unix después de los laboratorios Bell fue la Universidad de Berkeley en California. Desde aproximadamente 1977, el C.S.R.G (University of California at Berkeley's Computer Systems Research Group) se encargo de crear y desarrollar un fork [i]del Unix original de los laboratorios Bell, al cual se le llamo BSD (Berkeley Software Distributions), que fue desarrollado en sucesivas versiones (1BSD, 2BSD, 3BSD y 4BSD) durante los años 70's y 80's.

Durante todo este tiempo, las mejoras aportadas por las diferentes versiones de BSD, fueron incorporadas en el UNIX original, o adaptadas, algunos ejemplos son:

- Nuevo soporte de memoria virtual.
- Sockets[ii].
- Incorporación de los protocolos de red (TCP/IP) utilizados por la Defense Advanced Research Projects Agency (DARPA)
- Llamadas al sistema o syscalls.
- La librería termcap.
- El verificador de código C link, entre otros.

3.3.1 Distribuciones BSD: NetBSD, FreeBSD y OpenBSD.

Tras varios años de investigación y desarrollo, el C.S.R.G consiguió a comienzos de los 90's publicar una versión de su sistema 4.4BSD (4.4BSD-Lite) que no requería que el usuario tuviera la licencia del código fuente de Unix. De este sistema surgieron dos alternativas dentro del mundo del software libre que evolucionaron en base a NetBSD y FreeBSD, que aparecen sobre los años 1991 y 1992.

Uno de los primeros commiters[iii] del proyecto NetBSD junto a Chris Demetriou fue Theo de Raadt.

Ambos comenzaron con el proyecto NetBSD con una máquina con CVS[iv] montada por Chris y trabajando sobre el código de lo que sería el primer NetBSD. El proyecto comenzó a crecer, varios desarrolladores fueron uniéndose al grupo, entre ellos Charles Hannum del M.I.T. (Massachusets Institute of Technology). A raíz de las diferencias con Hannum, Theo se separa definitivamente del proyecto NetBSD. A los pocos meses, crea un repositorio de código junto a algunos desarrolladores que no estaban de acuerdo con su exclusión del proyecto NetBSD y nace el proyecto OpenBSD.

3.3.2 Objetivos del proyecto OpenBSD.

En la página del proyecto [v] se puede observar una lista de los objetivos globales, algunos de ellos son:

- Proveer al usuario con acceso total a las fuentes desarrollados por el proyecto.
- Integrar cualquier tipo de código que disponga de una licencia aceptable, la idea es disponer de un código que sea accesible para cualquier usuario, tal y como se dice en el punto anterior, pero permitiendo al usuario haga lo que necesite con ese código.
- Intentar llevar un seguimiento de posibles bugs[vi], fallos y corregirlos antes que nadie, de esta forma se pretende conseguir el sistema operativo más seguro posible.
- Implementar en la medida de lo posible los estándares (ANSI, POSIX, etc.)
- Ser un proyecto totalmente apolítico.
- Sacar una versión en CD cada seis meses de desarrollo, lo que ayuda a financiar el proyecto.

Estos son tan sólo algunos de los objetivos del proyecto, aunque posiblemente el punto que más se conoce del proyecto y más importante, tratar de ser el número uno en cuanto a seguridad en sistemas operativos.

El enfoque del proyecto en este sentido ha sido claro desde las primeras versiones hasta la actual (4.3), mejorando versión a versión e incluyendo mejoras como la generación aleatoria de PIDs (Process ID o ID de proceso, que es el número con el que podemos referenciar a cada uno de los procesos del sistema), la generación aleatoria de los números de secuencia iniciales de las conexiones TCP, la integración de algoritmos de criptografía en el kernel, la separación de privilegios para la mayoría de daemons del sistema, soporte de más sistemas operativos y sobre todo el soporte para un mayor de hardware incluyendo chipsets para dispositivos inalámbricos (wireless), entre otros.

Se puede observar en la página http://www.openbsd.org/plus.html de todas las mejoras que se han aportado a nivel de seguridad por los desarrolladores de OpenBSD. Algo muy interesante, en la mayoría de los casos, esas mejoras son adoptadas luego no sólo por los demás sistemas derivados del BSD original, si no también por otros sistemas como Linux, Solaris, etc.

3.3.3 Plataformas soportadas.

OpenBSD soporta gran variedad de plataformas entre las que se pueden enumerar en la siguiente tabla 3.1.

Alfa	Sistemas Alfa- Digital.
Amd64	Sistemas de AMD64.
Armish	Aplicaciones Brazo-basadas (por Thecus, IO-Datos, y otros).
hp300	Sitios de trabajo de la serie 300 y 400 del HP 9000 de Hewlett-Packard.
Hppa	Sistemas de la arquitectura de la precisión de Hewlett-Packard (PA-RISC).
I386	La PC estándar y se reproduce basado en la arquitectura de Intel i386 y los procesadores compatibles.
luna88k	Sitios de trabajo LUNA-88K y LUNA-88K2.
mac68k	Motorola 680x0-based Apple Macintosh.
macppc	Apple PowerPC-, iMac **mvme68k** Sistemas de Motorola 680x0-based VME.
mvme88k	Sistemas de Motorola 881x0-based VME.
SGI	Estaciones de trabajo SGI.
Sparc	Sistemas SPARC
sparc64	Sistemas de UltraSPARC
Vax	Sistemas VAX-Digital
Zaurus	Zaurus C3x00 PDAs

Tabla 3.1. Plataformas que soportan el Sistema Operativo OpenBSD

3.4 OpenBSD y seguridad.

Desafortunadamente vivimos en un mundo sensible, en donde se rompen leyes, roban e invaden nuestros lugares personales. Por lo cuál tomamos acciones como levantar una cerca en nuestra casa, poner una malla electrificada, alarma al automóvil, contratar guardias de seguridad, etc. que por lo menos nos haga sentir un poco más seguros.

Las cosas no son diferentes en el mundo de las redes. Internet brinda acceso a lugares donde tienen oportunidades de realizar actividades como: consultar una página WEB, enviar un correo electrónico, visitar un museo virtual, etc. Pero también da oportunidad de realizar actividades cuestionables, como robar información, interrumpir servicios de red, espiar comunicaciones, destruir datos, falsificar información y afectar a grandes sistemas, todo esto realizado por individuos que incluso lo ven como un estilo de vida, por motivos de dinero, desafío o simplemente por curiosidad o jactarse de algo. Actualmente las nuevas tecnologías permiten ampliar el ataque a un número de redes, comprometerlos y a través de ello conseguir afectar a otras. Una persona puede ser potencialmente peligrosa ya que puede causar daño a un número inimaginable de equipos. Se tiene la idea de que la red de una universidad o caseras no tienen un valor para un atacante, pero si para que a través de ellas ataquen a otras, comprometiéndola y poniendo en riesgo la información.

En resumen, la mejor manera de luchar contra los ataques es la prevención. Para evitar problemas muchas organizaciones invierten grandes sumas de dinero en tecnologías, capacitación de su personal, implementación de seguridad, etc., para poder mantener segura su información.

3.4.1 OpenBSD, seguro por defecto.

Un sistema seguro por defecto es como se puede denominar a OpenBSD, esto ha hecho que la comunidad de UNIX observe con mayor atención al sistema y demostrar a los desarrolladores que no existe un sistema seguro.

Seguro por defecto, en el contexto del proyecto OpenBSD, significa un sistema que "*out-of-the-box*" como se suele decir, o recién instalado, sea lo más seguro posible sin necesidad de pasar un tiempo configurándolo. OpenBSD recién instalado no solo no tiene servicios corriendo por defecto, si no que los que tiene están configurados de forma que no expone al sistema a ataques externos.

Existen otras razones técnicas como la madurez que tiene el código, hay más de 25 años de desarrollo almacenados en el código BSD desde 1976, su estabilidad y gracias al plan de desarrollo del sistema lo hace uno de los sistemas operativos libre más seguro.

3.4.2 ¿Qué significa seguridad proactiva?

Seguridad proactiva, siempre hablando dentro del contexto del proyecto OpenBSD, significa que se intenta buscar fallas, auditar todo el código, localizar bug, explorando con técnicas que se van descubriendo en el campo de la seguridad informática, tratando de identificar errores en el resto del código.

De esta forma se consigue tener un sistema en constante fase de auditoria, aumentando la posibilidad de ser los primeros en encontrar fallas en cualquier parte del sistema y no solo corrigiéndola para OpenBSD, si no ayudando a otros proyectos a corregirlos y mejorar la seguridad de sus sistemas en general.

3.5 Firewall.

Un firewall es un método de protección de hosts[vii] y redes conectadas con otras redes contra ataques (un ataque se define como el o los intentos de acceder de manera no autorizada a una red, para destruir servicios, "escuchar" la red, alterar las comunicaciones, robar y/o alterar datos o software). Cuando se habla del término "Firewall" generalmente se piensa en una configuración de red para cierto propósito, o un producto de software y dispositivo (hardware).

También es importante mencionar que no se considera un firewall, como un único elemento en un esquema de seguridad, que con este se protegerá totalmente cualquier host de una red, puede controlar quién se conecta, pero no previene la salida de información confidencial de algún punto de la red.

3.5.1 ¿Porqué utilizar un firewall?

Un firewall es una de las herramientas esenciales para la seguridad de la información, debido al trabajo que realizan ya que son la primera línea de defensa contra ataques externos. Consiste en una mezcla de hardware y software colocados en puntos estratégicos de una red y generalmente es el primero contacto con otras redes. Su propósito principal es revisar los paquetes de datos que fluyen en la red y según unas reglas bloquear dichos paquetes o dejarlas pasar, según la política de filtración de paquetes.

En los últimos diez años, el firewall ha adquirido una funcionalidad adicional mucho más que filtrar paquetes en una red. La conversión de red (Network Address Translation) NAT, apoyo en los filtros del SPAM[viii], configuración de reglas dinámicas y otras funcionalidades avanzadas.

Hay tres formas de *operar* los firewalls:

- *Filtrado de paquetes*. Cada paquete de información se analiza con respecto a una serie de filtros. Los paquetes que logran pasar los filtros se envían a la computadora que lo solicitó y todos los demás se descartan.
- *Proxy*. Las peticiones internas son enviadas al firewall, esta a su vez envía al proxy en donde se analiza la información y determina los paquetes que van a tener salida.
- *Inspección estática*. No se examinan los paquetes de la información, pero se comparan ciertas partes clave de cada paquete en búsqueda de datos confiables. Los datos que salen de la red local se analizan registrando patrones específicos, de tal manera que la información entrante debe cumplir con esos patrones. Si hay un cierto margen de coincidencia, el material entrante pasa sin problema; en otro caso, se descarta.

3.5.2 Firewalls, filtrado de paquetes.

Los firewalls de filtrado de paquetes consisten en un software que, dependiendo de una serie de reglas establecidas, modifican el tráfico de red a través de un determinado dispositivo de red. Dicha reglas controlan el acceso a servicios como el Word Wide WEB (WWW), File Transfer Protocol (ftp) o de mensajería instantánea, entre otros. Por ello, muchos usuarios detrás de un firewall no pueden recibir archivos a través de la mensajería instantánea, o tampoco pueden acceder a algunos sitios de la WEB que pueden estar clasificados como distribuidores de programas maliciosos o virus.

Este tipo de firewalls son cada día más utilizados por su sencillez de configuración y su eficacia, además de disponer de diferentes tipos para los sistemas operativos basados en software libre, lo que hace que se pueda disponer de firewalls muy seguros y estables a un costo muy bajo. Algunos ejemplos de software de filtrado de paquetes en el ámbito del software libre son netfilter para el kernel de Linux, o ipf, ipfw o pf[ix] para sistemas basados en BSD. Este último es el que se utilizó en el desarrollo del esquema de seguridad para el IIMAS y que se mencionará en el siguiente capítulo de la presente investigación.

Los filtros de un firewall se definen a partir de ciertos criterios, tales como:

- *Direcciones IP[x]*. Se puede bloquear el acceso desde una IP específica, evitando ataques o consultas masivas a equipos servidores y clientes.
- *Nombres de dominio*. Consiste en tablas con nombres de computadoras vinculadas al DNS en donde no se permite el acceso de los usuarios locales.
- *Palabras clave*. Programa de captura de tramas de red (sniffer) en los firewalls revisan el contenido de la información en búsqueda de palabras vinculadas con información o sitios no permitidos.
- *Puertos*. Cada aplicación o servicio que usa la red IP, genera una conexión hacia un puerto. El 80 es el común para los servidores WWW y el 21 para las transferencias de archivos. Un firewall registra estos servicios, qué computadoras pueden acceder a ellos y cuáles no.
- *Protocolos*. Es factible restringir el uso de algunos protocolos, como HTTP o Telnet (para sesiones remotas). Así se evita que usuarios mal intencionados del exterior de la red, intenten acceder a un equipo local mediante un protocolo específico.

3.6 ¿Qué es Packet Filter ?

Es el software de filtrado de paquetes creado y desarrollado por el equipo del proyecto OpenBSD. Desde la versión 3.0 de OpenBSD es la opción utilizada por defecto.
Algunos de los puntos fuertes de packet filter (pf) son:

- Filtrado de paquetes IPv4 e IPv6
- Network Address Translation (NAT)
- Normalización de paquetes
- Balanceo de carga
- Modulación de ancho de banda
- Análisis de paquetes
- Autenticación de usuarios contra el firewall

Pf es lo que se conoce como un *stateful packet filter* o, lo que es lo mismo, un software de filtrado de paquetes que controla el estado de las conexiones. Debido a esto, en lugar de dejar pasar todo el tráfico hacia un determinado puerto, se puede permitir solo el paso del primer paquete, el resto del tráfico podrá pasar igualmente debido a que el firewall ha guardado información referente a esa conexión y sabe que paquetes pertenecen a la misma.

Las reglas se encuentran en un archivo llamado "pf.conf" y tiene 3 clases de reglas:

- *block*: bloquea paquetes de datos.
- *pass:* permite pasar los paquetes de datos.
- *antispoof*: un especial caso de la regla "block"

Las reglas de filtración de paquetes, como la mayoría de las reglas usan una gramática especial, capaz de describir detalles:

- *La acción*: (block o pass). Indica la acción que tomará cuando se encuentra un paquete. Está parte es requerida.
- *La dirección* (in o out). Decide cual paquete entra o sale. Esta parte es requerida.
- *El log* (log). Va describiendo una bitácora de los paquetes entrantes y salientes. Está parte es opcional.
- El *quick* una vez ejecutada discrimina a otra regla similar que describa o tenga la misma ejecución.
- *La interface name* (interfase). Esta es opcional, pero rara vez se omite. Cuando no se coloque, la regla se aplica a todas las interfaces.
- *Direcciones* (IPv4 y/o IPv6) Está parte es opcional.
- *Protocol Name (Nombre del protocolo).* Se coloca el protocolo a utilizarse, es opcional.
- *Source host address and port number (host y puerto).* Nombre y puerto del host origen.
- *Target host address and port number* (*host y puerto*). Nombre y puerto del host destino.

Ejemplos:

block in all *(bloquea todo los paquetes que entren a la red local)*	pass in all *(permite pasar todos los paquetes que entren a la red local)*
block out all *(bloquea todos los paquetes que salgan de la red local)*	pass out all *(permite salir todos los paquetes de datos de la red local)*

3.7 Tipos de firewalls.
3.7.1 Firewall Bridge.

Un bridge [xi] es la unión de dos o más interfaces de red (tarjeta de red NIC), entre sus objetivos se encuentran:

- Ruteo de paquetes.
- Políticas de protocolo.
- Filtrado de información.
- Proteger equipos sin necesidad de modificar a los clientes.

El firewall bridge contiene el pf que protegerá la red de ataques externos a través del filtrado de paquetes.

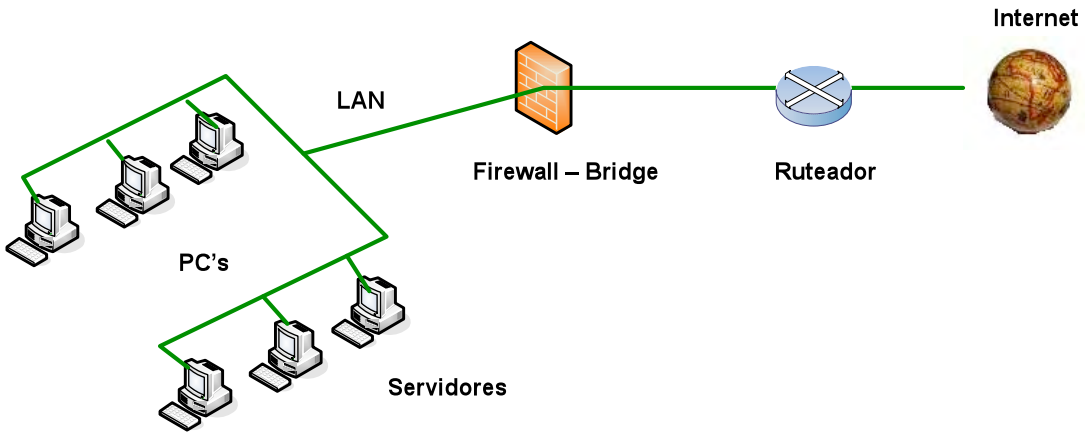

Figura 3.2 Firewall (Bridge)

En la figura 3.2 después del ruteador se coloca inmediatamente el firewall, a través de las políticas se protegerá a la red interna, el firewall decidirá a que equipo de la red interna podrá dejar pasar o no el paquete de datos.

Características de Bridge Firewall:

- Filtrado de paquetes, por medio de reglas de Firewall.
- Probabilidades de vulnerabilidades muy bajo.
- No cuenta con IP
- Es también conocido con el término de "firewall transparente"

3.7.2 Firewall NAT.

NAT (*Network Address Translation*), es un sistema que se utiliza para asignar una red completa (o varias redes) a una sola dirección IP. NAT es necesario cuando la cantidad de direcciones IP que nos haya asignado nuestro proveedor de Internet sea inferior a la cantidad de computadoras que queramos que accedan a Internet. Se describe en el RFC 1631.

A través de NAT permite aprovechar los bloques de direcciones reservadas que se describen en el RFC 1918. Generalmente, una red interna se suele configurar para que use uno o más de estos bloques de red. Estos bloques son:

10.0.0.0/8 (10.0.0.0 - 10.255.255.255)
172.16.0.0/12 (172.16.0.0 - 172.31.255.255)
192.168.0.0/16 (192.168.0.0 - 192.168.255.255)

En un sistema OpenBSD configurado para NAT tendrá como mínimo dos adaptadores de red, una para Internet y la otra para la red interna. NAT se encargará de traducir los requerimientos desde la red interna, de modo que parezca que todos provienen del sistema OpenBSD en el que se encuentra configurado NAT.

3.7.2.1 ¿Cómo funciona NAT?

Cuando un cliente en la red interna (LAN) contacta a otra computadora en Internet, envía paquetes IP destinados a esa máquina. Estos paquetes contienen toda la información de direccionamiento necesaria para que puedan ser llevados a su destino. NAT se encarga de estas piezas de información:

- Dirección IP de origen (por ejemplo, 192.168.1.35)
- Puerto TCP o UDP de origen (por ejemplo, 2132)

Cuando los paquetes pasan a través del firewall NAT, son modificados para que parezca que se han originado y provienen del NAT, este registra los cambios que realiza en su tabla de estado, para así poder:

1) Invertir los cambios en los paquetes devueltos, y
2) Asegurarse de que los paquetes devueltos pasen a través del firewall y no sean bloqueados.

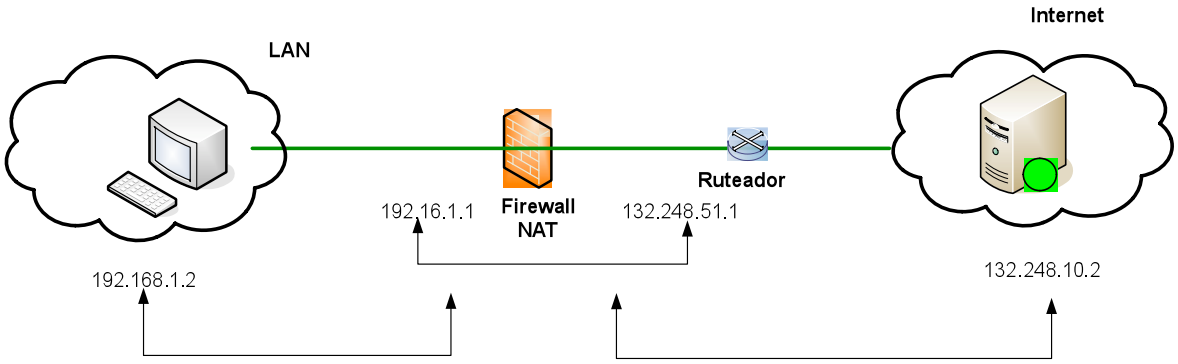

Figura 3.3. Funcionamiento del Firewall NAT

Como se puede observar en la figura 3.3 ni la máquina interna ni el servidor en Internet se dan cuenta de estos pasos. Para la máquina interna, el sistema NAT es simplemente un paso más para salir a Internet. Para el servidor en Internet, los paquetes parecen venir directamente del firewall NAT.

Cuando el servidor en Internet responde a los paquetes internos de la computadora, los direcciona a la IP externa de firewall NAT (132.248.21.1) y su puerto (80). El firewall NAT busca entonces en la tabla de estado para determinar si los paquetes de respuesta concuerdan con alguna conexión establecida. Entonces encontrará una única concordancia basada en la combinación de la dirección IP y el puerto, y esto indica a packet filter que los paquetes pertenecen a una conexión iniciada por la máquina interna 192.168.1.2. A continuación realizará los cambios opuestos a los que realizó para los paquetes salientes, y reenvía los paquetes de respuesta a la máquina interna.

Existen tres tipos de reglas del NAT:

- nat: Translada un grupo de direcciones IP's no homologadas[xii] a una sola dirección IP homologada[xiii]
- rdr: Redireccionamiento de una dirección IP y puerto.
- binat: Translado bidireccional entre una IP no homologada y una IP homologada.

3.8 Otros elementos de seguridad.

3.8.1 Sistema de detección de intrusos (IDS).

Una *intrusión* se le puede denominar como un conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso. Analizando esta definición, podemos deducir que una intrusión no tiene por qué consistir en un acceso no autorizado a un equipo también puede ser una negación de servicio.

A los sistemas utilizados para detectar las intrusiones o los intentos de intrusión se les denomina sistemas de detección de intrusiones (Intrusion Detection Systems) IDS, es un programa usado para detectar accesos no autorizados a una computadora o a una red. Estos accesos pueden ser ataques de habilidosos de usuarios o cracker a través de diversas herramientas.

Una de las primeras cosas que se planteo a través de esta investigación es si realmente necesitamos uno de ellos en el entorno de trabajo del Instituto; a fin de cuentas, se debe tener ya un sistema de protección perimetral basado en un firewall, y por si el firewall fallará, cada sistema deberá estar configurado de una manera correcta, de forma que incluso sin el firewall cualquier máquina pudiera seguirse considerando relativamente segura.

¿Es necesario tener un IDS además de un firewall? La respuesta es, sin duda, sí; debemos esperar que en cualquier momento alguien consiga romper la seguridad de de información y por lo tanto se consideró importante detectar ese problema tan pronto como sea posible (incluso antes de que se produzca, cuando el potencial atacante se limite a probar suerte con los equipos en la red del Instituto).

Ningún sistema de información puede considerarse completamente seguro, pero incluso, aunque nadie consiga violar las políticas de seguridad, los sistemas de detección de intrusos se encargarán de mostrar todos los intentos de multitud de ataques para penetrar el entorno, y si estar conscientes de que los equipos en la red están seguros porque nadie sabe de existencia o porque no son interesantes para los intrusos.

Un IDS también simplifica la tarea de verificar y categorizar las amenazas en los informes que se presentan a la administración ejecutiva. Esta información sólida ayuda a la Dirección a aceptar la administración de la seguridad adicional.

3.8.2 Sistema de prevención de intrusos (IPS)

Los sistemas de prevención de intrusiones de red (Intrusion Prevention Systems) IPS son una tecnología novedosa que esta diseñada para detectar y prevenir los ataques *antes* de que logren ingresar a la red objetivo. Y como dichos sistemas están localizados en la red para que cumplan su objetivo, los mismos deben ser probados.

Un IPS no es un IDS. El IPS esta diseñado para bloquear los ataques y asegurar que el segmento de la infraestructura que protege se mantiene seguro. Por lo tanto reportar es necesario pero la exactitud de los reportes se convierte en menos importante que en un IDS, siempre y cuando se este bloqueando de manera apropiada.

Como parte integral de la misión de un IPS, debe estar en capacidad de reforzar las políticas de seguridad de la red, reportando y/o bloqueando la posibilidad de ingreso como “root” a los sistemas sin canal encriptado por ejemplo. Cada organización tiene diferentes políticas de seguridad por lo tanto no todos los refuerzos de políticas deben estar habilitados de forma predeterminada, sin embargo si debe permitirlo. Y adicionalmente ser suficientemente flexible como para poder configurarlo con esto en mente.

Tres operaciones se pueden distinguir en la operación de un IPS. Su implementación esta altamente ligada a las necesidades de la organización:

1. *Bloqueo de intentos de Intrusión*: mitigar los ataques que pueden conducir a un escalamiento de privilegios y/o a la ejecución de código remoto en el sistema objetivo.
2. *Reducir los DoS [xiv] y refuerzo de políticas de tráfico*: proteger la infraestructura de ataques lanzados con el propósito de interrumpir el servicio total o parcialmente y/o inundar los enlaces de comunicaciones.
3. *Investigación de túneles*: detectar canales de comunicación con propósitos de fugas de información o eludir las políticas de seguridad y/o enviar órdenes desde el exterior a sistemas comprometidos en el interior.

3.8.3 Sistema de detección de intrusos de red (NIDS)

Un sistema detección de intruso de red (Network Intrusion Detection System) NIDS puede proteger contra los ataques que entran a través del firewall hasta la LAN. Los firewalls pueden estar mal configurados, permitiendo la introducción de usuarios o código no deseado en nuestra red. Incluso cuando funcionan correctamente, los firewalls normalmente dejan pasar alguna aplicación que puede ser peligroso. Lo que llega a los puertos del firewall, y está permitido por las reglas, se envía a los servidores internos provocando un tráfico potencialmente dañino. Un NIDS puede comprobar dicho tráfico y marcar los paquetes sospechosos. Configurado correctamente puede hacer una doble comprobación de las reglas del firewall y proporcionar protección adicional para los servidores de aplicación.

Aunque es útil para proteger contra ataques externos, una de las ventajas principales de un NIDS es buscar los ataques y la actividad sospechosa de origen interno.

El firewall protegerá de muchos ataques externos, sin embargo, cuando el atacante se encuentra en la red local puede hacer muy poco. Sólo puede ver el tráfico que lo atraviesa desde el exterior y son ciegos respecto a la actividad de la LAN. Por lo tanto se puede deducir que los NIDS y los firewalls son dispositivos de seguridad complementarios, una protege un perímetro y el otro el interior de la red.

Hay una buena razón para vigilar el tráfico de red interno. Las estadísticas demuestran que un setenta por ciento de los incidentes informáticos provienen de un origen interno. Por mucho que nos guste pensar que nuestros compañeros no van a hacer nada para dañarnos, aunque a veces no es el caso, los intrusos internos no siempre son usuarios que trabajan por la noche, pueden ser desde un administrador de sistemas contrariado, un empleado descuidado o hasta la señora de la limpieza.

El simple hecho de descargar un archivo o de abrir un archivo adjunto de un mensaje de correo electrónico puede cargar un troyano que creará un hueco de seguridad en el firewall para todo tipo de acciones que perjudiquen la información de la organización o a terceros. Con un NIDS, podemos captar este tipo de actividades como otros problemas en cuanto se producen.

3.9 Zona Desmilitarizada (DMZ).

Es común que una red LAN conectada a Internet exponga sus recursos como un servidor WEB, un servidor de correo electrónico, un servidor de base de datos, entre otros, todo esto crea toda clase de riesgos de seguridad que la red y un firewall tiene que afrontar.

DMZ (Demilitarized Zone) zona desmilitarizada se define como aquella zona de una red que no está protegida por el firewall, normalmente porque en ella se encuentran servidores que ofrecen servicios públicos en Internet, como los que se mencionaron anteriormente.[xv]

Estás zonas se crean con el objetivo de que su contenido sea fácilmente accesible desde el exterior, y esa misma particularidad las convierte en sumamente susceptibles de sufrir todo tipo de ataques internos, por lo cual es mejor tenerlas separadas del resto de la red por el riesgo potencial que suponen.

Muchos firewalls corporativos incluyen como opcional la creación de DMZ's simplemente conectados los servidores de la zona a una ethernet diferente al que está conectando el resto de la LAN y sobre la que no se aplican las reglas del firewall.

Por supuesto, nunca debe colocarse en los servidores de una DMZ información valiosa o susceptible de ser robada.

3.10 Conclusiones.

Implementar seguridad se refiere a realizar una gama de actividades, medidas a tomar, etc., y una de ellas es elegir que herramientas ayudarán en dicha implementación. Muchas veces se adquiere hardware o software desconociendo sus capacidades y en varias ocasiones no se utiliza en su totalidad.

Dentro del software libre existen herramientas que puede apoyar esa fase operativa en la gestión de seguridad en una organización. El capítulo 3 muestra y justifica al Sistema Operativo OpenBSD como una plataforma segura y robusta para la configuración de firewall y plataforma para la instalación y configuración de otros servicios de red.

Otro punto importante mencionar es que cualquier esquema de seguridad no es suficiente tener un firewall, aunque es un elemento de seguridad importante dentro del proyecto deben utilizarse otros elementos como un Proxy, IDS, ISP, etc., que se mencionan en el presente capítulo.

Una vez definido los conceptos básicos sobre la plataforma que se utilizó en el caso de estudio, el siguiente capítulo inicia con el análisis de riesgos, previo a la revisión de seguridad en el Instituto.

[i] Llamada para crear procesos en Unix. HP-UX version 9.05. User´s & Programmers Manual. BSD Concepts Manuals
[ii] Concepto que se utiliza para la conexión de programas.
[iii] Término designado a los colaboradores que tienen acceso de escritura al repositorio de código
[iv]El Concurrent Version System (CVS) es un sistema de mantenimiento de código fuente usado ampliamente por los proyectos de desarrollo de software de fuente abierta (open-souce). http://www.nongnu.org/cvs/
[v]Referencia: http://www.openbsd.org
[vi] Término aplicado a los errores descubiertos al ejecutar un programa informático.
[vii] Host: es un equipo que va a conectado a una red de datos y que generalmente brinda un servicio (transferencia de archivo, correo electrónico, WWW, etc.)
[viii] Spam son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas.
[ix] Pf (Packet Filter) firewall del Sistema Operativo OpenBSD. Artymiak, Jacek, Building Firewalls with OpenBSD and PF, Second Edition, Editorial Lublin, 2003.
[x] Internet Protocol
[xi] Es un dispositivo que conecta dos o más subredes. Network Security, Private Communication in a Public World, C. Kaufman, R. Perlman, M.Speciner, Ed. Prentice Hall, 2002, 2da. Edición.
[xii] IP no homologada es una dirección no ruteable (privada)
[xiii] IP homologada es una dirección de red valida dentro de Internet o ruteable
[xiv] DoS (*Denial of Service)* Denegación de servicios: es un ataque a un sistema o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
[xv] Building DMZs for Enterprise Networks, R.J. Shimonski, W. Schmied, V. Chang, T.W. Shinder,Editorial Syngress; 2003

CAPÍTULO 4

REVISIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL IIMAS

4.1 Introducción.

La seguridad de la información no se reduce únicamente a grandes corporaciones; ni siquiera podemos hablar de un máximo o un mínimo de presupuesto. Garantizar el acceso y la integridad de la información ha pasado a ser una prioridad en las organizaciones que quieren abrirse al mundo, independientemente de su actividad y tamaño.

El nivel más alto dentro de una organización debe ocuparse de proteger dicha información además de tener conocimiento de todos los riesgos a que están expuestos y las medidas de protección en caso de que los riesgos se materialicen. Por lo cuál se debe desarrollar una gestión de seguridad de la información que permita que está sea compartida y resguardada, así como también los activos.

ISO 17799 se refiere al análisis de riesgos, como un paso importante en la gestión de la seguridad, en base a ese análisis se desarrollará los controles necesarios y se tomará las decisiones concernientes al tratamiento del riesgo.

Un análisis de seguridad se inicia con definir el valor de la información y su sensibilidad, es decir, que tan importante es la información que se maneja, bien por procesos de la organización o por necesidad de compartir datos; después se identifican las amenazas sobre las aplicaciones o activos, y lo más importante será tratar de cuantificar los daños que pueden causar en caso de que las amenazas sean ejecutadas.

Para el presente caso de estudio, la revisión de la Seguridad de la Información, se efectúo en el Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas (IIMAS) con la colaboración de las Secretarias Académica y Técnica, cabe mencionar que la información que se utilizó se obtuvo de la página WEB[i] del Instituto con la autorización del mismo.

Con base a los requerimientos de ISO 17799, la organización debe contar con una gestión de administración de la seguridad, para esto, se siguieron los pasos que a continuación se menciona:

Inicio del proyecto
Actividades:

- Junto con la Secretaría Técnica se investigó los requerimientos y expectativas de la seguridad en el Instituto además se revisó la seguridad actual.
- Se insistió en la importancia y compromiso de la organización para poder impulsar el proyecto.
- Por otra parte se definió el alcance del proyecto que se describe en este capítulo (véase 4.6).

Inventario de los activos y análisis de riesgos **Actividades:** • Con la Secretaría Técnica se identificaron los activos que pueden afectar a la organización en caso de algún incidente de seguridad (véase 4.7.1) • Se detectó las amenazas y vulnerabilidades a los activos del Inventario**.** • Se elaboró junto con la Secretaría Técnica, el análisis de riesgos dependiendo del valor del activo y sus posibles amenazas y vulnerabilidades (véase 4.7.2).
Revisión de la seguridad **Actividades:** Asimismo, como parte de la presente investigación se procedió a realizar una revisión de seguridad al IIMAS a partir de los 11 dominios y 133 controles específicos que define el ISO 17799. (véase Apéndice A)
Selección de Controles **Actividades:** Para reducir el riesgo evaluado se desarrollaron y propusieron dos controles de seguridad : • Políticas General de seguridad de la Información (Véase Apéndice B). • Gestión de seguridad en la red. (Véase Capítulo 5)

Como parte del proyecto de Gestión de Seguridad de la Información en el Instituto, es importante describir los objetivos, misión, visión y estructura de la organización como lo menciona el estándar para iniciar con el proyecto.

4.2 Antecedentes.

El Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas tiene como antecedente al Centro de Cálculo Electrónico (CCE), fundado en 1958, año en que se instala la primera computadora en la Universidad Nacional Autónoma de México, con el fin de utilizarla para el avance de la ciencia en el país

En 1967 se modernizo el Centro y, en particular, se adquiere una computadora con tecnología muy avanzada para su tiempo. Su uso se difunde rápidamente, pasando de 60 a 2000 usuarios activos. El programa de formación de especialistas se incrementó.

Al intensificarse sustancialmente las actividades relacionadas con el servicio a los usuarios, se decide dividir al CCE en dos Centros, por lo que en 1973 se crean el Centro de Servicios de Cómputo (CSC) y el Centro de Investigaciones en Matemáticas Aplicadas y en Sistemas (CIMAS). A partir de ese año se amplían los grupos de trabajo y se diversifican las actividades. Se desarrollan Investigaciones en Aplicaciones de Software, en Computación Teórica, Electrónica Digital, Estadística, Investigación de Operaciones y Teoría de la Probabilidad. Se forman grupos de trabajo con alta productividad, consistencia y madurez, lo que finalmente conduce a que el Centro se convierta en el Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas (IIMAS) al ser aprobado por el Consejo Universitario, en su sesión extraordinaria del 10 de marzo de 1976. Del grupo de análisis surgen dos más: el de análisis funcional y el de ecuaciones diferenciales: dedicado a la investigación de operaciones, se origina el de análisis numérico. En 1997 se hizo entrega de las instalaciones del Edificio Anexo, espacio donde se ubica el Auditorio-IIMAS, los posgrados y la biblioteca-IIMAS, una de las bibliotecas especializadas más importantes del país en las áreas que maneja.

En el Instituto se ha llevado acabo una parte significativa de la investigación en Matemáticas Aplicadas, Probabilidad y Estadística, Análisis Numérico y Ciencias de la Computación que se realiza en el país. El IIMAS ha tenido y tiene un alto impacto en los sectores público y privado por medio de sus egresados y también a través de investigadores interesados en vincularse a la solución de problemas de interés nacional. Sus egresados tienen una presencia muy importante en la docencia, la investigación, la administración pública y la privada, tanto nacional como internacionalmente.

Además participa en cuatro programas de posgrado: Ciencia e Ingeniería de la Computación, Ciencias Matemáticas y de la Especialización en Estadística Aplicada, Ciencias de la tierra, así como el de Ingeniería.

4.3 Misión y objetivos del IIMAS.

4.3.1 Misión.

El IIMAS tiene como misión garantizar la existencia de grupos de investigación en Matemáticas aplicadas, Ciencia e Ingeniería de la Computación y los Sistemas, para lograr que estas disciplinas se mantengan actualizadas y se enriquezcan, contribuyendo de esta manera al conocimiento universal de las mismas. Además, se pretende que proporcionen, tanto al Subsistema de la Investigación Científica como al resto de la comunidad universitaria y a la sociedad, los medios necesarios para acceder a dichos conocimientos.

4.3.2 Objetivos.

- Realizar investigación científica original en Matemáticas Aplicadas, en Sistemas y en Ciencias e Ingeniería de la Computación.
- Participar, activamente, en los Posgrados con sede en el Instituto: Ciencia e Ingeniería de la Computación; Ciencias Matemáticas y de la especialización en Estadística Aplicada. Además, colaborar en los Posgrados en Ingeniería y en el de Ciencias de la Tierra, de los cuales forma parte como entidad académica.
- Participar en los programas de licenciatura de las facultades de Ciencias e Ingeniería, entre otras.
- Formar recursos humanos a través de proyectos de investigación.
- Divulgar el conocimiento científico.

4.3.3 Visión.

El IIMAS tiene la visión de ser un Instituto de investigación líder a nivel nacional e internacional en las disciplinas de las matemáticas aplicadas, ciencia e ingeniería de la computación y sistemas. Para ello, el Instituto deberá crecer tanto en su planta de investigadores como en su infraestructura y equipamiento para continuar realizando sus actividades de investigación básica y aplicada, formación de recursos humanos de alto nivel y divulgación. La diversidad de las disciplinas que se cultivan en el IIMAS da al Instituto la fortaleza para estudiar y proponer soluciones a problemas complejos nacionales e internacionales.

4.4 Situación actual.

Para poder cumplir con sus objetivos, misión y visión, el IIMAS está conformado por seis departamentos académicos coordinados por la Dirección, agrupados en dos áreas académicas: Matemáticas Aplicadas y Ciencia e Ingeniería de la Computación, como se puede observar en la figura 4.1.

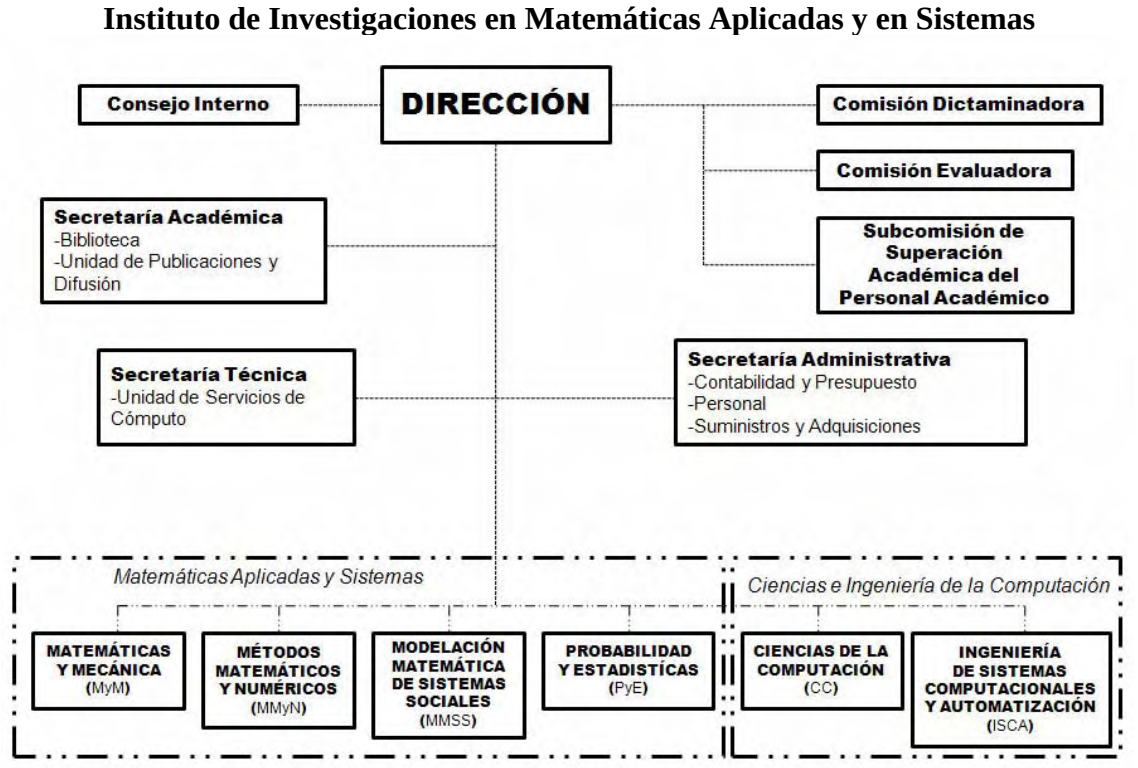

Figura 4.1. Organigrama del IIMAS.

La Dirección se apoya de tres Secretarías: Académica, Técnica y Administrativa. Además se auxilia de varios órganos colegiados: el Consejo Interno, la Comisión Dictaminadora, la Comisión Evaluadora del PRIDE[ii] y la Subcomisión de Superación Académica del Personal Académico. Apoya a varios posgrados y cuenta con servicios y recursos tales como: Biblioteca, la Unidad de Publicaciones y Difusión, y la Unidad de Servicios de Cómputo.

4.4.1 Comisiones.

También existen varias comisiones encargadas de salvaguardar la seguridad lógica y física del Instituto:

Consejo Interno

Este consejo se encarga de las decisiones que involucran a todo el Instituto, está conformada por el Director General, la Secretaria Académica y Técnica, las jefaturas de Departamento y un representante de cada Área.

Comisión Local de seguridad
Comisión encargada de la seguridad física del edificio del Instituto, la conforma el Director, un representante de cada área y la Secretaria Técnica.

Comisión Local de higiene y seguridad
Comisión encargada de la supervisión del mantenimiento y limpieza del Instituto y aspectos que puedan afectar la seguridad del personal, lo conforman un representante del sindicato, la Secretaria Técnica, Administrativa y un representante (Técnico Académico).

Comité Interno de cómputo
Se encarga de la seguridad física y lógica de la infraestructura de red, equipo de cómputo del Instituto, está conformado por la Secretaría Técnica, Académica y un representante de cada Departamento.

4.4.2 Personal en el Instituto.

El personal adscrito al Instituto está conformado por:
Personal Académico: incluye 54 investigadores, 38 técnicos académicos.
Personal Administrativo: 23 trabajadores en actividades secretariales y 57 trabajadores de apoyo administrativo entre vigilantes, intendentes y otros.
Está información se recabó hasta Octubre del 2007.

4.4.3 Infraestructura física.

El IIMAS tiene aproximadamente 7,200 metros cuadrados de construcción, la cual está integrada por un edificio principal con una superficie construida de 4,100 metros cuadrados, donde se ubican los Departamentos de investigación y las Unidades de Servicios de Cómputo y de Publicaciones y Difusión. Cuenta además con un edificio anexo con una superficie de 3,100 metros cuadrados donde se ubica el auditorio, las aulas de Posgrados y la Biblioteca.

4.5 Apoyo de la Dirección.

Para la revisión de la gestión de la seguridad de la información se requirió el apoyo de la Dirección del Instituto, esto se llevo a cabo mediante la Secretaría Académica y Técnica. Fue importante dicho apoyo, ya que de ello dependió el buen resultado de la revisión de algunos controles de seguridad de la información. Cabe señalar que una buena implementación del ISO hará que la seguridad se incorpore a la organización de manera transparente, algunos puntos que debe considerarse son:

1) Informar a la organización sobre la gestión de seguridad de la información
2) Difundir que la gestión de seguridad de la información es un complemento a sus actividades, desechar la idea que es un castigo o la suspensión de servicios.
3) Concienciar al personal sobre la seguridad de la información, a través de difusión de los beneficios de la seguridad de la información.
4) Incorporar seguridad de la información a la organización siendo orientada desde la Dirección.

4.6 Alcance de la revisión de seguridad de la Información.

Una de las labores iniciales es definir el alcance de la revisión de seguridad, esto se determinó junto con la Secretaría Técnica del Instituto, una planeación adecuada proporciona una implementación exitosa a medida que el proyecto se va realizando.

El alcance del programa de seguridad de la información que se aplicó basándose en el ISO 17799, fueron:

1. Se revisó la gestión de la administración de seguridad de información en el Instituto.
2. Se elaboró un análisis de riesgos, mediante la identificación de los activos, amenazas y vulnerabilidades en los sistemas de información.
3. Se propuso un diseño de un nuevo esquema de seguridad en la infraestructura de red.
4. Se elaboró una serie de Políticas Generales de Seguridad de la información, basándose en la revisión de la seguridad.
5. Se evaluó si el Instituto cumplió los 133 controles específicos de seguridad según el ISO 17799.

4.7 Administración de riesgos.

La razón principal de administrar los riesgos es proteger los recursos de una organización. Entender los riesgos permite a los administradores o dueños de los sistemas de información proteger y conocer el valor que tiene la información en la organización. Cabe aclarar que aunque con dicha administración de riesgos no se reducen estos a cero, la organización podrá evaluar la magnitud del riesgo y priorizar los recursos, además de mantener la funcionalidad de la misma.[iii]

4.7.1 Identificación de activos.

Un **activo** es una parte o componente de un sistema total de una organización, para la cual tiene un valor (dentro de la organización) y que requiere ser protegida. Todos los activos dentro del alcance fueron revisados (véase figura 4.2) en donde se muestra el Inventario de Activos del Instituto, el dueño del recurso, formato y clasificación, dicha información sirvió más adelante para el Análisis de riesgos. Según ISO 17799 cada activo debe estar claramente identificado y valorado por su dueño y se clasifica en:

Activos de información: bases de datos y archivos de datos, documentación del sistema, manuales de usuario, materiales de entrenamiento, procedimientos operativos de apoyo, planes de continuidad.
Documentos impresos: documentos impresos, contratos, lineamientos, documentos de la compañía, documentos que contienen resultados importantes de la organización.
Activos de software: Software de aplicación, software de sistemas, herramientas de desarrollo.
Activos físicos: Equipos de comunicación y computación, medios magnéticos u otros equipos técnicos.
Personas: Personal, clientes, suscriptores.
Servicios: Servicios de computación y comunicación, otros servicios técnicos.
Algunos datos que se utilizó en el presente caso de estudio se omitieron a petición de la Dirección y por cuestiones de seguridad.

Instituto de Investigaciones en Matemáticas Aplicadas y Sistemas

DISTRIBUCIÓN DE ACTIVOS Y SUS PROPIETARIOS

	ACTIVOS	PROPIETARIOS	FORMATO	CLASIFICACIÓN
No.	**Documentos**			
1	Oficios de la Dirección	Dirección, Secretaria Ténica y Académica	Papel	Reservado
2	Convenios	Dirección, Secretaria Ténica y Académica	Papel	Confidencial
3	Contratos	Secretaría Administrativa y jefatura de personal	Papel	Confidencial
4	Nómina	Secretaría Administrativa y jefatura de personal	Papel	Reservado
5	Resguardos de Bienes	Secretaría Administrativa, jefatura de suministros y adquisiciones	Papel y electrónico	Público
6	Reportes de Gastos e Ingresos	Secretaría Administrativa, jefatura de contabilidad y presupuesto	Papel	Confidencial
	Información			
7	Informes y estadísticas de los departamentos, secretarías y Dirección.	Los departamentos y áreas del Instituto.	Papel y electrónico	Reservado
8	Bitácoras de los servidores	Unidad de Cómputo, CC, ISCA, MYM, MMSS, PyE, Biblioteca	Papel	Confidencial
9	Proyecto de estadísticas de población y censos (INEGI)	Departamento de Probabilidad y Estadística	Papel y electrónico	Reservado
10	PREP (Programa de Resultados Electorales Preliminares) IFE	Departamento de Probabilidad y Estadística	Papel y electrónico	Reservado
11	Proyecto Universitario de Fenómenos Nolineales y Mecánica, **FENOMEC**	Departamento de Matemáticas y Mecánica	Papel y electrónico	Reservado
12	Reducción singular de sistemas hamiltonianos con simetría, Funciones polinomiales	Departamento de métodos matemáticos y numéricos	Papel y electrónico	Reservado
13	Proyecto DIME (Diálogos Inteligentes Multimodales en Español)	Departamento de Ciencias de la Computación	Papel y electrónico	Reservado
14	Imagenología ultrasónica, Percepción remota y modelación, Arquitecturas y algoritmos para cómputo de alto desempeño	Departamento de Ingeniería de Sistemas Computacionales y Automatiza	Papel y electrónico	Reservado
15	Proyectos sobre análisis de redes sociales	Departamento de Modelación Matemática de Sistemas Sociales	Papel y electrónico	Reservado

	Fijos	
16	Edificio	Dirección
17	UPS	Secretaría Administrativa
18	Equipo de Telecomuniccaiones (Switches, Hub's, ruteadores, Access Point, etc)	Secretaría Técnica
19	Conexión de fibra a DGSCA	Secretaría Técnica
20	Servidores	Unidad de Cómputo, CC, ISCA, MEM, MMSS, PyE, Biblioteca
21	Computadoras	Todos los departamentos y áreas del Instituto.
22	Laptop	Dirección, Secretaría Académica y Técnica, Jefes de Departamentos
23	Equipo de Videoconferencia	Secretaría Técnica
24	Proyector de datos (cañón)	Secretaría Técnica
25	Tarjetas inalámbricas	Secretaría Técnica
26	Impresora láser	Los departamentos y áreas del Instituto.
27	Impresora a color	Los departamentos y áreas del Instituto.
28	Aire acondicionado	Secretaría Técnica
29	Conmutador telefónico	Secretaría Técnica

	Servicios	
30	Servidor de Correo (leibniz)	Unidad de Cómputo
31	Servidor de Correo (fourier)	Unidad de Cómputo
32	Servidor de Correo (uxdea4)	Unidad de Cómputo
33	Servidor Web (volwer)	Unidad de Cómputo
34	Servidor de Base de Datos, DGB (magno)	Biblioteca
35	Servidor de Base de Datos (siac)	Secretaría Académica
36	Servidor de Biblioteca (ariel)	Biblioteca
37	Servidor de Video por Demanda (canal)	Unidad de Cómputo
38	Servidor de archivos (samba)	ISCA, MyM
39	Servidor de impresión	CC, ISCA, MMyN, EyA, MMSS, MEM, PyE, Biblioteca
40	Servidor espejo	CC
41	Firewall	CC, ISCA, EyA, PyE, MyM
42	Cluster	ISCA, MyM
43	Biblioteca	Dirección

ISCA: Ingeniería de Sistemas Computacionales y Automatización
MMyN: Métodos Matemáticos y Numéricos
EyA: Sección de Electrónica y Automatización
MMSS: Modelación Matemática de Sistemas Sociales
PyE: Probabilidad y Estadística
CC: Ciencias de la Computación
MyM: Matemática y Mecánica.

Figura 4.2 Listado de Activos - Propietario

4.7.2 Descripción del análisis de riesgos.

El análisis de riesgos es un proceso sistemático que permite determinar el valor de los activos en coordinación con los objetivos, misión y visión de la organización, las actividades de gestión de riesgos permiten elaborar un plan de seguridad que, una vez implementado, satisfaga los objetivos propuestos con el nivel de riesgo que se acepta.

Además proporciona un modelo del sistema en términos de activos, amenazas y vulnerabilidades, la piedra angular para controlar todas las actividades con fundamento.

Un activo como ya antes se había citado en el punto anterior, son los recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos.

El activo es esencial debido a que es la información que maneja el sistema; o sea los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes como:

- **Los servicios** que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- **Las aplicaciones** *(software)* que permiten manejar los datos.
- **Los equipos** *(hardware)* y que permiten almacenar datos, aplicaciones y servicios.
- **Los soportes de información** que son dispositivos de almacenamiento de datos.
- **Las redes de comunicaciones** que permiten intercambiar datos.
- **Las instalaciones** que resguardan equipos informáticos y de comunicaciones.
- **Las personas** que explotan u operan todos los elementos anteriormente citados.

El método del análisis de riesgos que se utilizó para la presente investigación, consistió en la elaboración de tablas, en la primera columna se enumera los activos. A continuación se reconoció cada activo en las siguientes dimensiones:

a) **Confidencialidad**: ¿Qué daño causaría que lo conociera quien no debe? La cual se refiere a proteger toda la información que se maneja en el IIMAS tanto del personal como de los investigadores, por medio de la red se transfieren datos de reportes de desarrollo de investigaciones, datos de nómina y asuntos de personal de acceso, la finalidad es proteger la información que viaja por la red y que una tercera persona intente capturar los datos o manipularlos según su conveniencia.

b) **Integridad**: El servicio de integridad es el que permite que la información sea adecuada, completa y auténtica en el momento de ser procesada, presentada, guardada o transmitida. En el caso del IIMAS transmitir datos de control de cualquier asunto, relacionado con nómina o aspectos de investigaciones, no deben llegar manipulados ya que las consecuencias finales podrían ser perjudiciales a la organización. En algunos casos mantener y garantizar esta característica es más importante que la confidencialidad.

c) **Disponibilidad**: Como su nombre lo indica la disponibilidad se refiere a que todos los servicios puedan prestar en determinado momento. ¿Qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios

Se procedió a valorar cada activo una vez que se determinó qué dimensiones de seguridad interesan. La valoración es la determinación del costo que supondría salir de una incidencia que perjudicaría al activo.

Dicho análisis se realizo mediante tablas, se utilizó como guía MAGERIT[iv]; se trata de un método formal para realizar un análisis de riesgos y recomendar los controles necesarios para minimizarlos. MAGERIT se basa en una aproximación cualitativa que intenta cubrir un amplio espectro, gracias a un enfoque orientado a la adaptación del mecanismo dentro de diferentes entornos, generalmente con necesidades de seguridad y nivel de sensibilidad también diferentes.

Para realizar la valoración se utilizo la siguiente escala:

	Valor
A : Alta	6
M: Medio	3
B: Bajo	1

El siguiente paso consistió en determinar las amenazas que pueden afectar a cada activo. Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasar a los activos y causar un daño.

Hay accidentes naturales (terremotos, inundaciones, etc.) y desastres industriales (contaminación, fallas eléctricas, etc.) ante ellos los activos son víctimas pasivas; pero no por ser pasivos hay que permanecer indefensos. Hay amenazas causadas por las personas, bien errores o ataques intencionados, etc.

Una vez determinado que tipo de amenazas puede perjudicar a un activo, se evaluó la frecuencia de la posible ocurrencia con los siguientes valores:

100	Muy frecuente	A diario
10	Frecuente	Mensualmente
1	Normal	Una vez al año

Y por último la vulnerabilidad que se define como la posibilidad de ocurrencia de la materialización de una amenaza sobre un activo. Y se utilizo la siguiente escala:

	Definición
Bajo	0 – 40% posible ocurrencia de la vulnerabilidad durante un año.
Medio	41- 75% posible ocurrencia de la vulnerabilidad durante un año.
Alto	76% al 100% posible ocurrencia de la vulnerabilidad durante un año.

Cabe señalar que el análisis se realizó en conjunto con la Secretaria Técnica del Instituto que es el encargado de toda la Infraestructura de la dicha dependencia.

A continuación en la Tabla 4.3, se describen los riesgos de los activos del Instituto ya mencionados.

Instituto de Investigaciones en Matemáticas Aplicadas y Sistemas

		Valor						
	Activos	**Confidencial**	**Integridad**	**Disponibilidad**	**Amenazas**	**Posible Ocurrencia**	**Vulnerabilidad**	**Posible Ocurrencia**
1	Oficios de la Dirección	6	6	3	Pérdida de documento, retraso en la entrega	1	Error de captura, deficiencia en el envío	B
2	Convenios	3	6	3	Pérdida del documento, alteración, privacidad	1	Datos incompletos, error de captura	B
3	Contratos	6	6	6	Alteración, pérdida del documento, datos incorrectos	1	Datos incompletos, error de captura, deficiencia en la impresión	B
4	Nómina	6	6	6	Fraude, falta de seguridad en el recibimiento y envío, modificación incorrecta	1	Deficiencia envío	B
5	Resguardos de Bienes	3	6	3	Modificación incorrecta	1	Errores de captura	B
6	Reportes de Gastos e Ingresos	6	6	6	Alteración y errores al procesarlo, mala interpretación, poco detalle	1	Error de captura, acceso no autorizado	B
7	Informes y estadísticas de los departamentos, secretarías y Dirección	1	6	3	Alteración de la información, falsificación, privacidad	1	Error de captura, datos incompletos, control de documentos	B
8	Bitácoras de los servidores	6	6	6	Falsificación, alteración,pérdida de datos	1	Acceso no autorizado, personal no calificado	B

		Valor						
	Activos	**Confidencial**	**Integridad**	**Disponibilidad**	**Amenazas**	**Posible Ocurrencia**	**Vulnerabilidad**	**Posible Ocurrencia**
9	Proyectos de Investigación							
	Documentación	6	6	3				
10	Sistemas	6	6	6	Alteración de la información, pérdida de los documentos, falla en los sistemas.	1	Uso inadecuado, personal no calificado, controles de acceso	B
11	Publicaciones	3	6	6				
12	Equipo de Telecomunicaciones (Switches, hub's, ruteadores, Acess Point, etc)	1	6	6	Falla en el hardware o software, acceso no autorizado, polvo, humedad	1	Personal no calificado	B
	Conexión de fibra a DGSCA	6	6	6	Falla en la red de la UNAM, polvo, robo, humedad	1	Falla del cableado	B
13	Servidores	6	6	6	autorizado, falta de mantenimiento	1	de respaldos y/o actualizaciones	B
	Computadoras							
	Investigadores	6	6	6		1		B
	Administrativos	3	6	6	Falla de hardware o software y de			
14	Alumnos	1	3	6	mantenimiento, robo, virus informático		Uso inadecuado	
	Laptop							
15	Servicios	1	6	6		1		M
16	Investigadores	6	6	6	Polvo, robo, humedad, falla de hardware, virus informático		Falla del equipo	

		Valor						
	Activos	**Confidencial**	**Integridad**	**Disponibilidad**	**Amenazas**	**Posible Ocurrencia**	**Vulnerabilidad**	**Posible Ocurrencia**
17	Tarjetas inalámbricas	1	3	1	Falla de hardware, robo	1	Error de operación	B
18	Impresora láser	1	6	3	Polvo, robo, humedad	1	Utilizado por personal no capacitado	B
19	Impresora a color	1	6	6	Polvo, robo, humedad	1	Utilizado por personal no capacitado	B
20	Aire acondicionado Laboratorios Oficinas	1 1	6 3	6 3	Falla técnica, falta de mantenimiento	1	Uso inadecuado	B
21	Conmutador telefónico	1	6	6	Falla técnica, falta de mantenimiento	1	Uso inadecuado	B
22	Servidor de correo (leibniz)	6	6	6	Virus, falla del equipo	1	Sistema operativo y/o software no actualizado	B
23	Servidor de correo (fourier)	3	6	6	Virus, falla del equipo	1	Sistema operativo y/o software no actualizado	B
24	Servidor de correo (uxdea4)	6	6	3	Virus, falla del equipo	1	Sistema operativo y/o software no actualizado	B

		Valor						
	Activos	**Confidencial**	**Integridad**	**Disponibilidad**	**Amenazas**	**Posible Ocurrencia**	**Vulnerabilidad**	**Posible Ocurrencia**
25	Servidor web (volwer)	3	6	3	Virus, falla del equipo	1	Sistema operativo y/o software no actualizado	B
26	Servidor de base de datos, DGB (magno)	3	6	6	Fallas en la red universitaria, acceso no autorizado, errores de captura, falta de respaldos	1	Mala administración, utilizado por personal no autorizado y/o capacitado	B
27	Servidor de base de datos (siac)	6	6	6	Fallas en la red universitaria, acceso no autorizado, errores de captura, falta de respaldos	1	Mala administración, utilizado por personal no autorizado y/o capacitado	B
28	Servidor de Biblioteca (ariel)	3	6	3	Fallas en la red universitaria, acceso no autorizado	1	Uso inadecuado	B
29	Servidor de video por demanda (canal)	1	6	6	Fallas en la red.	1	Mala administración, utilizado por personal no autorizado y/o capacitado	B
30	Servidor de archivos (samba)	3	6	3	Virus informático, falta de mantenimiento, fallas del equipo, accesos no autorizados	1	Mala administración	B
31	Servidor de impresión	1	6	6	Falla técnica, falta de mantenimiento	1	Uso inadecuado	B
32	Servidor espejo	6	6	6	Falla técnica, falta de mantenimiento, virus informático	1	Mala administración, acceso no autorizados	B
33	Firewall	6	6	6	Polvo, falta de mantenimiento, falta de energía	1	Sistema operativo no actualizado	B

Figura 4.3 Descripción de riesgos

4.7.3 Determinación de la vulnerabilidad a las amenazas.

Para determinar la vulnerabilidad (cuánto perjudica el que se pierda o manipule determinado tipo de información), primero se asignó un nivel de riesgo a cada amenaza, para ello se debió combinar la probabilidad de que la amenaza ocurra con la debilidad de la aplicación hacia dicha amenaza (carencia de recursos que no permitan el acceso a quien no lo debe de tener).

La localización de los edificios del Instituto, el manejo de la información, las relaciones laborales, el manejo de los sistemas entre otras fueron las razones que llevaron a identificar las diversas actividades que en cada área se desempeñan para poder determinar el riesgo que corren y según lo observado:

En las áreas de INFORMÁTICA se encuentran equipos tales como: Computadoras personales, estaciones de trabajo, servidores, switches. Su principal actividad es compartir recursos de software y de hardware. Es responsable de las comunicaciones confiables de voz y datos, administra y restaura fallas en la red que trabaja sobre plataforma LINUX, da mantenimiento a los equipos de cómputo, mantiene y restaura cada uno de los servidores. Elabora y da mantenimiento a los diversos sistemas que tiene el Instituto, apoya a los investigadores en diversas aplicaciones, entre otras actividades.

Las actividades del área ADMINISTRATIVA en relación a seguridad física: Supervisa el control de acceso a los empleados, visitantes, alumnos y clientes, registro de acceso a instalaciones así como la seguridad en instalaciones. En el Almacén se concentra una gran cantidad de información de entradas y salidas, esta área requiere compartir información con el Administrativo. En la Dirección general y Administrativa: existe una gran cantidad de información, mantienen enlaces a equipos centrales para manejo de información presupuestal y contable. Se elabora la generación de información administrativa, de adquisiciones, personal, comercialización, servicios generales, auditoria, correspondencia y archivos, organización y métodos, además se requiere un alto volumen de comunicación de voz y necesita compartir información con administración, y por último el área de mantenimiento: da seguimiento de órdenes de trabajo y coordina tareas de grupo de trabajo.

En el área de INVESTIGACIÓN. Consideramos que el Instituto tiene una concentración de 54 investigadores y equipos de apoyo para ellos, llevan a cabo intercambio de datos con el exterior, realizan búsquedas de información en banco de datos internacionales y requiere de equipos personales.

Los documentos y sistemas que desarrollan es el punto medular a proteger en el Instituto, toda la información que manejan son resguardadas por el dueño de cada activo (publicación, sistema, documentos impresos o electrónicos) y aún cuando cada investigador protege mediante respaldos y solamente tienen acceso a dicha información las personas involucradas, los responsables de Informática utilizan mecanismos (firewalls, segmentación de redes, detector de intrusos y otros elementos de seguridad de la información) para su protección.

4.7.4 Conclusiones del análisis de riesgos.

Según la tabla 4.3, se identificaron las vulnerabilidades y la posibilidad de ocurrencia de las amenazas descritas sobre un activo, después del análisis se obtuvieron riesgos bajos, pero aún así fue importante considerar en mejorar los procedimientos, ya que a través de este análisis se hicieron las siguientes observaciones:

- Involucrar al personal sobre el conocimiento en sus actividades sobre la seguridad de la información, y enfatizarlo al personal de vigilancia e intendencia.
- Actualizar la documentación de la infraestructura de red.
- Ofrecer pláticas sobre temas de seguridad de la información al personal del Instituto.
- Diseñar un plan de capacitación sobre temas de seguridad de la información, según las necesidades del personal.

4.7.5 Selección de Opciones Apropiadas de Tratamiento del Riesgo.

Una vez que se identificaron y evaluaron los riesgos, el próximo paso fue evaluar qué acción más apropiada tomar para tratar los riesgos. La decisión debe ser tomada basada en los activos involucrados y su impacto en la organización, este paso se realizo junto con la Secretaría Técnica.

El estándar ISO 17799, requiere que la organización en relación al tratamiento del riesgo siga cuatro posibles acciones:
• Aplicación de controles apropiados para reducir los riesgos. Seguir el modelo del ISO.
• Aceptar objetivamente los riesgos partiendo del supuesto que satisfacen la política de la organización y su criterio para la aceptación del riesgo.
• Evitar los riesgos
• Transferir el riesgo asociado a otras partes.

Después de varias reuniones se desarrollaron dos controles para tratar los riesgos de seguridad detectados:
1) Políticas Generales de Seguridad de la Información.
2) Propuesta de un esquema de seguridad en la infraestructura de red del Instituto.
Y se describen en el capítulo 5.

4.8 Revisión de seguridad de la información.

Una vez concluido el análisis de riesgos, se continuó con la revisión de la seguridad del Instituto a través de un listado de 11 dominios junto con los 133 controles específicos del ISO 17799, se hizo mención a cada control, después de una serie de observaciones realizadas a través de entrevistas y lecturas de documentos, se mencionó si cumple o no con dichos controles, además se propuso una evaluación final de lo que requiere el Instituto para cumplir con dicho estándar. La revisión se encuentra en el Apéndice A de está tesis

4.9 Conclusiones

Iniciar con un plan de gestión de la seguridad de la información es desarrollar una serie de puntos estratégicos para su implementación y mantenimiento. Un análisis de riesgos es una de las partes primordiales que sugiere la ISO 17799 y necesaria para una certificación, además ayuda a la organización a conocer sus activos, riesgos, amenazas y vulnerabilidades, que pueden afectarla.

En este capítulo se llevó a cabo la revisión de seguridad de la información del IIMAS, se hizo referencia a la historia dentro de la UNAM, así mismo con la misión y visión. Además de la estructura organizacional, las áreas, departamentos, comisiones, personal, etc. que la conforman, destacando que estos puntos son importantes para iniciar la implementación del estándar.

El análisis realizado, arrojó una serie de activos, amenazas y vulnerabilidades que sirvieron al Instituto para visualizar los riesgos que pueden tener, por ejemplo: desde un acceso no autorizado al edificio hasta el robo de información de una publicación de algún investigador. Asimismo, dicho análisis servirá de referencia para posibles eventos que puedan afectar a la seguridad del Instituto.

Y por último, se estructuraron a través de una listado los dominios y controles del estándar para su revisión sobre el cumplimiento o no de dichos controles.

Dentro de dicha revisión de los 133 controles específicos y del análisis de riesgos se concluyó desarrollar dos controles como parte del caso de estudio y de los requerimientos del Instituto en el siguiente capítulo.

---

[i] http://www.iimas.unam.mx

[ii] Programa de Primas al Desempeño del Personal Académico de Tiempo Completo de la UNAM.

[iii] Peltier, Thomas R., Information Security Risk Analysis, Aurebach Publications, 2001.

[iv] Metodología de Análisis y gestión de Riesgos de los sistemas de Información de las Administraciones públicas http://www.csi.map.es/csi/pg5m20.htm

Controles Específicos Propuestos

5.1 Introducción.

Una vez realizado los requerimientos a partir de la identificación de los activos y la valoración de los riesgos, se deben seleccionar e implementar los controles.

Un control se puede definir como un conjunto de acciones, documentos, medidas a adoptar, procedimientos y técnicas, las cuales reducen los riesgos de seguridad de las actividades vulnerables dentro de la organización. Además de seleccionar controles teniendo en cuenta el valor de la implementación ya que muchas veces la organización debe evaluar el costo-beneficio, es decir si el control para algún riesgo ayudará a reducir alguna pérdida que llevará a producir alguna violación de seguridad y ocasionar una mala imagen ante sus usuarios.

Los controles son aplicables a la mayoría de las organizaciones, pero se debe tener en cuenta que si bien, todos los controles mencionados son importantes, la relevancia de cada uno de ellos debe ser determinada teniendo en cuenta los riesgos específicos que afronta la organización.

Una vez finalizado el inventario de activos y análisis de riesgos en el capítulo 4, se decidió en coordinación con la Secretaría Técnica desarrollar dos controles de los 133 que especifica el ISO, el primer control se desarrolló por considerarse dentro de un marco estratégico para la Dependencia, el segundo por la necesidad de administrar y controlar los que sucede en la red, mantener la seguridad en los sistemas y aplicaciones a través del conocimiento de la información que circula por ella.

Estos controles son:

***Control**:*
5.1. Política de seguridad de la información
10.6. Gestión de seguridad en la red.

El primer control Políticas de seguridad de la Información, se realizo debido a la existencia de reglamentos y lineamientos aislados de seguridad sin contar con un documento general sobre Políticas de seguridad, es por esto que se propusieron 18 políticas (véase Apéndice B).

El segundo control sobre la gestión de seguridad en la red, se diseñó a partir del interés del Instituto por tener sistemas de información seguros, se estudió cuáles son las mejores alternativas para aprovechar al máximo las mezclas de tecnologías, se utilizaron firewalls que constituyen actualmente como una de las formas más confiables además de IDS, IPS, Proxy, DHCP, DNS que se expone en este capítulo.

5.2 Política de Seguridad de la Información.

Para estos temas y para ser más claros, se respetará la numeración que el estándar le asigna a cada uno de los controles:

5.- POLITICA DE SEGURIDAD[i]
5.1. Política de seguridad de la información

OBJETIVO: Proveer el apoyo de la administración de la seguridad de la información desde nivel de la Dirección, establecer políticas claras y mantener la información de la seguridad en toda la organización.

5.1.1. Documentación

La implementación de las políticas de seguridad de la información se llevó a cabo mediante la identificación de los activos de la organización, además de los responsables de dichos activos. Una vez identificados se investigó y analizó los riesgos que tienen, además de las diversas amenazas y vulnerabilidades. A partir de ese punto se inició con las políticas de seguridad para el Instituto, se desarrolló junto con la Secretaría Técnica, que pondrá a consideración del Consejo Interno para su aprobación. Cabe mencionar que dichas políticas se desarrollaron a nivel estratégico.

Cada política contiene:

- Objetivo
- Alcance
- Descripción de la política
- Responsabilidades
- Sanciones

5.1.2. Revisión de la política de seguridad de la Información.

El mantenimiento y la revisión de las políticas en principio serán llevadas a cabo por la Secretaría Técnica junto con el Consejo Interno, quienes aprobarán las mismas.

Está revisión se hará en periodos definidos por la Secretaría Técnica o cuando ocurriera algún evento o incidente de seguridad el cual obligué a modificar y/o mejorar dichas políticas. Debido a que el Instituto tiene varias áreas y departamentos los cuales podrán retroalimentar, realizar revisiones, recomendaciones para dicho documento y que podrán reportar en las reuniones del Consejo Interno.

A continuación se listan los once dominios de control del ISO 17799, dentro de cada área se enumeró las políticas de seguridad de acuerdo al rubro; que se realizaron a partir del caso de estudio (véase Apéndice B)

- **5-POLÍTICA DE SEGURIDAD**

Se desarrollo un grupo de 18 Políticas de seguridad.

- **6- ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**

POLITICA 9: RESPALDO Y BORRADO DE INFORMACIÓN. **POLITICA 17**: SEGURIDAD PARA TERCEROS.

- **7- CLASIFICACIÓN Y CONTROL DE ACTIVOS**

POLITICA 4: CLASIFICACION DE LA INFORMACIÓN.

-

- **8- SEGURIDAD DEL PERSONAL**

POLITICA 2: ROLES Y RESPONSABILIDADES **POLITICA 3**: SEGURIDAD EN EL PERSONAL

.

- **9- SEGURIDAD FÍSICA Y AMBIENTAL**

POLITICA 5: SEGURIDAD FÍSICA Y AMBIENTAL **POLITICA 7**: MONITOREO DE SEGURIDAD **POLITICA 8**: PROTECCIÓN DE REDES INTERNAS **POLITICA 13**: PROTECCIÓN DE EQUIPO DE CÓMPUTO **POLITICA 14**: EQUIPOS PORTÁTILES

- **10 -ADMINISTRACIÓN DE LAS COMUNICACIONES Y OPERACIONES**

POLITICA 6: INCIDENTES DE SEGURIDAD **POLITICA 10**: ANTIVIRUS Y CODIGO MALICIOSO

-

- **11- CONTROL DE ACCESO**

POLITICA 11: AUTENTICACIÓN Y CONTROL DE ACCESOS. **POLITICA 12**: USUARIOS Y CONTRASEÑAS

-

- **12- ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**

POLITICA 15: DESARROLLO Y MANTENIMIENTO DE SISTEMAS

-

- **13- ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**

POLITICA 1: ADMINISTRACIÓN DE RIESGOS

-

- **14- ADMINISTRACIÓN DE CONTINUIDAD DEL NEGOCIO**

POLITICA 18: ADMINISTRACIÓN DE LA CONTINUIDAD.

-

- **15- CONFORMIDAD (CUMPLIMIENTO)**

POLITICA 16: LICENCIAMIENTO DE SOFTWARE

.

SANCIONES

5.3 Administración de comunicaciones y operaciones.

Este control contiene un grupo de treinta y dos recomendaciones, es el más extenso y específicamente se trabajó en el control específico:

10.6 Gestión de seguridad de la red

Los dos controles que conforman este apartado hacen hincapié en la necesidad de administrar y controlar lo que sucede en la red, es decir, implementar todas las medidas posibles para evitar amenazas Se deben implementar controles técnicos, que evalúen permanentemente los servicios que la red ofrece, tanto propios como de terceros.

Para llevar a cabo el control se diseñó un nuevo esquema de la infraestructura de red a partir de la situación actual (véase Figura 5.3).

5.3.1 INFRAESTRUCTURA DE RED EN EL IIMAS.

5.3.1.1 Descripción de la red.

El Instituto tiene dos edificios, el principal está conformado de cuatro niveles. En la zona norte del primer piso se encuentra la Dirección, las Secretarias Académica, Técnica y Administrativa y en la zona sur el Departamento de Probabilidad y Estadística. Al centro de este piso se ubica el cuarto de red, con los equipos de Telecomunicaciones necesarios para que el Instituto tenga conexión a REDUNAM e Internet, a través de fibra óptica.

En el segundo piso se localiza el Departamento de Matemáticas y Mecánica en la zona sur, en la zona norte se ubica el Departamento de Modelación Matemática de Sistemas Sociales, la Unidad de Servicios de Cómputo y la Unidad de Publicaciones y Difusión. También tiene un cuarto de red para brindar servicio al segundo piso.

El tercer piso está conformado, en la zona sur, por la Sección de Electrónica y Automatización, el Departamento de Métodos Matemáticos y Numéricos, y en la zona norte por el Departamento de Ingeniería de Sistemas Computacionales y Automatización. En este piso también se encuentra un cuarto de red que da servicio al tercer y cuarto nivel.

Se cuenta con servicio de Voz sobre IP en la zona sur del primer piso y en la zona norte del segundo piso.

El sistema de comunicaciones tiene cableado estructurado, que utiliza fibra óptica en su vertical para intercomunicar los tres cuartos de red, la distribución horizontal en cada piso tiene un cableado que cumple con las normas y estándares de comunicación.

El edificio anexo tiene tres pisos, en planta baja se encuentre la Hemeroteca y Auditorio, en el primer piso la Biblioteca, en el segundo piso aulas del Posgrado de Ciencias Matemáticas y Especialidad en Estadística y en el tercero se encuentran las aulas del Posgrado en Ciencias de la Computación. (Véase figura 5.1 y 5.2)

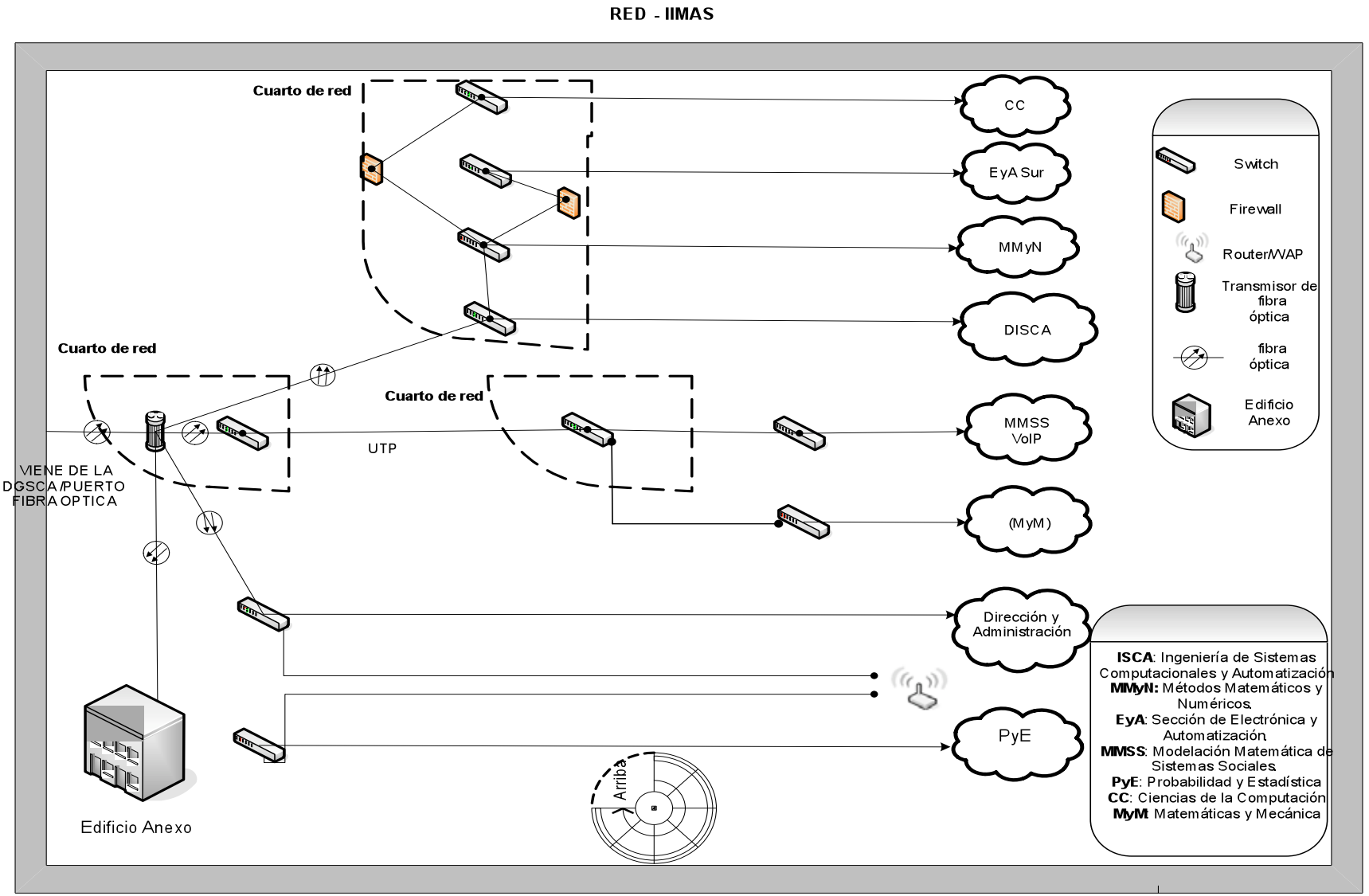

Figura 5.1. Estructura actual de red del IIMAS

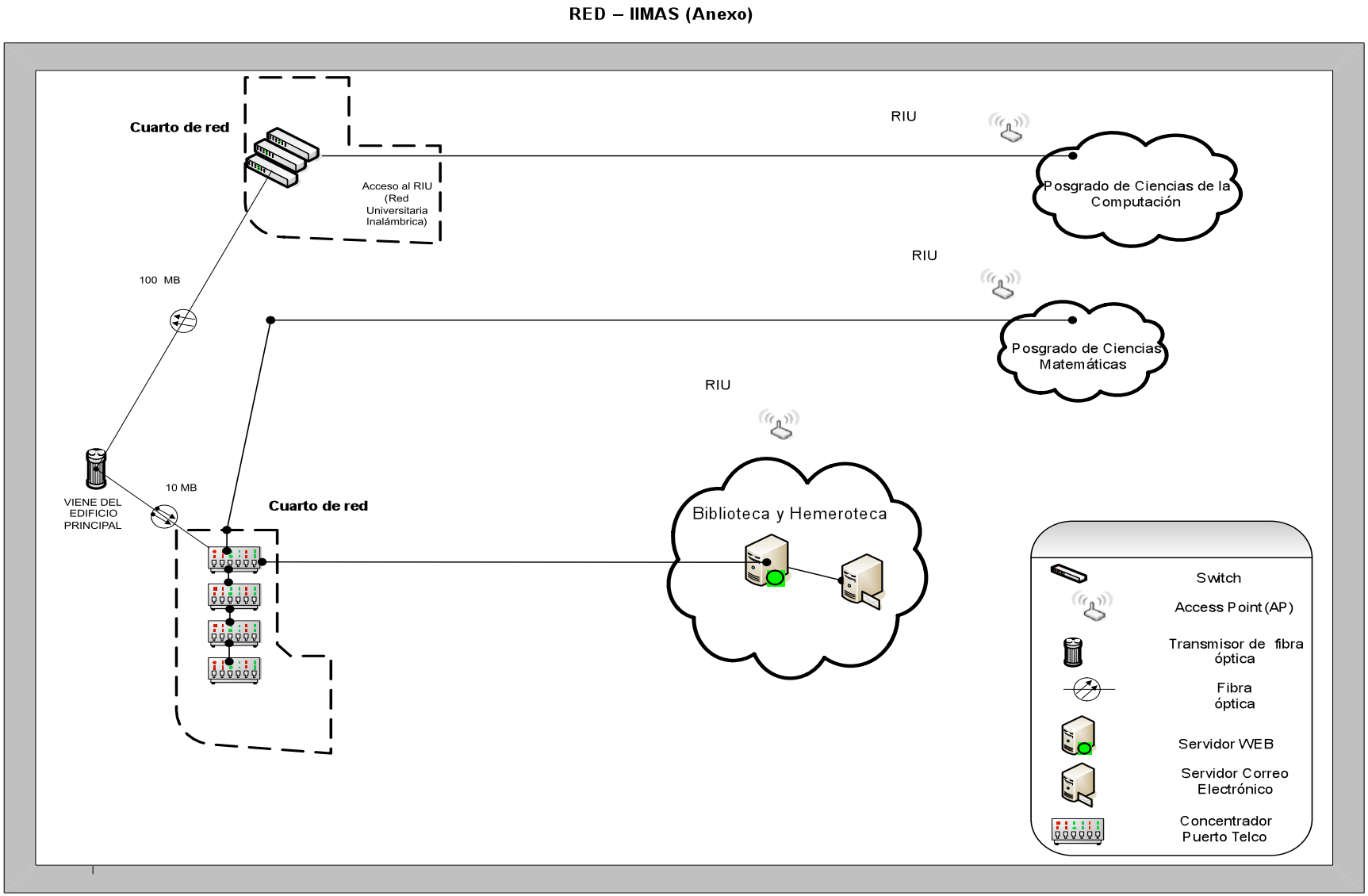

Figura 5.2. Estructura de red del IIMAS (Anexo)

5.4 Propuesta de esquema de seguridad en la red.

A partir de las dos figuras anteriores, surgió la necesidad de implementar un esquema de seguridad de la información en el Instituto, capaz de apoyar y complementar con lo que se tenia instalado y así cubrir los requerimientos de los usuarios.

El esquema junto con las políticas de seguridad se diseñó para implementar seguridad en el Instituto y así obtener un modelo confiable. A través de la identificación de zonas desmilitarizadas [ii], estándares de programación segura, configuración de los firewalls, IDS, IPS, apoyará la respuesta de incidentes, así como mitigará los riesgos de un ataque interno o externo.

De acuerdo al caso de estudio y a varias pruebas en el Instituto, además de la experiencia profesional en el rubro de la seguridad informática, se concluyó utilizar el sistema operativo OpenBSD por ser un sistema seguro y robusto y que se acopló con las necesidades de la Dependencia (véase Capítulo 3).

El aumento y la gravedad de los ataques hoy en día hacen que los sistemas de detección de intrusos sea una parte indispensable dentro de la seguridad. En efecto, cualquier organización que no esté buscando ser objeto de un intento de intrusos, no tiene idea acerca de cuáles son las amenazas que están allí. Por lo cuál también se propone un IDS. Una vez implementado, el sistema reportará las amenazas que pueden respaldar las sospechas de que la red del Instituto está siendo atacada, además, entender la frecuencia y los tipos de ataques permitiéndole a la organización determinar los controles de seguridad que se deben adoptar.

5.4.1 DISEÑO DEL ESQUEMA DE SEGURIDAD.

Basados en un esquema de seguridad similar a la del Centro COAPA de la DGSCA, se propuso una representación gráfica dividida en subredes que contienen equipos de diversas áreas y/o departamento del Instituto, de acuerdo con la Secretaría Técnica y que se concluyó después de varias reuniones.

A continuación se observa en la figura 5.3 el esquema de seguridad propuesto, se identificó el enlace de la DGSCA, ya que es un punto importante dentro de la infraestructura de red; se evaluó configurar un firewall transparente, el cual resguardará la red del IIMAS contra cualquier amenaza de la red externa, este dispositivo no tiene una dirección IP no se puede acceder de forma remota y ni la red interna y/o externa lo identifican, por lo mismo que se configuró sin dirección.

De igual modo se instaló y configuró un firewall NAT con cinco interfaces, cada una tiene configurado una subred con direcciones IP's distintas, las subredes se creó según los activos, recursos, servicios, personas y seguridad del Instituto:

1) Servicios: son los equipos que almacenan los servicios como IDS; IPS, DNS, DHCP, estos sistemas requieren ser localizados en la infraestructura de red con una seguridad, que permita sólo a los administradores.
2) Subred de aulas: Por ser parte de los objetivos del Instituto de mantener la seguridad de la información, se creo está subred, para localizar los equipos que requieren cierto nivel de seguridad para sus usuarios.
3) Oficinas: Otra subred que contiene equipos e información necesarias para la misión y visión de la Dependencia por lo cual requiere cierto nivel de seguridad y confiabilidad.
4) Área de investigación y laboratorios: en está subred se localiza los recursos de los investigadores, desarrolladores del Instituto.
5) Servidores: Como parte de los servicios que ofrece el Instituto, como pueden ser WEB, correo electrónico, etc. en está subred se localizan todos los servidores con información de los usuarios, de difusión, etc. Algunos de los servidores son públicos y otros sólo para usuarios de la red interna.

Cada subred se configuró con direcciones IP's no homologas,[iii] por el Firewall NAT, además de la protección de los firewalls que ya existen.

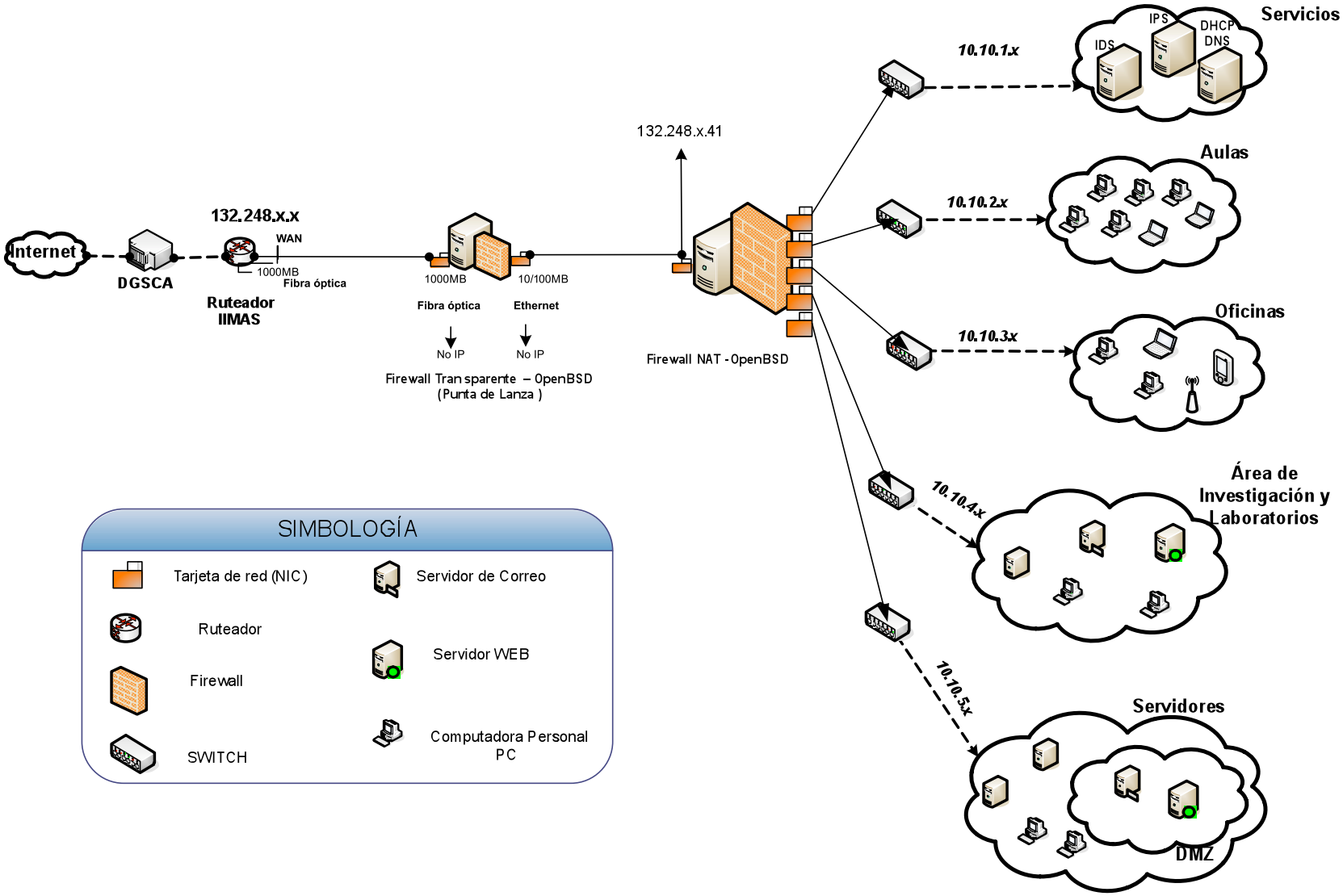

Figura 5.3. Esquema propuesto para la seguridad en la red

5.4.2 Objetivo de la propuesta técnica.

Mantener la red de datos en zonas seguras, las cuales tienen como prioridad proteger la información así como mantener la confidencialidad de la misma, recalcando en el esquema de seguridad que es confiable y en plataformas seguras.

5.4.3 Alcance de la propuesta.

Proteger la red, ante cualquier incidente de seguridad que pueda realizarse de una forma externa o interna, así como tener los elementos necesarios para realizar las verificaciones pertinentes, la cuales aumentan día a día el nivel de seguridad, bajo políticas y procedimientos que ya se han señalado en otros capítulos.

5.5 Implementación del esquema de seguridad.

La implementación del esquema de seguridad propuesto de la tabla 5.3, se divide en 5 fases que se describen en la tabla 5.4.

FASE 0	Se identificó y seleccionó la red LAN y WAN del IIMAS, además se asignó un direccionamiento homologado y no homologado (Ruteo, Mascaras de Red, etc.)
FASE 1	Se determinó el Hardware que soporte del sistema operativo OpenBSD, en cada una de las zonas.
FASE 2	Se estableció el número de dispositivos que se tendrá como firewalls, así como las redes o segmentación que se realizara de forma interna en la red del Instituto.
FASE 3	Se diseñó la arquitectura de seguridad en TI bajo la plataforma de OpenBSD
FASE 4	Se implementó el esquema de seguridad en TI bajo la plataforma de OpenBSD
FASE 5	Se aplicó las políticas de seguridad así como los controles para el seguimiento de la arquitectura de seguridad, la cual tendrá validez y reconocimiento por los directivos del IIMAS.

Tabla 5.4 Descripción de la fases de implementación del esquema de seguridad

5.5.1 Descripción de las fases

FASE 0
La Fase 0 tuvo como objetivo identificar las redes que se involucraron en el diseño de seguridad del IIMAS, como se muestra en las siguientes tablas (5.5 y 5.6)

Identificación de la red WAN

Segmento de red	132.248.51.x
Mascara de Red	255.255.255.0
Puerta de enlace (Router)	132.248.x.x
DNS	132.248.204.1
Tipo de enlace o ancho de banda	1GB

Tabla 5.5

Identificación de la red LAN

Segmento de red	10.10.x.x
Mascara de Red	255.255.255.0
Puerta de enlace (Router)	10.10.x.x
DNS	10.10.10.10
Tipo de enlace o ancho de banda	10/100Mb

Tabla 5.6

Fue importante identificar los puntos de contacto de la Red WAN de la UNAM, ya que tiene relación directa para cualquier evento que se pudiera presentar en la configuración e incidente de seguridad de acuerdo a las políticas y procedimientos.

La interpretación de las tablas se muestra en la siguiente figura 5.7 para su comprensión y asignación de segmentación en la red LAN del IIMAS, en la cual se pudo identificar cada segmento y configuración por dispositivo asignado.

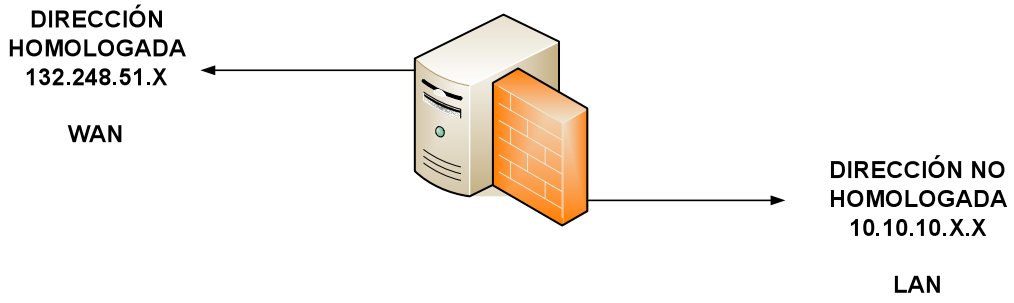

Figura 5.7

FASE 1
Se determinó el hardware que soporté el soporte al sistema operativo OpenBSD, en cada una de las zonas. Tabla 5.8 y 5.9

Firewall (punta de lanza)	
CPU	Pentium IV a 1GHz o superior
Memoria Ram	512 o Superior
2 tarjeta de red	Modelo 3Com de preferencia.

Tabla 5.8

Firewall, NAT	
CPU	Pentium IV a 1GHz o superior
Memoria Ram	512 o Superior
5 tarjetas de red	Modelo 3Com de preferencia.
OPCIONAL: 2 tarjeta de red (Quad)	Contenga drivers para OpenBSD[iv]

Tabla 5.9

El mouse y teclado se utilizó en su configuración inicial, posteriormente mediante consola serial y administración remota.

FASE 2
Se estableció el número de dispositivos (tarjeta de red) del firewall, así como las redes o segmentos (véase Figura 5.3) en la red interna del IIMAS, como se observa en las tablas 5.10 al 5.15

Red WAN del IIMAS	
Direccionamiento homologado	132.248.51.x
Identificación de la red UNAM	
IP Homologada del Firewall NAT : 132.248.51.41 Dirección del ruteador o puerta de enlace de la UNAM: 132.248.51.254 Netmask o mascara de red: 255.255.255.0 Servidores de nombre (DNS): 132.248.204.1 y 132.248.10.2 Identificador de red: xl0	

Tabla 5.10

Red LAN del IIMAS, Firewall NAT / Zona Servidores (DNS, IPS, DHCP)	
Direccionamiento no homologado	10.10.1.x
Identificación de la red IIMAS	
IP Homologada del Firewall NAT Interna para la interface 1: 10.10.1.1 Dirección del ruteador o puerta de enlace de la UNAM: 10.10.1.254 Netmask o mascara de red: 255.255.255.0 Servidores de nombre (DNS): 10.10.1.1 Área: Equipos para DHCP, DNS, IDS e IPS Identificador de red: xl1	

Tabla 5.11

La siguiente área contiene servicios necesarios para la implementación y administración del Firewall NAT, además de detectores de intrusos que complementaron el diseño de seguridad de la red.

Red LAN del IIMAS, Firewall NAT / Zona aulas	
Direccionamiento no homologado	10.10.2.x
Identificación de la red IIMAS	
IP Homologada del Firewall NAT Interna para la interface 2: 10.10.2.1 Dirección del ruteador o puerta de enlace de la UNAM: 10.10.2.254 Netmask o mascara de red: 255.255.255.0 Servidores de nombre (DNS): 10.10.1.1 Área: Aulas Identificador de red: xl2	

Tabla 5.12

Red LAN del IIMAS, Firewall NAT / Zona Oficinas	
Direccionamiento no homologado	10.10.3x
Identificación de la red IIMAS	
IP Homologada del Firewall NAT Interna para la interface 3: 10.10.3.1 Dirección del ruteador o puerta de enlace de la UNAM: 10.10.4.254 Netmask o mascara de red: 255.255.255.0 Servidores de nombre (DNS): 10.10.1.1 Área: Oficinas Identificador de red: xl3	

Tabla 5.13

Red LAN del IIMAS, Firewall NAT / Zona Investigadores	
Direccionamiento no homologado	10.10.4.x
Identificación de la red IIMAS	
IP Homologada del Firewall NAT Interna para la interface 4: 10.10.4.1 Dirección del ruteador o puerta de enlace de la UNAM: 10.10.4.254 Netmask o mascara de red: 255.255.255.0 Servidores de nombre (DNS): 10.10.1.1 Área: Investigadores Identificador de red: xl4	

Tabla 5.14

Red LAN del IIMAS, Firewall NAT / Zona DMZ	
Direccionamiento no homologado	10.10.5.x
Identificación de la red IIMAS	
IP Homologada del Firewall NAT Interna para la interface 5: 10.10.5.1 Dirección del ruteador o puerta de enlace de la UNAM: 10.10.5.254 Netmask o mascara de red: 255.255.255.0 Servidores de nombre (DNS): 10.10.1.1 Área: DMZ Identificador de red: xl5	

Tabla 5.15

FASE 3

Se instaló el sistema operativo OpenBSD en los servidores, se configuró los servicios y se realizaron las pruebas necesarias para su correcto funcionamiento.

FASE 4

Se diseñó las arquitecturas de los firewalls. La implementación del Firewall transparente, (punta de lanza) de acuerdo a la siguiente figura 5.16.

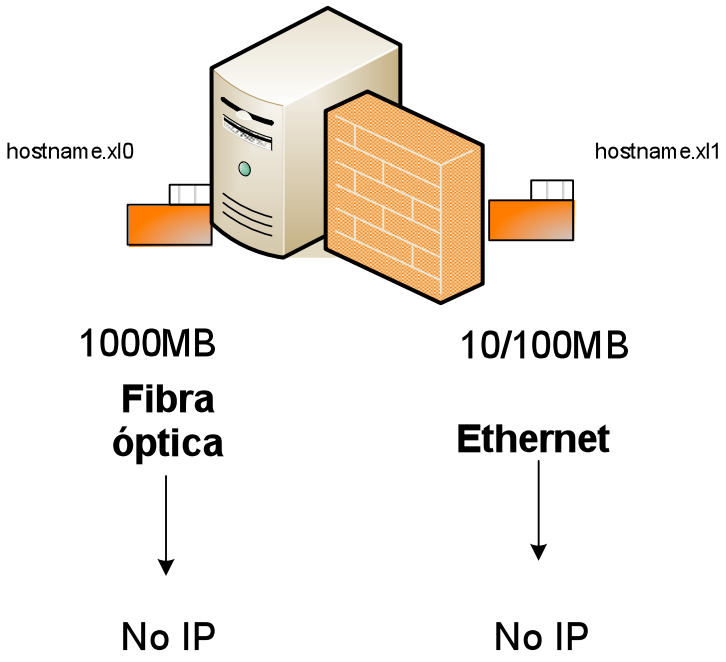

Figura 5.16

Como se observa, una de las características del firewall transparente en su configuración es que no contiene direcciones IP, es porque esto, que se le denomina firewall transparente o brigde, y su configuración técnica se describe a continuación.

5.6 Configuración, reglas y comandos de un firewall transparente

En el Apéndice C, se describen las instrucciones necesarias para configurar un Firewall transparente.

5.7 Esquema de seguridad del Firewall NAT.

La estructura de un firewall NAT requiere configuraciones a partir del número de segmentos de red que se va a utilizar, en la siguiente figura 5.17 se muestra gráficamente el diseño.

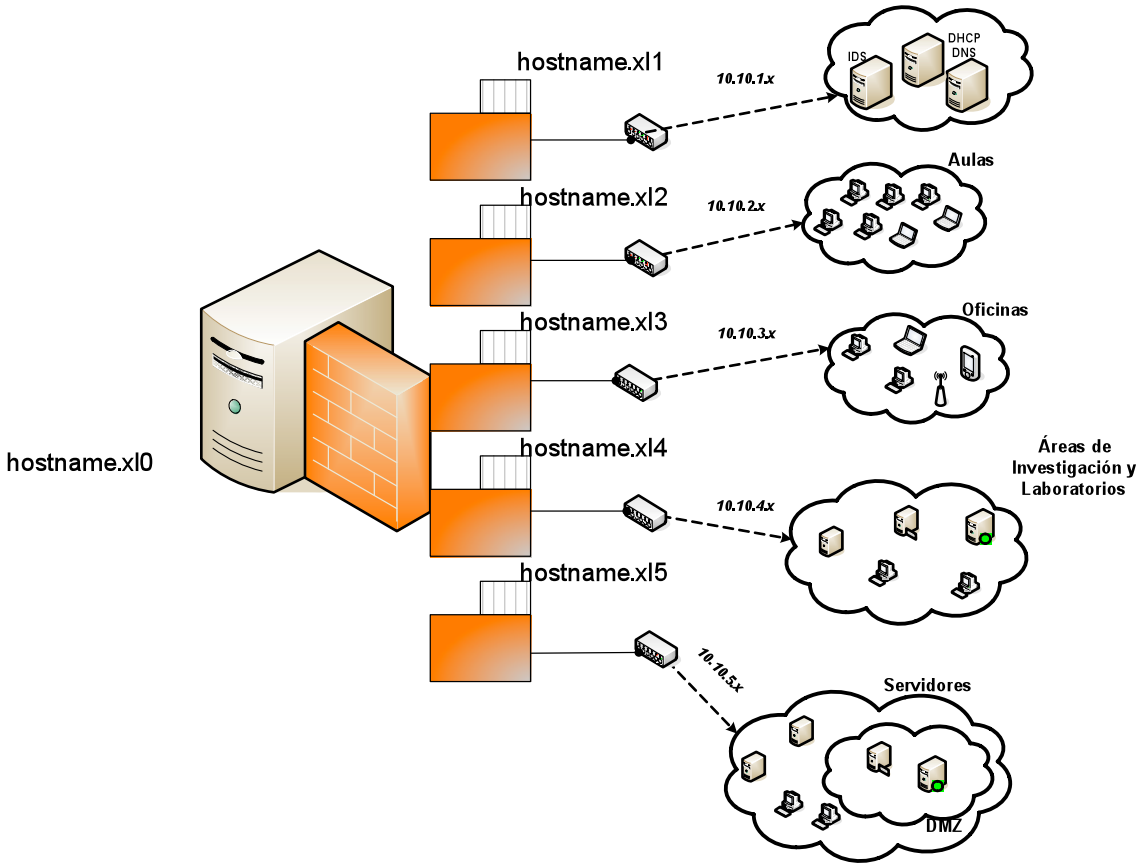

Figura 5.17 Diseño de un firewall NAT

5.7.1. Configuración, reglas y comandos de Firewall NAT

En el Apéndice D, se describen las instrucciones necesarias para configurar un Firewall NAT.

FASE 5

Una vez que se configuró los firewalls y los servicios necesarios para la implementación de seguridad, se propuso la capacitación técnica sobre la instalación, configuración y administración de dichos equipos.

5.8 Conclusiones

Es necesario hacer hincapié que los controles seleccionados en este capítulo fueron de acuerdo a los requerimientos identificados en el análisis y tratamiento del riesgo.

Un punto muy importante fue definir ¿qué es un control? se tiene la impresión de algo muy técnico; en el caso del estándar ISO 17799, el concepto de control es mucho más que eso, pues abarca un conjunto de acciones, documentos, medidas a adoptar, procedimientos, medidas técnicas, etc.

El estándar especifica cada control, agrupándolos en once dominios. Cada uno se definió y describió brevemente. Cabe aclarar que un control proporciona una buena base de referencia. Los 133 controles específicos al día de hoy, son los mínimos que se deberán aplicar, o justificar su no aplicación, pero esto no da por completa la aplicación de la norma si dentro del proceso de análisis de riesgos aparecen aspectos que quedan sin cubrir por algún tipo de control. Por lo tanto, a través de la evaluación de riesgos se determina si es necesaria la creación de nuevos controles, la implantación del SGSI impondrá la inclusión de los mismos, de otra forma el ciclo no estará cerrado y presentará huecos claramente identificables.

Además en este capítulo se diseñaron y propusieron dos controles específicos:

1) Política de seguridad de la información
2) Gestión de seguridad en la red.

De la primera se plantearon 18 políticas de seguridad de la información que se pueden encontrar en el Apéndice B de este caso de estudio.

Y del segundo control, a partir del análisis del caso de estudio y de una investigación de la situación actual de la red del Instituto, se propuso un esquema de red que apoyé de esta manera a la seguridad de la información en dicha dependencia.

[i] ISO/IEC17799:2005 Information Technology. Security Techniques
[ii] Es una red local (una subred) que se ubica entre la red interna de una organización y una red externa, generalmente Internet.
[iii] Dirección privada o no homologada sólo es válida para identificar a la computadora dentro del servicio de acceso, no directamente hacia el resto de Internet."
[iv] AEI P430TX PCI 10/100 Quad Fast Ethernet Card (http://www.telephonyware.com/telephonyware/order.html)

Conclusiones

Hoy en día la mayoría de las organizaciones tienen un gran nivel de **dependencia informática** debido a la automatización de muchos procedimientos, esto implica que sean más **vulnerables a las amenazas de seguridad**, por lo cual se considera de suma importancia poder resguardar la información que se genera. Todo esto se puede lograr a través del uso de un **estándar** que guíe los mecanismos necesarios para garantizar la seguridad.

El utilizar un estándar internacional ayudará a la organización a relacionarse con los sistemas de otras organizaciones con las que comparte información y ser compatibles con dichos sistemas, así mismo utilizar un estándar homologado, provocará que haya pocas posibilidades de cambios en el manejo de la **seguridad** cuando se establezcan acuerdos con otras partes. Además permitirá aplicar auditorias a los sistemas de información no obstante no exista una ley que los imponga.

Por lo cual el objetivo de la presente tesis ha sido diseñar, desarrollar y proponer un esquema de seguridad en los servicios de red junto con una serie de políticas, de acuerdo a las recomendaciones de **ISO 17799** para así conservar la integridad, confiabilidad y disponibilidad de la información en el Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas (IIMAS).

El estándar internacional ISO 17799 es una compilación de recomendaciones para buenas prácticas de seguridad que toda organización puede aplicar. Dicho estándar contiene las especificaciones técnicas o criterios precisos para ser usados consistentemente como reglas, guías, o definiciones de características, asegurando de esta forma que los materiales, productos, procesos y servicios sean apropiados para lograr los objetivos trazados.

Sin embargo, el estándar no tiene una forma de valoración de las soluciones técnicas, por lo que deberá enriquecerse con otros estándares y así poder implementar seguridad teniendo en cuenta los aspectos de tecnología informática y de comunicaciones.

Para cualquier organización y en particular al IIMAS es importante la implementación de seguridad en su información, es por esto que se presentaron propuestas con base al ISO 17799 para apoyar con lineamientos y esquemas de seguridad a los desarrollos tecnológicos e investigación que se originan en el Instituto.

ISO 17799 propone un conjunto de 11 dominios (dominio es cada una de las áreas del estándar) y 39 objetivos para una eficaz administración de la seguridad de la información (Véase Capítulo 2). Dichos dominios contienen una serie controles específicos y que en su totalidad suman 133.

Los dominios son agrupados de la siguiente forma:

1.- Política de seguridad
2.- Organización de la seguridad de la información
3.- Gestión de activos.
4.- Seguridad en recursos humanos
5.- Seguridad física y ambiental

6.- Gestión de comunicaciones y operaciones.
7.- Control de accesos.
8.- Adquisición, desarrollo y mantenimiento de sistemas de información.
9.- Gestión de incidentes de seguridad de la información
10.- Gestión de continuidad del negocio.
11. Conformidad.

La determinación de los controles que se analizaron se definió de acuerdo a los siguientes pasos:

El primero fue analizar junto con las autoridades de Instituto el **compromiso** de garantizar la seguridad en la información y la **importancia** de implementar la seguridad, es decir hasta que punto la Dependencia se compromete, así como la identificación de sus requerimientos y expectativas. Para ello se definió el alcance del estudio.

El segundo paso fue identificar los activos que pueden afectar a la organización si se presenta algún incidente en ellos. Para lo cual se elaboró un **inventario de dichos activos,** así como un **análisis de riesgos** definiendo las posibles vulnerabilidades y amenazas.

Del análisis de riesgos se obtuvieron las siguientes observaciones:

- Deben garantizarse la seguridad de los recursos tanto físicos como lógicos ya que son esenciales para las actividades que realiza el Instituto.
- La información generada por los académicos (publicaciones, proyectos etc.) se considera el recurso más valioso del Instituto de acuerdo al objetivo, misión y visión de la dependencia.

El tercer paso fue revisar la seguridad de la información través de los 133 controles específicos del ISO 17799. A partir de ello se identificaron qué controles se llevan a cabo dentro del Instituto, y se evaluó si se debían mejorar. Adicionalmente se analizaron dos de ellos como: *Seguridad en recursos humanos,* que contemple la descripción de cada rol en aspectos de seguridad de la información; *Seguridad física y ambiental* en el cual se recomienda al Instituto documentar todos los mecanismos de protección.

Otros controles que se propuso desarrollar son: documentar el procedimiento del uso de contraseñas en los sistemas, las especificaciones de seguridad como parte de los requisitos en el desarrollo de sistemas e incidentes de seguridad, entre otros (Véase Apéndice A).

Algunas propuestas derivadas de la revisión de los 133 controles específicos son:

a) Es necesario que cada miembro del Instituto involucrado con la seguridad, conozca el valor de la información que maneja, además de la continua colaboración de la parte técnica para que la información cuente con los debidos métodos de seguridad.
b) Se debe capacitar a todo el personal involucrado directa o indirectamente con la información, para que conozcan los métodos de seguridad y de los lineamientos que se establezcan para el manejo y seguridad de la información, todo esto con el fin de

evitar que los propios usuarios sean quienes provoquen incidentes y con ello causen algún riesgo a la dependencia.

c) El Instituto debe realizar un estudio de costo-beneficio para saber hasta qué punto puede invertir en un proyecto de seguridad óptimo y así evitar futuras modificaciones que repercutan en las inversiones de largo plazo, tales como actualizaciones drásticas o bien que el sistema implementado no se adapte en su totalidad a las necesidades requeridas.
d) Mantener un análisis permanente de los puntos críticos identificados y atacar los puntos débiles en la seguridad de la información.
e) Contar con apoyo especializado en caso de que alguna situación problemática se presente, ya que puede reducir costos y el tiempo de espera para resolver dicho problema.
f) No suponer que las soluciones que se hayan tomado para resolver los problemas de seguridad sean suficientes para enfrentarlos en un futuro. Se deben tener en cuenta los avances tecnológicos y la astucia de los nuevos intrusos.

Después de dicha verificación dentro del alcance y expectativas del Instituto se desarrollaron dos controles específicos: **Documento de política de seguridad de la información y seguridad en los servicios de red** basados en el estándar ISO 17799.

- *Documento de política de seguridad de la información*: se propone una serie de políticas basadas en el análisis de riesgos y revisión de seguridad que se aplicó al Instituto, tales como: administración de riesgos, clasificación de la información, antivirus y código malicioso, entre otros, los cuáles servirán al IIMAS como parte de la Gestión de la Seguridad de la Información (Véase Apéndice A).

- *Seguridad en los servicios de red.* Para la implementación de este control, el Instituto apoyó con equipo (computadoras personales, equipo de telecomunicaciones etc.) para realizar pruebas sobre el esquema de seguridad propuesto bajo BSD como una plataforma segura y robusta para la configuración e instalación de servicios de red como: Firewalls, servidores DNS, DHCP, Proxy. Se demostraron algunas ventajas del sistema como: la corrección del código, la portabilidad, la seguridad proactiva y la criptografía integrada, además de apoyarse en otros elementos como un Proxy, IDS, ISP para la implementación de seguridad en la Dependencia.

También se propuso utilizar un firewall transparente, es decir, un “bridge” que no tiene dirección IP, (i. e. es invisible), con el objetivo de que no se pueda determinar si existe o no en la red.

En resumen los resultados derivados de este trabajo de tesis apoyarán en la gestión de seguridad de la Información del IIMAS, servirán de guía para aquellos interesados en el estándar ISO 17799, y como punto de partida en el diseño y desarrollo de otros controles a futuro como el de *Gestión de continuidad del negocio* que proporcionará un plan de continuidad, considerando los procesos críticos que realiza la dependencia.

Apéndice A

Revisión de la Administración de Seguridad de la Información

Revisión de la Administración de Seguridad de la Información

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
5	**Política de Seguridad**			
5.1	***Política de Seguridad de la Información***			
5.1.1	**Documento de Política de Seguridad**	La organización debe contar con políticas de seguridad que haya sido aprobada por la Dirección y que se haya publicado y comunicado a todo el personal.	Existen ciertas reglas aisladas, sin ser un documento formal de políticas de seguridad de la información. Además de procedimientos administrativos de la UNAM.	Organizar las reglas existentes y complementarlas para obtener un documento formal de Políticas General de la Seguridad de la Información que se propone en el apéndice B, en una primera versión.
5.1.2	**Revisión de las Políticas de Seguridad**	La política debe tener un propietario, responsable del mantenimiento y revisión de la misma de acuerdo con un proceso definido. También deben programarse revisiones periódicas	Actualmente el Comité Interno de Cómputo se encarga de revisar las reglas.	Establecer un procedimiento para que cada cierto tiempo (una vez al año) la Secretaría, Técnica revisé y actualicé las políticas.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
6	**Organización de la seguridad de la información**			
6.1	***Organización interna***			
6.1.1	**Compromiso de la Dirección con la seguridad de la Información**	La Dirección debe dar un apoyo manifiesto de las iniciativas de seguridad. Promover la seguridad dentro de la Organización mediante un adecuado compromiso y una apropiada reasignación de recursos.	Existe apoyo y disposición en caso de surgir iniciativas	Solicitar que la Dirección delegue la iniciativa, se comprometa y apoyé en la implementación de seguridad de la Información.
6.1.2	**Coordinación de la Seguridad de la Información**	Las actividades de la seguridad de la información son coordinadas por los representantes de diferentes áreas o responsables en la organización, con roles y responsabilidades adecuadas.	Se hacen planteamientos aislados.	Las áreas correspondientes en el Instituto (puede ser la Comité Interno de Cómputo) serán las encargadas de organizar y coordinar las actividades necesarias de administrar la seguridad de la información, a través de una Comisión de Seguridad.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
6.1.3	**Asignación de las responsabilidades de la seguridad de la información**	Serán identificadas y definidas la protección de los activos, cada dueño debe especificar el nivel de seguridad que requiere cada recurso.	Cada usuario y/o dueño tiene un resguardo de todos los activos asignados y de los cuales es responsable.	Se revisará y actualizará dicho procedimiento.
6.1.4	**Proceso de autorización de recursos para tratamiento de la información**	Debe establecerse un proceso para nuevas instalaciones de procesamiento de información	No aplica, el Instituto no establece nuevo lugares de procesamiento de información.	No aplica.
6.1.5	**Acuerdos de confidencialidad**	La organización debe tener acuerdos de confidencialidad para la protección de la información.	Existen documentación general a nivel Universidad para ciertas áreas (áreas administrativas) y en otros casos no hay reglas escritas.	Verificar y formalizar en un documento los acuerdos.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
6.1.6	**Contacto con autoridades**	Se debe mantener contacto con autoridades policiales o de seguridad, organismos reguladores, proveedores de servicios de información y operadores de telecomunicaciones, a fin de garantizar que, en caso de producirse un incidente relativo a la seguridad, puedan tomarse las medidas adecuadas y obtenerse asesoramiento con prontitud. Del mismo modo, se debe tener en cuenta a los miembros de grupos de seguridad y foros de la industria.	El Instituto actualmente mantiene contacto con autoridades como CERT-UNAM y áreas de la UNAM encargadas de apoyar en cuestiones de seguridad física como bomberos, primeros auxilios, auxilio UNAM etc.	El IIMAS por ser parte de la UNAM, depende de otras áreas o dependencias encargadas para este fin.
6.1.7	**Contacto con los grupos de interés especial**	Deben existir contactos apropiados con los grupos de interés especial u otros foros de la seguridad además de especialistas.	El Instituto tiene contacto con las organizaciones encargadas de la seguridad a nivel Institucional	Se sugiere que mantenga dicho contacto además de apoyarse con personas dedicadas a ello y documentarlo.
6.1.8	**Revisión independiente de la seguridad de la información**	Es el documento que establece la política y las responsabilidades para la seguridad de la información. Su implementación debe ser revisada. Dicha revisión puede ser llevada a cabo por la función de auditoria interna, o una organización externa especializados en esta índole.	En este momento los documentos sobre políticas y reglamentos son revisados por el Comité Asesor Interno de seguridad del Instituto.	Se propone buscar apoyo de otras áreas externas del Instituto para su revisión y en su caso su actualización como puede ser CERT-UNAM.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
6.2	***Terceras partes***			
6.2.1	**Identificación de riesgos por el acceso de terceros**	Mantener la seguridad de las instalaciones donde se procesa información y de los recursos de información de terceros.	Existen controles de acceso al edificio y a las áreas restringidas.	Se diseñó una política de seguridad para formalizar dicho proceso.
6.2.2	**Consideración de la seguridad en los tratos con clientes.**	Identificar todos los requerimientos de seguridad que podrían estar orientados a llevar el acceso a la información de la organización o activos a los clientes	Al igual que el punto anterior cualquier acceso de terceros, sean proveedores, alumnos o personal de otra dependencia de la UNAM, debe contar con un control.	Se sugiere que se mantenga informado a los responsables del acceso a las áreas sobre las medidas de seguridad así como cualquier cambio. Y si el acceso es lógico disponer de documentación sobre las medidas de seguridad asignadas.
6.2.3	**Consideración de la seguridad en contratos con terceros**	Acuerdos con terceros sobre el acceso, procesamiento y administración de información en la organización, además de las facilidades para procesar dicha información y añadir servicios que cubran los requerimientos de seguridad que se necesitan.	Generalmente el Instituto no maneja información con terceros. Solo comparte información con otras dependencias a través de sistemas de información.	Se debe documentar y formalizar dicho procedimiento entre el Instituto y el tercero.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
7	**Gestión de activos**			
7.1	***Responsabilidad sobre los activos***			
7.1.1	**Inventarios de activos**	Todos los activos deben estar identificados con un inventario o un registro de los activos más importantes.	Cada activo dentro del Instituto cuenta con un número de inventario asignado por Proveeduría para su registro.	Documentar procedimiento.
7.1.2	**Propiedad de los activos**	Cada activo debe estar identificado con un custodio (administrador que maneja la información), además de su clasificación y nivel seguridad definida y acordada, restricciones de acceso que se revisarán cada cierto tiempo.	Cada activo está registrado con su custodio, además de su ubicación. Se cuenta con resguardos firmados por el custodio.	Se recopilo una lista de los activos sensibles con sus custodios.
7.1.3	**Uso aceptable de activos**	Se debe determinar el uso aceptable de la información y los activos asociados con el procesamiento de información. Además de documentarlo e implementarlo.	El instituto no cuenta con documentación sobre el uso aceptable de algunos activos.	Documentar el buen uso de cada activo.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
7.2	***Clasificación de la Información***			
7.2.1	**Guías de clasificación**	La información debe estar clasificada en términos de su valor, sensibilidad y que tan critica es para la organización.	De acuerdo al uso de la información esta se encuentra clasificada como administrativa, técnica y académica	Se realizo una investigación de los activos de acuerdo a su valor (confidencial, integridad y disponibilidad) aún es necesario documentar dicha clasificación.
7.2.2	**Marcado y tratamiento de la información**	Se debe contar con algún procedimiento para etiquetar la información de acuerdo al esquema de clasificación de la organización.	En este momento la información no está etiqueta.	Al igual que el punto anterior al clasificar la información, también se recomienda etiquetarla.
8	**Seguridad en recursos humanos**			
8.1	***Previa a la contratación***			
8.1.1	**Roles y responsabilidades**	Los papeles de seguridad y responsabilidades de los empleados, contratistas y usuarios terceros deben estar definidos y documentados de acuerdo con la política de la seguridad de la información en la organización. Además deben comunicarse claramente a los empleados durante el proceso de	Existen el estatuto y el contrato colectivo para el caso del personal, para los contratistas y prestadores de servicios se tienen contratos y bases para concurso que especifican los términos	Independientemente de la descripción del puesto, se sugirió al Instituto contemple la descripción de cada rol en aspectos de seguridad de la información.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
		contratación.	para su contratación.	
8.1.2	**Selección y verificación de candidatos**	Se debe verificar e investigar a todos los candidatos referentes a su comportamiento, ética, calificaciones profesionales y otros requerimientos que la organización necesita.	Para el caso de contratación de personal, normalmente son personas conocidas o que han tenido algún contacto con el personal del área interesada , en el caso de contratación de prestadores de servicios son empresas registradas en la Dirección General de Proveeduría	Se recomienda documentar dicho proceso, además de orientarla más en medidas de seguridad que el empleado debe conocer y aceptar en el uso de la Información que manejará en el Instituto.
8.1.3	**Términos y condiciones en la relación laboral.**	Se deben definir los términos y condiciones de empleo, establecer la responsabilidad del empleado con la organización respecto a la seguridad de la información.	El contrato colectivo de los trabajadores y los contratos para prestadores de servicios indican implícitamente las responsabilidades.	Al igual que el anterior punto se sugiere que el Instituto realice su propio documento sobre las responsabilidades del empleado en aspectos de seguridad de la información.
8.2	***Durante el empleo***			
8.2.1	**Responsabilidades de la Dirección**	La Dirección debe dar a conocer todos los empleados las medidas de seguridad de acuerdo a las políticas de información y	Aunque se tiene conocimiento de los empleados y el manejo	Se sugiere que el Instituto realice la documentación sobre

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
		procedimientos establecidos en la organización. Además de conocer los roles y responsabilidades sobre todo de aquellos empleados que manejan información sensible de la organización.	de información está no se encuentra documentada.	este punto y se la haga saber a los empleados responsables.
8.2.2	**Conocimiento y formación en la seguridad de la información**	Todos los empleados deben recibir la capacitación adecuada al conocimiento de la seguridad de la organización, actualizaciones regulares referentes a las políticas y procedimientos de organización dependiendo su rol en ella.	Se cuenta con la información que se genera y distribuye a través del Consejo Interno, Comisión Local de Seguridad y comité de cómputo.	Se debe realizar un plan integral de capacitación para todos los empleados por año o según las necesidades del Instituto.
8.2.3	**Proceso disciplinario**	Debe existir un proceso disciplinario para los empleados sobre la seguridad de la información.	No se cuenta con un proceso disciplinario.	Se sugirió realizar un documento que describa dicho proceso.
8.3	***Terminación o cambio de empleo***			
8.3.1	**Responsabilidades al término del contrato**	Las responsabilidades al término de su labor en la organización o cambio deben estar claramente definidas.	Se revisan los resguardos para la entrega de equipo y mobiliario, se da un tiempo de tres meses de gracia con las cuentas en los servidores	Se sugiere que el procedimiento de entrega de recursos este documentado y tenga conocimiento el empleado.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
8.3.2	**Devolución de activos**	Debe existir un proceso que asegure la entrega de activos que estuvieron bajo el resguardo del empleado al término de su contrato o acuerdo con la organización.	Se revisan los resguardos para la entrega de equipo y mobiliario y este documentado el procedimiento	Existe un manual de procedimientos.
8.3.3	**Eliminación de privilegios de acceso.**	Se debe remover los derechos de acceso tantos físicos como lógicos a la información a todos los empleados que hayan terminado su contrato o acuerdo con la organización	Se da un tiempo de tres meses de gracia con las cuentas (correo, sistemas, acceso a los archivos, etc.) en los servidores	Se recomienda actualizar dicho procedimiento.
9	**Seguridad física y ambiental**			
9.1	***Áreas seguras***			
9.1.1	**Perímetro de seguridad física**	La protección física puede llevarse a cabo mediante la creación de diversas barreras físicas alrededor de la organización y en las áreas donde hay procesamiento de información. Cada barrera establece un perímetro de seguridad, cada uno de los cuales incrementa la protección total provista.	Las áreas donde se procesa información está resguardas a través de cuartos con llave o gabinetes con llave, además de que los equipos tienen contraseñas.	Se recomienda documentar los mecanismos de protección y se revisen periódicamente.
9.1.2	**Controles físicos de entrada**	Las áreas protegidas deben ser resguardadas por adecuados controles que	El área de vigilancia se encarga del control de	Documentar los controles de accesos y

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
		permitan garantizar el acceso solo a personal autorizado.	acceso mediante tarjetones de colores, rondines en todo el edificio, controles electrónicos de acceso, y censores detectores para el control de Biblioteca, Además de un sistema de monitoreo permanente	seguridad perimetral general. .
9.1.3	**Seguridad de oficinas, instalaciones y recursos**	Un área protegida puede ser una oficina cerrada con llave, o diversos recintos dentro de un perímetro de seguridad física, el cual puede estar bloqueado y contener cajas fuertes o gabinetes con cerraduras.	Cada área o departamento tiene un acceso, el cual está resguarda por una secretaria y si es un cubículo de investigación, se encuentra cerrada.	Documentar dichos controles de accesos, responsabilidades y obligaciones del personal sobre seguridad física.
9.1.4	**Protección contra amenazas externas y ambientales**	Diversas protecciones físicas deben ser diseñadas y aplicadas como por ejemplo: en caso de incendio, inundaciones, terremoto, y otras formas de desastre natural o artificial.	El IIMAS cuenta con el apoyo de auxilio UNAM Bomberos y del Centro Médico Universitario mediante teléfonos con línea directa y exclusiva a estos servicios.	Se recomienda revisar periódicamente las medidas de protección y alarmas contra incendios/humo, inundaciones, control de climatización, independientemente del apoyo UNAM.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
9.1.5	**Trabajo en áreas seguras**	Para incrementar la seguridad de un área protegida pueden requerirse controles y lineamientos adicionales. Esto incluye controles para el personal o terceras partes que trabajan en el área protegida, así como para las actividades de terceros que tengan lugar allí.	Como se describió en puntos anteriores el Instituto tiene áreas restringidas.	Los controles existentes deben difundirse entre el personal del Instituto.
9.1.6	**Áreas de acceso público, carga y descarga**	Las áreas de entrega y carga deben ser controladas y, si es posible, estar aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados. Los requerimientos de seguridad de dichas áreas deben ser determinados mediante una evaluación de riesgos.	El almacén se encuentra junto al vestíbulo de acceso al edificio y lejos de las zonas de proceso de información	Se recomienda documentar los controles de las áreas de acceso, entrega de materiales, zonas públicas y privadas.
9.2	***Seguridad de los equipos***			
9.2.1	**Instalación y protección de equipos.**	El equipo debe ser ubicado o protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y acceso no autorizado	Se cumple adecuadamente	Se recomienda que todas estás medidas sean revisadas cada cierto tiempo además estén documentadas y se comunique a todo los usuarios.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
9.2.2	**Suministros**	Los equipos deben estar protegidos con respecto a posibles fallas en el suministro de energía u otras anomalías eléctricas. Dicho suministro debe cumplir con las especificaciones del fabricante o proveedor de los equipos.	Se cuenta con una planta de emergencia que respalda a todo el edificio en luminarias y contactos generales, también cuenta con un sistema de energía de no interrupción para todo el equipo de cómputo.	Revisar y actualizar documentación de la planta. Supervisar el mantenimiento a la planta.
9.2.3	**Seguridad del cableado**	El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe estar protegido contra interceptación o daño. Si es necesario deben realizarse algunos controles adicionales de la seguridad en el lugar donde hay información crítica o sensible.	Todo cableado de voz datos y potencia van por tuberías y ductos ocultos con registros controlados y restringidos.	Documentar y actualizar planos de instalaciones, antenas, canales de comunicaciones, cableado u otros, además certificación de los mismos, etc.
9.2.4	**Mantenimiento de equipos**	El equipamiento debe mantenerse en forma adecuada para asegurar que su disponibilidad e integridad sean permanentes.	La Secretaría Técnica se encarga de la programación del mantenimiento preventivo y correctivo del equipo.	Se recomienda mantener actualizadas las garantías de los equipos, ya que no se cuenta con un proveedor de mantenimiento correctivo y preventivo.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
9.2.5	**Seguridad de equipos fuera de la organización**	El uso de equipo destinado al procesamiento de información, fuera del ámbito de la organización, debe ser autorizado por la Dirección. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la organización, para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma. El equipamiento de procesamiento de la información incluye todo tipo de computadoras personales o cualquier otro equipo necesario para el trabajo fuera del lugar habitual de trabajo.	Los equipos personales requieren de controles de entrada y salida y está cubierto por un seguro contratado.	Se recomienda documentar y crear políticas de seguridad para los equipos que se encuentren fuera de la organización.
9.2.6	**Seguridad en la reutilización o eliminación de equipos.**	La información puede verse comprometida por algún descuido en la reutilización del equipo. Los medios de almacenamiento que contienen material sensible o software con licencia deben ser destruidos o sobrescritos en forma segura antes de reutilizarlo.	Se cuenta con procedimientos de limpieza y formateo de equipos previo a la reasignación.	Se recomienda documentar dicho proceso y comunicárselo a los usuarios.
9.2.7	**Retiro de propiedad**	Equipo, información y software no puede ser utilizado fuera de las instalaciones de la organización, sin previa autorización.	Se cuenta con controles para tal efecto.	Documentar, revisar y/o actualizar dicho control.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
10	**Gestión de comunicaciones y operaciones**			
10.1	***Procedimientos y responsabilidades de operación.***			
10.1.1	**Documentación de procedimientos operativos**	Se deben documentar y mantener los procedimientos operativos identificados. Los procedimientos operativos deben ser tratados como documentos formales y los cambios deben ser autorizados a nivel Dirección, además de estar disponibles a los usuarios que lo requieran.	Todos los procedimientos son documentos formales y disponibles avalados por la Dirección	Se recomienda actualizar dichos documentos de forma sencilla y comprensible, disponibles a todos los usuarios que los necesiten, segregando adecuadamente los servicios y las responsabilidades para evitar un uso inadecuado de los mismos.
10.1.2	**Gestión de cambios**	Se deben controlar los cambios en los sistemas e instalaciones de procesamiento de información. El control inadecuado de estos cambios es una causa común de las fallas de seguridad y de sistemas. Se deben implementar responsabilidades y procedimientos formales para garantizar un control satisfactorio de todos los cambios en el equipamiento, el software o los procedimientos. Cuando se cambian los	Se cuenta con registros del software instalado con número de licencia, usuario y equipo así como fecha de instalación y caducidad.	Se debe identificar los procedimientos en donde se realizan cambios y utilizar los controles adecuados para su revisión cuando se requiera además de documentar el proceso.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
		programas, se debe tener un registro de auditoria que contenga toda la información relevante.		
10.1.3	**Separación de funciones**	La separación de funciones es un método para reducir el riesgo de mal uso, accidental o deliberado de los sistemas. Se debe considerar la separación de la gestión o ejecución de ciertas tareas o áreas de responsabilidad, a fin de reducir las oportunidades de modificación no autorizada o mal uso de la información o los servicios.	La administración y manejo de la información se lleva a cabo de acuerdo su clasificación, información administrativa, académica, técnica etc.	Se recomienda documentar y revisar dicho procedimiento.
10.1.4	**Separación de los recursos para desarrollo, pruebas y producción**	La separación entre los ambientes de desarrollo, prueba y producción es importante para lograr la separación de los roles involucrados. Se deben definir y documentar las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo o de producción. Contar con perfiles y ambientes seguros para las pruebas, así como de los datos sensibles que se requieran.	Aunque el Instituto desarrolla sistemas para la investigación, cada responsable realiza la tarea de separar ambientes.	Se sugirió documentar y revisar el procedimiento.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
10.2	***Gestión de la provisión de servicios contratados a terceros***			
10.2.1	**Provisión de servicios**	Tomar medidas que aseguren el control de seguridad, definir el servicio y nivel de entrega del servicio de terceros de acuerdo a la implementación, operación y mantenimiento.	Existen mecanismos para el control en la asignación del servicio, de los tiempos de entrega y las condiciones de garantía y servicio	Documentar adecuadamente los servicios que se están prestando (acuerdos, Obligaciones, responsabilidades, confidencialidad, operación, mantenimiento, etc.).
10.2.2	**Seguimiento y revisión de servicios de terceros.**	Los servicios, reportes y registros proporcionados por terceros, debe ser monitoreado y revisado regularmente.	Cada área es responsable de dar seguimiento a los proveedores de servicio que les corresponda	Documentar las medidas adoptadas para la revisión, monitorización y auditoria de los mismos
10.2.3	**Gestión de cambios en servicios de terceros**	Todos los cambios en los servicios, incluyendo mantenimiento, mejoras de los procedimientos y controles, deben ser administrados y documentados, tomando en cuenta lo critico que puede ser para la organización.	El cambio en los servicios solo se daría en beneficio del Instituto mediante previa revisión de las condiciones existentes y las propuestas.	Documentar adecuadamente, para permitir un eficiente control de cambios en estos servicios.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
10.3	***Planeación y aceptación del sistema***			
10.3.1	**Planificación de la capacidad**	Para minimizar el riesgo de fallas en los sistemas se requiere de una planeación y preparación anticipada para garantizar la disponibilidad de capacidad y recursos adecuados. Deben realizarse proyecciones para futuros requerimientos de capacidad, a fin de reducir el riesgo de sobrecarga del sistema. Establecer, documentar y probar los requerimientos operativos de nuevos sistemas antes de su aprobación y uso.	Los sistemas que desarrollan y que generalmente son para proyectos de investigación, toman en cuenta los lineamientos que menciona el presente control.	Se sugirió que se documente dicha planeación y se utilicé según sea el caso en todos los sistemas que desarrollen a futuro.
10.3.2	**Aceptación del sistema**	Se deben establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, se deben llevar a cabo adecuadas pruebas de los sistemas antes de su aprobación.	No cuenta con documentación.	Se sugirió al Instituto que tenga criterios documentados en relación a la actualización y aceptación de los sistemas con los que cuenta o se desarrollen a futuro.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
10.4	***Protección contra software malicioso y código móvil***			
10.4.1	**Medidas y controles contra software malicioso**	Se deben implementar controles de detección y prevención para la protección contra software malicioso, y procedimientos adecuados de concienciación de usuarios.	Se cuenta con las recomendaciones del comité de cómputo para el uso de equipo y conexión a red, la instalación de firewalls, antivirus y antispyware.	Se diseño una política de seguridad en relación a virus informáticos, como una primera versión. (véase Apéndice B)
10.4.2	**Medidas y controles contra código móvil**	El uso de código móvil debe ser autorizado de acuerdo claramente a las políticas de seguridad.	Existen políticas de seguridad y un IPS para mantener la seguridad respecto al código móvil.	Se recomienda actualizar dicha política y hacerla llegar a los usuarios que la necesiten.
10.5	***Copia de seguridad***			
10.5.1	**Copia de seguridad de la información**	Realizar copias de seguridad de la información y software de acuerdo a las políticas de respaldo.	Los discos originales se respaldan y se guardan, los discos de respaldo se usan para instalaciones. La información de los servidores se respalda periódicamente.	Se diseñó políticas de respaldo para el Instituto (véase Apéndice B). Además se recomendó documentar todos los procedimientos de recuperación y capacitar al personal sobre estos. Además de comprobar que cada respaldo se haya realizado.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
10.6	***Gestión de la seguridad de red***			
10.6.1	**Controles de red**	La red debe ser correctamente administrada y controlada, para protegerla de amenazas, y así mantener la seguridad de los sistemas y aplicaciones que intercambian información a través de la red. Los controles implementados deben ser seguros para la información en la red y proteger las conexiones de amenazas como accesos no autorizados.	Se llevan a cabo los procedimientos de administración de acuerdo al conocimiento, experiencia de los administradores y guiándose de foros de seguridad y literatura especializada	Se sugirió al Instituto documentar dichos procedimientos.
10.6.2	**Seguridad en los servicios de red**	Las características, niveles de servicio y administración de requerimientos de todos los servicios de red, debe estar identificados. Si el servicio de red está habilitado, debe estar administrado y seguro, a través de un monitoreo y correctamente auditado.	Los servicios de red que tiene implementado el Instituto se encuentra en constante monitoreo para su correcto funcionamiento.	Se propuso un esquema de seguridad para toda la red del Instituto (Ver **Capítulo 4)**
10.7	***Utilización de los soportes de información***			
10.7.1	**Gestión de soportes extraíbles**	Deben existir procedimientos para administrar medios removibles, como cintas, discos, memorias, etc. Todos los procedimientos y niveles de autorización deben estar claramente	Cada dueño es responsable de los medios extraíbles que maneja y por lo tanto de su información.	Se diseñó una política de seguridad sobre medios extraíbles como una primera versión (véase Apéndice B).

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
		definidos y documentados.		
10.7.2	**Eliminación de medios**	Cuando ya no son requeridos, el contenido de los medios informáticos debe eliminarse de manera segura. Si los mismos no se eliminan cuidadosamente, la información sensible puede filtrarse a personas ajenas a la organización. Se deben establecer procedimientos formales para la eliminación segura de los medios informáticos, a fin de minimizar este riesgo.	No existe procedimiento sobre el borrado de información.	Se diseñó una política de seguridad respecto al borrado de información en diversos medios. (véase Apéndice B)
10.7.3	**Procedimientos de utilización para la información**	Se deben establecer procedimientos para el manejo, almacenamiento y protección de la información contra el uso inadecuado o divulgación no autorizada.	Cada dueño es responsable del almacenamiento de su información y está documentada en las políticas de cómputo.	Se recomienda revisar y/o actualizar dicha política.
10.7.4	**Seguridad de la documentación de sistemas**	La documentación de los sistemas puede contener cierta cantidad de información sensible, por ejemplo: descripción de procesos de aplicaciones, procedimientos, estructuras de datos, procesos de autorización	El Instituto no cuenta con dicha documentación.	Aunque los sistemas administrativos que maneja el Instituto, no son desarrollos propios se sugirió que documente todos los incidentes referentes a estos sistemas y mantenga contacto con

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
				los desarrolladores. Los sistemas de investigación si son documentados, pero no en cuestiones de seguridad.
10.8	***Intercambio de información***			
10.8.1	**Políticas y procedimientos para el intercambio de información**	Deben existir políticas de intercambio de información, procedimientos y controles para proteger la información.	Existen procedimientos que indican la ruta de la información, son responsables tanto el emisor como el receptor de seguir estos procedimientos.	Se realizó una política de seguridad sobre el intercambio de información como una primera versión (véase Apéndice B). Y se sugirió diseñar algún procedimiento en el intercambio de información en línea.
10.8.2	**Acuerdos para el intercambio de información**	Deben existir acuerdos establecidos respecto al intercambio de información y software entre la organización y externos. La seguridad debe estar de acuerdo al contenido y sensibilidad de la información.	El intercambio de información se realiza a través de los procedimientos establecido por los dueños de la información, el Instituto	Se sugirió revisar dichos procedimientos, que contengan algunos de los siguientes puntos: - Acuerdos, funciones, obligaciones,

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
			como tal no cuenta con acuerdos a nivel de la organización..	responsabilidades y sanciones de todas las partes que intervienen. -Consideraciones para los casos de mensajería electrónica.
10.8.3	**Soportes físicos en tránsito**	Si el medio contiene información debe estar protegido contra accesos no autorizados y corrupción de datos durante el transporte fuera de la organización.	Existen respaldos que conserva el emisor, el envío se hace con mensajería y en sobre cerrado haciendo uso de firmas de recepción.	Se propuso una política de seguridad (véase Apéndice B) respecto a la seguridad de dicha información electrónica transferida como puede ser que vaya cifrada. Además de revisar otras medidas de protección física de la información en tránsito.
10.8.4	**Mensajería electrónica**	Cualquier información relacionada con la organización y se envié electrónicamente debe estar protegida. Los mensajes electrónicos incluyen correo electrónico, intercambio de datos electrónicos y mensajería instantánea.	No cuentan con procedimientos para proteger información electrónica.	Se diseñó una política de seguridad (véase Apéndice B) de información que describe algunos aspectos importantes a considerar al utilizar la mensajería electrónica.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
10.8.5	**Sistema de información de negocios**	Deben existir políticas y procedimientos dirigidos a proteger la información asociadas con la interconexión de los sistemas de información.	No tienen documentación sobre este punto.	Se diseñó una política de seguridad (véase Apéndice B) de información respecto al uso de los sistemas de información. Además contar con medidas particulares a implementar para los intercambios de información y en especial con otras organizaciones.
10.9	**Servicios de Comercio Electrónico**			
10.9.1	**Comercio Electrónico**	La información relacionada con el comercio electrónico va a transportarse a través de una red pública por lo cual debe protegerse de actividades fraudulentas y accesos o modificaciones no autorizadas. La aplicación de criptografía puede considerarse como un control de seguridad. Al utilizar comercio Electrónico entre socios se debe incluir documentación de acuerdo, el cual comprometa a ambas partes aceptar términos de acuerdo de	La seguridad del comercio electrónico es delegado a la DGSCA ya que cuenta con los medios adecuados para garantizar la seguridad de la información El Instituto solo se encarga de enviar la actualización de la información publicada a	Se recomienda al Instituto que aunque no sea prestadora de servicios de comercio electrónico directamente, si mantenga seguridad en el intercambio de información.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
		comercio, incluyendo problemas de seguridad.	dicha dependencia.	
10.9.2	**Transacciones en línea**	Las transacciones en línea deben estar protegidas para así prevenir transmisiones incompletas, mensajes no autorizados o duplicados, alteraciones o repeticiones.	No se realizan transacciones en línea	No aplica
10.9.3	**Información de difusión pública**	La integridad de la información pública disponible debe estar protegida contra cualquier modificación no autorizada.	El Instituto no pública directamente la información.	Se recomendó revisar la integridad de la información que envié o publiqué.
10.10	***Seguimiento o monitoreo***			
10.10.1	**Registros de auditoria**	Auditar los registros, actividades de los usuario y eventos de seguridad de la información que sean producidos durante un periodo de tiempo y que puede apoyar en futuras investigaciones y monitoreo de control de acceso.	El Instituto actualmente no audita los logs, solo eventos con actividad extrañas que los administradores detecten.	Se diseñó una política de seguridad respecto a la auditoria en los sistemas. (véase Apéndice B)

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
10.10.2	**Monitoreo al uso del sistema**	Deben existir procedimientos de monitoreo del uso de la información y así poder monitorear las actividades regularmente.	Los administradores son los encargados de la revisión de bitácoras para monitoreo detección y seguimiento a incidentes.	Se estructuró una política de seguridad (véase Apéndice B) de la información sobre el monitoreo de los sistemas.
10.10.3	**Protección del registro de la información (logs)**	Proteger todos los registros de información como puedes ser las bitácoras (logs) de los accesos no autorizados.	Todos los servidores cuentan con bitácoras "logs" de todos los accesos, se tiene como procedimiento que el administrador revise esos archivos y proceda en consecuencia.	Se recomienda documentar dicho procedimiento e implementar medidas robustas sobre dicha protección.
10.10.4	**Registro (logs) de las actividades de los administradores y operadores**	Se debe llevar un registro de las actividades de los administradores y operadores de los sistemas.	Cada administrador es responsable de su actividad y debe contar con bitácoras de administración	Se sugirió al Instituto que desarrollé una política que revise las actividades del administrador. Hay que destacar que una vez que se posee acceso a una cuenta de administración, se tiene control total de esa máquina y en la mayoría de los casos es un acceso para el resto de la

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
				infraestructura, es decir, se emplea esa máquina como puente o máquina de salto hacia las demás.
10.10.5	**Registro de errores**	Las fallas de los registros (logs), deben ser analizadas y en caso de algún incidente tomar acciones pertinentes sobre dichas fallas.	Como parte de la actividad de los administradores, revisan e interpretan los logs para corregir cualquier falla. Cada administrador cuenta con su bitácora para llevar un control.	Se recomienda implementar un sistema de alarmas que revisé el normal funcionamiento de los sistemas de generación de eventos de seguridad y/o Logs.
10.10.6	**Sincronización de relojes**	Los relojes del sistema de todos los sistemas de que procesan información deben estar sincronizados por ejemplo con el Coordinated Universal Time (UTC).	Los equipos están configurados para tomar el reloj vía red de sitios confiables.	Documentar y revisar si se utiliza el protocolo NTP (Network Time Protocol)
11	**Control de Accesos**			
11.1	***Requisitos de negocio para el control de acceso***			
11.1.1	**Políticas de control de accesos**	Se deben definir y documentar los requerimientos de negocio para el control de accesos. Las reglas y derechos del control de accesos, para cada usuario o grupo de usuarios, deben ser claramente	Como parte de las políticas de administración se establecen como controles de acceso la	Se desarrollo una política de seguridad para el control de accesos en los sistemas (véase Apéndice B)

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
		establecidos en una declaración de política de accesos. Se debe otorgar a los usuarios y proveedores de servicio una clara explicación de los requerimientos que deberán satisfacer los controles de acceso	clasificación de cuentas, contraseñas que no sean débiles, etc.	
11.2	***Gestión de acceso a usuarios***			
11.2.1	**Registro de usuario**	El acceso a servicios de información debe ser controlado a través de un proceso formal de registro de usuarios	La solicitud de cuentas usuarios se realiza mediante oficio con justificación y autorización del jefe inmediato.	Documentar dicho procedimiento para asegurar el correcto acceso y prevenir el no autorizado
11.2.2	**Gestión de privilegios**	Se debe limitar y controlar la asignación y uso de privilegios (cualquier característica o servicio de un sistema de información multi-usuario que permita que el usuario pase por alto los controles de sistemas o aplicaciones). El uso inadecuado de los privilegios del sistema resulta frecuentemente el más importante factor que contribuye a la falla de los sistemas a los que se ha accedido de forma no autorizada.	Los privilegios de los usuarios se asignan de acuerdo a la actividad desempeñada por el usuario.	Documentar dicho procedimiento dependiendo el nivel de privilegios.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
11.2.3	**Gestión de contraseñas de usuario**	Las contraseñas constituyen un medio común de validación de la identidad de un usuario para acceder a un sistema o servicio de información. La asignación de contraseñas debe controlarse a través de un proceso de administración formal.	Existen procedimientos para generar, asignar y modificar las contraseñas, esta labor se realiza como parte de la administración de los servidores.	Se desarrolló una política de seguridad de información sobre contraseñas. (véase Apéndice B)
11.2.4	**Revisión de los derechos de acceso de los usuarios.**	A fin de mantener un control eficaz del acceso a los datos y servicios de información, la administración debe llevarse a cabo un proceso formal a intervalos regulares, a fin de revisar los derechos de acceso de los usuarios Por ejemplo revisar cada tres meses privilegios especiales y cada seis meses privilegios normales.	Se hace revisión cuando hay algún cambio, pero no existe nada documentado.	Documentar los procesos sobre derechos de los usuarios periódicamente.
11.3	***Responsabilidades del usuario***			
11.3.1	**Uso de contraseña**	Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación de la identidad de un usuario y por lo tanto un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.	Se recomienda a los usuarios el cambio periódico de contraseñas, no anotarlas y mantenerlas a la vista, que sean contraseñas fáciles de recordad pero difíciles de descifrar.	Se sugirió al Instituto que se entreguen y actualicen dichas prácticas, además de documentarlas. También se estructuró una política de seguridad sobre este punto. (véase

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
				Apéndice B)
11.3.2	**Equipo desatendido por el usuario.**	Los usuarios deben garantizar que los equipos desatendidos estén protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo: estaciones de trabajo o servidores de archivos, pueden requerir una protección específica contra accesos no autorizados, cuando se encuentren desatendidos durante un largo periodo.	En términos generales los equipos servidores están en lugares cerrados a los que solo tiene acceso el administrador, los equipos clientes están en cubículos individuales y los equipos de laboratorios no contienen información crítica.	Se diseñó una política de seguridad sobre este rubro. (véase Apéndice B)
11.3.3	**Política de puesto de trabajo y bloqueo de pantalla**	Contar con una política clara sobre el uso de equipos de escritorio y remover medios de almacenamiento, así como de protector de pantalla.	Existen políticas de administración que desconectan automáticamente a los usuarios que tienen sesiones abiertas sin uso por un periodo determinado	Se desarrollo una Política de seguridad de la información sobre el bloqueo de equipos. (véase Apéndice B)
11.4	***Control de acceso a la red***			
11.4.1	**Política de uso de los servicios de red**	Las conexiones no seguras a los servicios de red pueden afectar a toda la organización. Los usuarios solo deben contar con acceso directo a los servicios para los cuales han sido expresamente	Este punto es cubierto por las políticas de asignación de cuentas de acuerdo a una	Se realizo una política de seguridad de información (véase Apéndice B) sobre el acceso a la información.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
		autorizados. Este control es importante para los usuarios que se conectan en sitios de alto riesgo, por ejemplo: áreas públicas o externas que están fuera de la administración y el control de seguridad de la organización.	clasificación	Además se recomienda documentar y asegurar que solo puedan acceder a los servicios específicamente autorizados.
11.4.2	**Autenticación de usuario para conexiones externas**	Las conexiones externas son un gran potencial para accesos no autorizados a la información de la organización Por lo cual, el acceso de usuarios remotos debe estar sujeto a la autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros.	Existen métodos de autenticación aun cuando los servicios y la información disponible para usuarios externos no son críticos.	Se diseñó una política de seguridad de información (véase Apéndice B), además se recomendó al Instituto que aunque no contenga información critica puede ser un punto de vulnerabilidad latente para los sistemas.
11.4.3	**Identificación de equipos en la red**	Se debe tener en cuenta la identificación de los equipos para autenticar conexiones a ubicaciones específicas y a equipos móviles. La identificación automática de los equipos es una técnica que puede utilizarse para que la sesión solo pueda iniciarse de un equipo o de una ubicación determinada.	Existe una base de datos en que contiene la dirección IP, la MAC, la ubicación y usuario del equipo, las redes inalámbricas tienen como mecanismo de control un servidor RADIUS.	Documentar dicho procedimiento además de utilizar las herramientas necesarias para identificar con certeza las direcciones, puertos y equipos que pueden o no ser considerados como seguros para acceder a

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
				las diferentes zonas del Instituto. Tanto desde una red externa como desde segmentos de la propia dependencia.
11.4.4	**Protección de puertos de configuración y diagnósticos remotos**	El acceso a los puertos de diagnóstico debe ser controlado de manera segura. Muchas computadoras y sistemas de comunicación son instalados con una herramienta de diagnóstico remoto, si no están protegidos estos puertos permitirán accesos no autorizados.	Los puertos de diagnóstico son cerrados y solo son accesibles a través de la consola.	Para toda esta actividad se deben implementar: IDSs, IPSs, FWs con control de estados, honey pots, listas de control de acceso, certificados digitales, protocolos seguros, túneles, etc. que son propuestos en el Capítulo 4.
11.4.5	**Dividir las redes.**	Un método para controlar la seguridad de redes extensas es dividirlas en dominios lógicos, por ejemplo: dominios de redes internas y externas de una organización, cada uno protegido por un perímetro de seguridad definido.	Existen firewalls que separan las redes por Departamentos.	Se sugiere que toda está información se encuentre documentada.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
11.4.6	**Control de conexión a redes**	Los requerimientos de la política de control de accesos para redes compartidas, especialmente aquellas que se extiendan mas allá de los limites de la organización, pueden requerir la incorporación de controles para limitar la capacidad de conexión de los usuarios	La capacidad de conexión esta limitada por los servicios que brinda el Instituto.	Se recomienda documentar dicho procedimiento.
11.4.7	**Control de escaneo de la red**	Debe existir una política de acceso para escanear las conexiones que están realizando los usuarios, tanto la fuente como el destino del flujo de información.	Los servidores relevantes bloquean a los equipos que hacen escaneo, recientemente se ha implementado un IPS que bloquea este tipo de actividad insegura.	Se diseñó una política de seguridad (véase Apéndice B) sobre el control de escaneo de la red.
11.5	***Control de acceso al sistema operativo***			
11.5.1	**Procedimientos de conexión segura**	El acceso al sistema operativo debe ser controlado por un procedimiento seguro de "logeo"	Los equipos personales cuentan con contraseñas desde el BIOS adicionalmente a las cuentas de usuario en el sistema operativo.	Se sugirió que este procedimiento se documenté, además se diseñó una política de seguridad sobre este punto (véase Apéndice B).
11.5.2	**Identificación y autentificación de**	Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de	Existen ID de usuario y de grupo.	Se recomienda documentar dicho procedimiento y que los

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
	usuarios	sistemas y administradores de bases de datos) deben tener un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable.		administradores de los servidores tengan conocimiento de ello.
11.5.3	**Sistemas de gestión de contraseñas**	Las contraseñas constituyen uno de los principales medios de validación de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas robustas.	La generación de cuentas se hace manual, pero siguiendo todas las recomendaciones en cuanto al número mínimo y máximo de caracteres alfanuméricos y símbolos	Se recomendó documentar dicho procedimiento, también se menciona en la política de seguridad sobre la administración de contraseñas (véase Apéndice B)
11.5.4	**Uso de los servicios del sistema**	Usar herramientas capaces de eliminar controles del sistema, su uso está restringido y rigurosamente controlado.	Este control se realiza desde la instalación del sistema operativo, es decir no se instalan utilerías que puedan vulnerar la seguridad.	Se recomendó documentar el proceso.
11.5.5	**Desconexión automática de las**	Las terminales inactivas en ubicaciones de alto riego, por ejemplo: áreas públicas o externas fuera del alcance de la gestión de seguridad de la organización, o que sirven	Este control es implementado como parte de las políticas de administración de los	Se diseñó una política de seguridad sobre este proceso. (véase

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
	sesiones	a sistemas de alto riego, deben apagarse después de un periodo definido de inactividad, para evitar el acceso de personas no autorizadas.	equipos.	Apéndice B)
11.5.6	**Limitación del tiempo de conexión**	Las restricciones de tiempo de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo. La limitación del periodo durante el cual se permiten las conexiones de los equipos a los sistemas reduce el espectro de oportunidades para el acceso no autorizado. Se debe considerar un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellos equipos instalados en ubicaciones de alto riesgo	Este control es implementado como parte de las políticas de administración de los equipos.	Se propuso una política de seguridad (véase Apéndice B)
11.6	***Control de acceso a información y aplicaciones***			
11.6.1	**Restricción de acceso a la información**	Los usuarios de sistemas de aplicación deben tener acceso a la información y a las funciones de los sistemas de aplicación de conformidad con una política de control de acceso definida, y conforme a la política de la organización para el acceso a la información	En este momento el Instituto no cuenta con política de seguridad sobre acceso y organización de la información.	Se estructuró una política de seguridad sobre el acceso y organización de seguridad de la información. (véase Apéndice B)

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
11.6.2	**Aislamiento de sistemas sensibles**	Los sistemas sensibles podrían requerir de un ambiente dedicado (aislado). Algunos sistemas de aplicación son suficientemente sensibles a perdidas potenciales y requieren un tratamiento especial. La sensibilidad puede señalar que el sistema de aplicación debe ejecutarse en una computadora dedicada, que sólo debe compartir recursos con los sistemas de aplicación confiables.	Los equipos que realizan procesos importantes se encuentran completamente aislados y forman un cluster al cual solo tienen acceso usuarios autorizados y que generalmente son los administradores.	Se recomendó documentar este procedimiento y difundirlo entre los usuarios autorizados.
11.7	***Cómputo móvil y teletrabajo (trabajo remoto)***			
11.7.1	**Cómputo móvil y telecomunicaciones**	Debe existir un control que adopte las medidas de seguridad necesarias para proteger contra cualquier riesgo el uso de cómputo móvil, como por ejemplo: PDA (Ayudante personal digital), computadoras portátiles, teléfonos móviles, etc.	Existen medidas de seguridad para este tipo de acceso y es la DGSCA quien hace las recomendaciones.	Se sugirió al Instituto que existan medidas documentadas, además de política de seguridad y procedimientos que permitan evaluar, implementar y controlar adecuadamente estos aspectos en el caso de poseer accesos desde equipos móviles.
11.7.2	**Teletrabajo**	El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un	No aplica, no se hace proceso de información remoto. Los accesos	No aplica, no se realiza teletrabajo en el

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
		lugar fijo fuera de la organización. Se debe implementar la protección adecuada del sitio de trabajo remoto contra, por ejemplo: el robo de equipo e información, la divulgación no autorizada de información, el acceso remoto no autorizada a los sistemas internos de la organización o el uso inadecuado de los dispositivos e instalaciones.	remotos son para revisión de correo y la conexión se hace a través de enlaces con la UNAM.	Instituto, únicamente leer correo electrónico o consulta vía WEB.
12	***Adquisición, desarrollo y mantenimiento de sistemas de información***			
12.1	***Requisitos de seguridad de los sistemas de información***			
12.1.1	**Análisis y especificación de los requisitos de seguridad**	Las comunicaciones de requerimientos comerciales para nuevos sistemas o mejoras a los sistemas existentes deben especificar las necesidades de seguridad. Tales especificaciones deben considerar los controles automáticos a incorporar al sistema y la necesidad de controles manuales de apoyo. Se deben aplicar consideraciones similares al evaluar paquetes de software para aplicaciones comerciales. Si se considera adecuado, la administración puede utilizar productos certificados y evaluados en forma	Proyectos respectos sistemas (por ejemplo: robots y cuestiones de medicina) lo realizan investigadores tanto internos y con otras organizaciones.	Se recomendó al Instituto la necesidad de realizar un análisis de los requerimientos en seguridad que deben exigirse a los sistemas que desarrolla, desde el punto de vista en donde la seguridad sea una parte integral en el Instituto.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
		independiente. Los controles introducidos en la etapa de diseño son significativamente menos costosos de implementar y mantener que aquellos incluidos durante o después de la implementación.		
12.2	***Procesamiento correcto en aplicaciones***			
12.2.1	**Validación de los datos de entrada**	Los datos de entrada en sistemas de aplicación deben ser validados para asegurar que son correctos y apropiados.	Se cumple con las técnicas de validación, el programador cuenta con la capacitación necesaria.	Se recomendó al Instituto documentar dichas técnicas.
12.2.2	**Control de procesamiento interno**	Los datos que han sido correctamente ingresados pueden viciarse al procesar errores o a través de actos deliberados. Los controles de validación deben ser incorporados a los sistemas para detectar tal corrupción. El diseño de aplicaciones debe asegurar que las restricciones se implementen para minimizar los riesgos de fallas de procesamiento, conducentes a una pérdida de la integridad.	Se cumple con las técnicas de validación, el programador cuenta con la capacitación necesaria.	Se requiere documentar este punto.
12.2.3	**Integridad de mensajes**	La autenticación de mensajes es una técnica utilizada para detectar cambios no autorizados en el contenido de un mensaje	En casos críticos se utilizan técnicas de encriptación	Documentar estos controles internos en el procesamiento de

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
		transmitido electrónicamente, o para detectar alteraciones en el mismo. Puede implementarse en hardware o software que soporte un dispositivo físico de autenticación de mensajes o un algoritmo de software.		información para verificar o detectar cualquier corrupción de la información a través de los procesos, tanto por error como intencionales,
12.2.4	**Validación de los datos de salida**	La salida de datos de un sistema o aplicación debe ser validada para garantizar que el procesamiento de la información almacenada sea correcto y adecuado a las circunstancias. Normalmente, los sistemas se construyen suponiendo que si se ha llevado a cabo una validación, verificación y prueba apropiada, la salida siempre será correcta. Esto no siempre se cumple.	Se cumple con las técnicas de validación, el programador cuenta con la capacitación necesaria.	Revisar las técnicas o desarrollar mecanismos para asegurar que los datos procesados, y su posterior tratamiento o almacenamiento, sea apropiado a los requerimientos de la aplicación.
12.3	***Controles criptográficos***			
12.3.1	**Política de uso de los controles criptográficos**	Decidir si una solución criptográfica es apropiada, deber ser visto como parte de un proceso más amplio de evaluación de riesgos, para determinar el nivel de protección que debe darse a la información. Esta evaluación puede utilizarse posteriormente para determinar si un control criptográfico es adecuado, que	El Comité de Cómputo sugiere las técnicas criptográficas y cada usuario como responsable de su información.	Se recomendó al Instituto desarrollar un documento que cubra todos los temas sobre los los procesos criptográficos que utilizan.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
		tipo de control debe aplicarse y con que propósito, y los procesos de la empresa. Una organización debe desarrollar una política sobre el uso de controles criptográficos para la protección de su información. Dicha política es necesaria para maximizar beneficios y minimizar los riesgos que ocasiona el uso de técnicas criptográficas, y para evitar un uso inadecuado o incorrecto.		
12.3.2	**Administración de claves**	La administración de claves criptográficas es esencial para el uso eficaz de las técnicas criptográficas. Cualquier compromiso o pérdida de claves criptográficas puede conducir a un compromiso de la confidencialidad, autenticidad y/o integridad de la información. Se debe implementar un sistema de administración para respaldar el uso por parte de la organización.	Se cumple con las técnicas de validación, el programador cuenta con la capacitación necesaria.	El Instituto a través del documento anterior, será el que guié la actividad criptográfica en la dependencia y evitará constantes redundancias, sobre todo inconsistencias en la aplicación de claves.
12.4	***Seguridad de los archivos del sistema***			
12.4.1	**Control del software operativo**	El mantenimiento del software suministrado por el proveedor y utilizado en los sistemas operacionales debe contar con el soporte del mismo. Cualquier	El software comercial es administrado por la Unidad de Cómputo teniendo cuidado de su	Se recomendó al Instituto que utilice herramientas para robustecer los sistemas

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
		decisión referida a una actualización a una nueva versión debe tomar en cuenta la seguridad, por ejemplo: la introducción de una nueva funcionalidad de seguridad o el número y la gravedad de los problemas de seguridad que afecten esa versión. Los parches de software deben aplicarse cuando pueden ayudar a eliminar o reducir las debilidades en materia de seguridad.	respaldo, las actualizaciones y parches de seguridad.	operativos independientemente del tipo de sistemas de archivos, ya que requiere un esfuerzo técnico adicional
12.4.2	**Protección de los datos de prueba del sistema.**	Los datos de prueba deben ser protegidos y controlados. Las pruebas de aceptación del sistema normalmente requieren volúmenes considerables de datos de prueba, que sean tan cercanos como sea posible a los datos operativos. Se debe evitar el uso de bases de datos operativas que contengan información personal.	Los datos que se utilizan como pruebas son validados por el desarrollador, siendo el responsable del buen uso de los mismos.	Se sugirió que se realice un procedimiento para cumplir dicho control, además de que se difunda con los desarrolladores.
12.4.3	**Control de acceso al código fuente del programa**	Con el fin de reducir la probabilidad de alteración de programas, se debe mantener un control estricto del acceso a las bibliotecas de código fuente.	Los desarrolladores son responsables de no utilizar el código de sus sistemas para otros fines diferentes al proyecto.	Se sugirió colocar controles y auditorias periódicas y adecuadas sobre el código fuente de los sistemas de investigación desarrollados para evitar cualquier incidente de seguridad, así como documentarlo.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
12.5	***Seguridad en los procesos de desarrollo y soporte***			
12.5.1	**Procedimientos de control de cambios**	A fin de minimizar la alteración de los sistemas de información, debe existir un control estricto de la implementación de los cambios. Se debe imponer el cumplimiento de los procedimientos formales de control de cambios. Estos deben garantizar que no se comprometan los procedimientos de seguridad y control, que los programadores de soporte tengan acceso a partes del sistema necesarias para el desempeño de sus tareas, y que se obtenga un acuerdo y aprobación formal para cualquier cambio.	Se realiza de forma aislada.	Se sugiere que desarrollé un procedimiento de control de cambios de los sistemas de investigación.
12.5.2	**Revisión técnica de aplicaciones por cambios en el sistema operativo**	Periódicamente es necesario cambiar el sistema operativo, por ejemplo: instalar una versión nueva de software o parches. Cuando se realizan los cambios, los sistemas de aplicación deben ser revisados y probados a través de un control, para garantizar que no se produzca un impacto desfavorable en las operaciones o en la seguridad.	Esta función se realiza según los cambios que considera el investigador pertinente.	Documentar dicho procedimiento.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
12.5.3	**Restricciones en los cambios a los paquetes de software**	En la medida de lo posible no se debe realizar modificaciones a los paquetes de software. Los paquetes de software suministrados por proveedores deben ser utilizados sin modificación.	Generalmente no se realizan cambios a no ser que el desarrollador considere necesario.	Su recomienda documentar este punto.
12.5.4	**Fuga de información**	Deben existir controles en lugares estratégicos para prevenir fuga de información como por ejemplo: la supervisión regular de las actividades del personal y del sistema.	Se lleva a cabo la supervisión mediante solicitud de informes y verificación de los mismos.	Su recomienda documentar este punto.
12.5.5	**Desarrollo externo de software**	Cuando terceros desarrollan software, se deben considerar los siguientes puntos: a) acuerdos de licencias, propiedad de códigos y derechos de propiedad intelectual b) certificación de la calidad y precisión del trabajo llevado a cabo; c) acuerdos de custodia en caso de quiebra de la tercera parte; d) derechos de acceso a una auditoria de la calidad y precisión del trabajo realizado; e) requerimientos contractuales con respecto a la calidad del código; f) realización de pruebas previas a la instalación para detectar códigos troyanos.	No aplica.	No aplica, ya que el Instituto desarrolla sistemas de investigación y no a través de terceros.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
12.6	***Administración de vulnerabilidades técnicas***			
12.6.1	**Control de vulnerabilidades técnicas**	Si se obtienen oportunamente las vulnerabilidades de los sistemas de información. La organización tendrá que tomar medidas oportunas y efectivas asociadas a ese riesgo.	Constantemente se realizan revisiones de posibles vulnerabilidades en los sistemas desarrollados.	Se recomienda documentar dicho procedimiento.
13	***Gestión de incidentes de seguridad de la información***			
13.1	***Comunicación de eventos y debilidades de seguridad de la información***			
13.1.1	**Comunicación de eventos de seguridad de la información**	Los incidentes relacionados con la seguridad de la información, deberán ser comunicados a través de canales apropiados lo más rápido a la Dirección de la organización.	Cualquier situación que afecte la seguridad de la información es reportada a la Unidad de Cómputo para analizar y en su caso resolver el problema	Se desarrolló una Política de Seguridad (véase Apéndice B) sobre los incidentes de seguridad, además se recomendó documentar el procedimiento actual y que sea del conocimiento de los usuarios.
13.1.2	**Comunicación de debilidades de seguridad**	Debe existir un procedimiento que apoyé a todos los usuarios de los sistemas de información y los servicios sobre como divulgar cualquier debilidad observada en	El personal de la Unidad de Cómputo está inscrito en listas de seguridad mediante las cuales se reciben los avisos de	Se recomendó documentar dicho procedimiento, además de crear una metodología para la

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
		ellas.	vulnerabilidades y como protegerse.	generación, monitorización y seguimiento de reportes, los cuales deben reflejar, tanto eventos de seguridad como debilidades de los sistemas.
13.2	***Administración de incidencias y mejoras de la seguridad de la información***			
13.2.1	**Responsabilidades y procedimientos**	La Dirección debe establecer procedimientos rápidos y eficaces para los incidentes de seguridad que se puedan presentar en la organización. Se debe supervisar los sistemas, las alarmas para detectar incidentes de seguridad de la información.	La Dirección delega a la Comisión Local de seguridad y al Comité de Cómputo los procedimientos de seguridad quienes sesionan una vez al mes para verificar y retroalimentar procedimientos.	Se hace la observación que también debe llevarse una organización de los incidentes en la seguridad de la información que se hayan presentado como código malicioso, denegación de servicios, etc. todo orientado a problemas en la información y así generar planes de contingencia.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
13.2.2	**Aprender sobre las incidencias de seguridad de la información**	Debe existir un mecanismo para identificar y para cuantificar el tipo, volumen y costos de incidentes de la seguridad de la información. Dicha información evaluada de los incidentes de seguridad que se han presentado será utilizada para identificar incidentes que se repiten o de alto impacto.	Hasta el momento los incidentes ocurridos en el Instituto solo han representado suspensión temporal de servicios sin que esto signifique pérdida económica, de los incidentes se ha tomado ejemplo para mejorar los sistemas de seguridad.	Se recomienda crear procedimientos a partir de los incidentes que se hayan presentado aunque sean menores.
13.2.3	**Acumulación de evidencias**	Las acciones de seguimiento contra una persona o una organización después de un incidente de seguridad de la información implica la demanda legal (civil o criminal). Si la evidencia referente al incidente está registrada, se puede presentar como evidencia en cuestiones legales.	No aplica ya que nunca la afectación es mayor a los costos que pudiera representar el seguimiento y la implementación de una demanda.	Se sugiere al Instituto que documente los incidentes que se presenten y evaluar si en algún momento se debe tomar alguna acción sobre alguna persona.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
14	***Gestión de continuidad del negocio***			
14.1	***Aspectos de seguridad de la información en la administración de continuidad del negocio.***			
14.1.1	**Inclusión de la seguridad de la información en el proceso de la gestión de continuidad del negocio**	Se debe implementar un proceso controlado para el desarrollo y mantenimiento de la continuidad en toda la organización. Este proceso debe comprender todos los riesgos en la organización, identificar los activos críticos del negocio, identificar los impactos de incidentes, considerar la puesta en práctica de controles preventivos adicionales y de documentar los planes de la continuidad del negocio que tratan los requisitos de la seguridad.	El Instituto no cuenta con un plan de continuidad, pero ante eventos como un incendio o algún incidente natural, por ser parte de la UNAM, se apoya de dichos planes ya generados.	Se sugirió al Instituto desarrollar un Plan de continuidad, considerar en ese plan los procesos críticos que realiza la dependencia. Como un punto de partida se desarrollo una Política de Seguridad sobre este tópico. (véase Apéndice B)
14.1.2	**Continuidad del negocio y evaluación de riesgos**	La continuidad de los negocios debe comenzar por la identificación de eventos que puedan ocasionar interrupciones en los procesos de los negocios, por ejemplo: fallas en el equipo, inundación e incendio. Luego debe llevarse a cabo una evaluación de riesgos para determinar el impacto de dichas interrupciones, debe desarrollarse un plan estratégico para determinar como se debe abordar la continuidad de los	La Comisión Local de seguridad es el responsable de detectar y evaluar los eventos y/o riesgos que pueden causar problemas en la continuidad de la dependencia.	La Comisión deberá evaluar los riesgos que impacten la continuidad en las actividades del Instituto, cuyas consecuencias deberá determinar cómo asumir.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
		negocios.		
14.1.3	**Redacción e implantación de planes de continuidad que incluyan la seguridad de la información**	Los planes deben ser desarrollados para mantener o restablecer las operaciones de los negocios en los plazos requeridos una vez ocurrida una interrupción o falla en los procesos críticos de los negocios.	El Instituto sólo cuenta con planes aislados.	Se recomendó desarrollar medidas o determinaciones para solucionar, minimizar, mejorar o asumir esos riesgos, deberán expresarse por medio de planes de continuidad de negocio (o planes de contingencia), los cuales tienen el objetivo de mantener y restaurar el nivel operacional de la Dependencia.
14.1.4	**Marco para la planificación de la continuidad de los negocios**	Se debe mantener un solo marco para los planes de continuidad del negocio, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento. Cada plan de continuidad debe especificar claramente las condiciones para su puesta en marcha, así como las personas responsables de ejecutar cada componente del mismo.	Los planes con las que cuentan el IIMAS son a nivel Institucional.	El Instituto debe desarrollar planes a nivel dependencia con objetivos claros, delimitados y responsables, etc.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
14.1.5	**Prueba, mantenimiento y reevaluación de planes de continuidad**	Los planes de continuidad de los negocios pueden fallar en el curso de las pruebas, frecuentemente debido a suposiciones incorrectas, negligencias o cambios en el equipamiento o el personal. Por consiguiente deben ser probados periódicamente para garantizar que están actualizados y sean eficaces. Las pruebas también deben garantizar que todos los miembros del equipo de recuperación y demás personal relevante estén al corriente de los planes.	Las pruebas que se realizan son planes de contingencia a nivel Institucional.	Una vez que se tengan los planes del punto anterior, deberán ser puestas a prueba para mantenerlo vigente y actualizarlo si lo requiere, así como también las del nivel Institucional.
15	***Conformidad***			
15.1	***Conformidad con los requisitos legales***			
15.1.1	**Identificación de la legislación aplicable**	Se deben definir y documentar claramente todos los requisitos legales, normativos y contractuales pertinentes para cada sistema de información. Del mismo modo deben definirse y documentarse los controles específicos y las responsabilidades individuales para cumplir con dichos requisitos.	El Instituto como dependencia de la UNAM se rige de la legislación de la Universidad.	Se sugiere identificar la legislación informática vigente que pueda ser aplicable al Instituto definiendo explícitamente y documentando todo lo que guarde relación con la seguridad de la información.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
15.1.2	**Derechos de propiedad intelectual (IPR)**	Se deben implementar procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material respecto del cual puedan existir derechos de propiedad intelectual, derechos de diseño o marcas registradas. La infracción de derechos de autor (derecho de propiedad intelectual) puede tener como resultado acciones legales que podrían derivar en demandas penales. Los requisitos legales, normativos y contractuales pueden poner restricciones a la copia de material que constituya propiedad de una empresa. En particular, pueden requerir que sólo pueda utilizarse material desarrollado por la organización, o material autorizado o suministrado a la misma por la empresa que lo ha desarrollado.	El Instituto como dependencia de la UNAM depende de los procedimientos que esta dicta para el registro de propiedad intelectual incluyendo las recomendaciones de seguridad que implica.	Otro parte importante por considerar de esté control es lo relacionado con los derechos de propiedad intelectual, debiendo generar procedimientos que aseguren el cumplimiento de las regulaciones para mantener los derechos de autor de los investigadores que desarrollan material científico.
15.1.3	**Protección de registros de la organización.**	Los registros importantes de la organización deben protegerse contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales del negocio.	Los recursos son resguardados por cada dueño y usuario de la información en el Instituto.	Se recomienda desarrollar procedimientos en donde se guarden los registros de algún tipo de información clasificada desde el punto de vista Legal.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
15.1.4	**Protección de datos y privacidad de la información personal.**	Diversos países han introducido leyes que establecen controles sobre el procesamiento y transmisión de datos personales (generalmente información sobre personas que pueden ser identificadas a partir de esta información). Dichos controles pueden imponer responsabilidades a aquellas personas que recopilan, procesan y divulgan información personal, y pueden limitar la capacidad de transferir dichos datos.	El Instituto a través de los dueños o usuarios de la información son los responsables de resguardar la información que utilizan	Se debe generar un procedimiento o mecanismo en la cual todos los registros de información, deben ser protegidos para evitar pérdidas, alteraciones y un aspecto muy importante: la divulgación inadecuada, y esto ya es una regulación generalizada en muchos países.
15.1.5	**Prevención del uso inadecuado de los recursos de procesamiento de información**	Los recursos de procesamiento de información de una organización se suministran con propósitos de la organización. Se debe autorizar el uso que se da a los mismos. La utilización de estos recursos con propósitos no autorizados o ajenos a los objetivos de la organización, sin la aprobación de la Dirección, debe ser considerada como uso indebido. Si dicha actividad es identificada mediante monitoreo u otros medios, se debe notificar al responsable para que se tomen las acciones disciplinarias que correspondan.	Al igual que el punto anterior cada usuario y dueño del procesamiento de información, es responsable de su uso.	Se sugirió prevenir el procesamiento incorrecto, ya que quedan expuestos (memorias temporales permanencia exterior, o transmisión insegura, etc.) Por lo tanto, para todo registro deberá ser identificado, analizado, y documentado

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
15.1.6	**Regulación de controles para el uso de criptografía**	Algunos países han implementado acuerdos, leyes, normas y demás instrumentos para controlar el acceso a los controles criptográficos o el uso de los mismos	El uso de criptografía dentro del Instituto es propuesto por el Comité Interno de Cómputo y cada usuario es responsable del uso.	El empleo de claves por parte de los usuarios y administradores de sistemas,.es muy pocas veces considerado en las organizaciones, debido a la deficiente política de derechos y obligación legales de la organización hacia sus empleados ya que muchos de ellos únicamente tienen la capacidad de acceso/control a las infraestructura, y/o descifrar información. Esto es un aspecto legal que debe ser claramente definido y puesto en conocimiento del personal.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
15.2	***Conformidad con políticas y normas de seguridad y conformidad técnica***			
15.2.1	**Conformidad con políticas y normas de seguridad**	La Dirección debe garantizar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad. Asimismo, se debe considerar la implementación de una revisión periódica de todas las áreas de la organización para garantizar el cumplimiento de las políticas y estándares de seguridad.	Todos los usuarios son responsables de su información y deben llevar a cabo el proceso de información de acuerdo a los lineamientos del Instituto.	Este punto trata de hacer hincapié en el control del cumplimiento de estas medidas, pues de nada sirve tener todo en regla con los aspectos legales, si luego el personal involucrado no da cumplimiento a las medidas y en definitiva, la seguridad falla.
15.2.2	**Verificación de la compatibilidad técnica**	Se debe verificar periódicamente la compatibilidad de los sistemas de información con los estándares de implementación de la seguridad. La verificación de la compatibilidad técnica comprende la revisión de los sistemas operacionales a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. Este tipo de verificación de cumplimiento requiere asistencia técnica especializada. Debe ser realizada manualmente (si es necesario, con el apoyo de adecuadas herramientas de software) que genere un	Aunque no existe un procedimiento o control que verifique la compatibilidad técnica, periódicamente los usuarios revisan dicho cumplimento.	Para evitar está incompatibilidad se debe asegurar que todos estos procedimientos se cumplan y verificar que sean aplicables y estén de acuerdo con toda la organización, además de documentarlo.

Estándar	Controles	La norma requiere	Estado Actual en el IIMAS	Medidas adoptadas y recomendadas después de la investigación
		informe técnico para su interpretación por parte de un especialista.		
15.3	***Consideraciones sobre la auditoria de sistemas de información***			
15.3.1	**Controles de auditoria de sistemas**	Los requerimientos y actividades de auditoria que involucran verificaciones de los sistemas operacionales deben ser cuidadosamente planificados y acordados a fin de minimizar el riesgo de discontinuidad de los procesos de negocio.	El software que se llega a desarrollar es para usos de investigación y en muy pocas ocasiones se llega a auditar.	Se recomienda utilizar herramientas de auditoría que puede servir para detectar puntos importantes en cuestiones de seguridad.
15.3.2	**Protección de las herramientas de auditoria de sistemas**	Se debe proteger el acceso a las herramientas de auditoria de sistemas, por ejemplo: archivos de datos o software, a fin de evitar el mal uso o el compromiso de las mismas. Dichas herramientas deben estar separadas de los sistemas operacionales y de desarrollo y no deben almacenarse en bibliotecas de cintas o en áreas de usuarios, a menos que se les otorgue un nivel adecuado de protección adicional.	No aplica, no se cuentas con herramientas de auditoría.	El empleo de una herramienta de auditoría de seguridad debe ser perfectamente regulado, en cuanto a su alcance, profundidad, potencialidad, horario, fechas, tiempo de operación, objetivo, resultados deseados, etc.

Apéndice B

Política General de Seguridad de la Información

PRESENTACIÓN

Las políticas que aquí se presentan tienen como objetivo tanto el de preservar en condiciones óptimas la información e infraestructura de cómputo del Instituto, así como establecer controles preventivos básicos en materia de seguridad de la información. Asimismo, se han detallado un conjunto de lineamientos que deberán ser observados para el aseguramiento de la información. Es por ello que se invita a adoptar este modelo como una norma de trabajo en las responsabilidades diarias, además que exista un compromiso con el aseguramiento de la información; y que este esfuerzo ayude a servir mejor y enorgullezca pertenecer a una Institución que cultiva valores de integridad, ética y transparencia.

POLÍTICA

Todo el personal (investigadores, académicos, alumnos, empleados y usuarios) del Instituto de Investigaciones en Matemáticas Aplicadas y en Sistemas (IIMAS) debe laborar dentro de un ambiente de trabajo que garantice la confidencialidad, integridad y disponibilidad de la información. El incumplimiento accidental o deliberado de las políticas descritas en este documento, será considerado una falta administrativa y tendrá consecuencias, dependiendo de la gravedad de la falta.

OBJETIVO

Las Políticas Generales de Seguridad tienen como objetivo establecer las directrices para poder cumplir con la misión y visión de seguridad de la información para el Instituto de Investigaciones Matemáticas Aplicadas y en Sistemas (IIMAS).

LINEAMIENTOS

1. Propiedades de la información

a. La seguridad de la información debe contemplar la implantación de controles de acuerdo a los siguientes criterios:

- Grado de **confidencialidad**, determinado por el daño o pérdida que puede tener el Instituto ante un acceso o divulgación de información no autorizada.
- Grado de **integridad**, determinado por el daño o pérdida que puede tener el Instituto ante la inexactitud de la información.
- Grado de **disponibilidad**, determinado por el daño o pérdida que puede tener el Instituto frente a la no-disponibilidad de la información cuando ésta sea requerida.

b. El término **información** incluye los expedientes, reportes, estudios, resoluciones, actas, investigaciones, desarrollos, oficios, correspondencia, acuerdos, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro tipo de registro que documente el ejercicio de las facultades o la actividad de la Dependencia, sin importar su fuente o fecha de elaboración.

c. La **información** que debe protegerse puede estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico.

d. Esta política se aplica a todas las manifestaciones de la **información** sin tomar en cuenta la forma ni el formato, así como a todos los recursos para el transporte de la misma.

e. El nivel de protección de la **información** debe estar basado en un proceso de análisis que contemple la valoración de amenazas, vulnerabilidades, probabilidad e impacto de los riesgos asociados a ésta.

2. Gestión de la seguridad

Para establecer una gestión de la seguridad se debe:

a. Diseñar un plan estratégico de seguridad de la información, el cual deberá ser revisado y actualizado anualmente.

b. Crear y mantener un grupo de políticas, estándares, guías y procedimientos de seguridad de la información que estén dirigidos hacía todos los niveles jerárquicos del Instituto.

c. Definir un plan de concienciación para asegurar el éxito de las iniciativas en materia de seguridad de la información.

d. Estructurar un esquema de clasificación de la información para establecer los niveles de protección de ésta.

e. Asegurar la división de funciones en el desempeño de las tareas relevantes de seguridad de la información, para ello se deben establecer los siguientes roles y responsabilidades:

i. **Dueño ó Propietario**: Tiene la responsabilidad de la clasificación de los activos de información, contando con la autoridad para definir el alcance de acceso a la información, para negar o permitir su consulta, su creación o actualización, su borrado o destrucción.

A continuación se describen las responsabilidades de los dueños de la información en cuanto a seguridad se refiere:

a. Identificar los activos de información de su propiedad.

b. Clasificar la información con base a su confidencialidad, integridad y disponibilidad.

c. Responsabilidad de valorar los riesgos asociados a la información.

d. Aprobar o rechazar la solicitud de accesos a la información.

e. Impulsar las sanciones para los accesos no autorizados, de acuerdo con su naturaleza y los daños ocasionados.

ii. **Custodio de la información**. Persona que tiene la responsabilidad de establecer y mantener los controles de seguridad adecuados en los sistemas de información, con base en el nivel de protección.

A continuación se describen las responsabilidades de los custodios de la información en cuanto a seguridad se refiere:

a. Administrar accesos a nivel de red (sistema operativo).

b. Administrar accesos a nivel de bases de datos.

c. Desarrollar procedimientos de autorización y autenticación.

d. Monitorear el cumplimiento de la política y procedimientos de seguridad en los activos de información que custodia.

e. Capacitar a los usuarios en aspectos de seguridad en nuevas tecnologías o sistemas implantados bajo su custodia.

f. Revisar periódicamente la información a su cargo para detectar amenazas o vulnerabilidades de seguridad o según instrucciones del área correspondiente.

g. Dar soporte para respuesta a incidentes de seguridad.

h. Mantener la confidencialidad, integridad y disponibilidad de los sistemas de información.

i. Redactar los procedimientos de operación y de respuesta a incidentes así como el plan de contingencia asociado.

j. Implementar controles definidos para los sistemas de información, incluyendo investigación e implementación de actualizaciones de seguridad de los sistemas (service pack, fixes, etc.)
iii. **Usuario de la información**. Persona que requiere de la autorización de los custodios para acceder a la información y poder realizar su función dentro del Instituto, a través de los recursos asignados y de la normatividad existente.

A continuación se describen las responsabilidades de los usuarios de la información en cuanto a seguridad se refiere:
a. Buen uso de su cuenta y contraseña asignada, equipo de cómputo asignado y medios magnéticos de transmisión de información.
b. Utilizar los sistemas de Información sólo para actividades relacionadas con las funciones de la organización.
c. No divulgar información clasificada sin autorización.
d. Conocer la clasificación de los activos de información que maneja.
e. El Instituto debe contar con un área encargada de la coordinación, implementación, monitoreo y mantenimiento de los mecanismos de seguridad de la información, asignación, roles y responsabilidades, así como la generación y difusión oportuna de la normatividad de seguridad de la información, definiendo sus procedimientos y relaciones entre las diferentes áreas de la Institución.
f. Mantener confidencial la cuenta y contraseña asignada.

3. Propiedad y uso de recursos de procesamiento de información

a. El Instituto considera los recursos de procesamiento de información como prioritarios para el ejercicio de sus funciones; por lo cual todos los usuarios de dichos recursos son responsables de dar buen uso.
b. Los recursos de procesamiento de información están diseñados para ser utilizados únicamente con fines relacionados con las actividades del Instituto.
c. Al terminar la relación laboral de una persona, los recursos de procesamiento de la información sea usuario, dueño o custodio de la Dependencia deben ser devueltos en buenas condiciones de operación, con toda la documentación original, medios de almacenaje y equipo periférico.
d. Los usuarios que utilizan herramientas de procesamiento de información de oficina (hojas de cálculo, procesamiento de palabras, etc.) son los responsables de garantizar la exactitud e integridad de los resultados obtenidos de dichas herramientas cuando éstas sean utilizadas para dar apoyo a la operación de los procesos que realiza el Instituto.

4. Definición y Actualización de la Política de la Organización

a. La Política General de Seguridad de la Información, se debe revisar y actualizar cuando ocurran cambios tecnológicos, en la misión de la Institución o por lo menos una vez cada año.

5. Clasificación y Control de Activos de Información

a. Toda la información utilizada por el Instituto debe contar con una clasificación de acuerdo al impacto en los procesos críticos de la organización, considerando aspectos como confidencialidad, integridad y disponibilidad.
b. La información debe ser etiquetada de acuerdo a su nivel de clasificación.

6. Seguridad para el Personal

a. Todo el personal contratado para aquellos cargos en donde se maneje información de tipo confidencial para la Dependencia debe ser evaluado y aprobado antes de laborar en ella.

b. El Instituto debe proporcionar entrenamiento a todo el personal sobre las medidas de seguridad de la información necesarias para minimizar riesgos sobre ésta.

c. Todo el personal, debe reportar inmediatamente cualquier incidente relacionado con fallas o comportamientos extraños en sistemas cuya operación puede tener un impacto sobre la seguridad de la información.

7. Seguridad Física y Ambiental

a. El acceso a las instalaciones del Instituto debe contar con los mecanismos de control que permitan asegurar que el personal que ingrese a las instalaciones tenga la autorización correspondiente.

b. Las áreas de cómputo de la Dependencia deben operar en áreas restringidas, en las cuales sólo puede acceder personal autorizado.

c. Cumplir con las medidas de seguridad física que ayuden a mantener en buen estado los equipos de cómputo y de comunicaciones, así como las instalaciones y los centros de cómputo.

8. Administración de Redes, Comunicaciones y Operaciones

a. Tener mecanismos de control para proteger toda la información que se opere en la infraestructura tecnológica de la Dependencia, que prevengan y detecten posibles intrusiones o robos a la información, y que de igual forma protejan toda aquella información con carácter confidencial que por necesidades de la Institución deba viajar ya sea a través de la red interna, redes externas o hacia otras redes incluyendo Internet.

b. Proteger la información residente en los equipos de cómputo de cualquier tipo de código malicioso (virus computacionales, caballos de Troya, gusanos de red, entre otros), los empleados de la Dependencia que hagan uso de equipo de cómputo, deben estar conscientes de todas las medidas para la prevención de virus informáticos.

9. Control de Acceso Lógico

a. El acceso a la información y a la infraestructura tecnológica de la Dependencia debe contar con mecanismos de control de acceso que permitan cumplir con los principios de prueba de identidad y responsabilidad.

b. Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado (cuenta de usuario y contraseña, biométrico, tarjeta inteligente), para acceder a los sistemas de información y a la infraestructura tecnológica de la Dependencia, por lo cual deberá mantenerlo de forma confidencial.

c. Es responsabilidad de los administradores de sistemas de información evaluar, proponer, asegurar que se implementen y monitoreen todos aquellos mecanismos de control de acceso que prevengan la intrusión no autorizada a la infraestructura del Instituto (red, sistemas operativos, bases de datos y aplicaciones).

10. Desarrollo y Mantenimiento de Sistemas

a. Todos los sistemas deben ser desarrollados con base en una metodología probada y apegada a estándares. Asimismo, se debe contar con procedimientos de control de

cambios en los sistemas así como en el proceso de implantación en producción de los mismos.

b. Los sistemas deben contar con controles de validación y edición de datos, de procesamiento y de salida, que garanticen que únicamente información válida, completa y correcta será procesada.
c. Los sistemas de información desarrollados internamente o adquiridos deben contar con los controles internos que garanticen la seguridad de los datos, y el registro de las actividades que los usuarios realizan en éstos.

11. Continuidad del Negocio y Recuperación ante Desastres

a. El IIMAS debe contar con un Plan de Continuidad, que permita garantizar que los procesos críticos de la Dependencia operen en caso de presentarse un desastre o contingencia que imposibilite su operación normal.
b. Nombrar a un coordinador o grupo de trabajo responsable del desarrollo, implantación, ejecución, pruebas y actualización del Plan de Continuidad.
c. Todo el personal del Instituto debe conocer la responsabilidad que se le ha asignado en el Plan de Continuidad, así como los procedimientos a ejecutar en dicho plan, para lo cual se debe establecer un programa de capacitación y entrenamiento periódico.

12. Cumplimiento

a. Todos los recursos de procesamiento de información (el software y hardware adquirido por el Instituto) son propiedad de la UNAM, independientemente de la asignación al personal o al equipo de trabajo en la que se instale.
b. Bajo ninguna circunstancia una persona puede instalar, utilizar o almacenar juegos u otro tipo de software no autorizado en ningún equipo de cómputo de trabajo o dispositivo de red de la Dependencia. La piratería de software es un delito federal bajo la Ley de Derechos de Autor, e implica sanciones penales, incluyendo multas y encarcelamiento.

El Instituto no tolerará el uso ilegal la copia o distribución de software no autorizado bajo ninguna circunstancia. La duplicación de software autorizado (excepto para fines de respaldo) está estrictamente prohibida.

13. Código de Conducta

a. Todo el personal de la Dependencia debe conocer los lineamientos de conducta relacionados con el manejo de la información que dicte la Dependencia.
b. No cometer o formar parte de actos ilícitos o no éticos que puedan llegar a afectar de forma negativa la reputación del Instituto.
c. Asumir el compromiso de notificar por los medios autorizados cualquier actividad relacionada que considere ilícita y cooperar en cualquier investigación que se derive de esta notificación.
d. Hacerse cargo del compromiso de ayudar en los esfuerzos relacionados con el entendimiento y aceptación de las medidas de seguridad adoptadas por la dependencia.
e. Adquirir el compromiso de no hacer mal uso de la información y los recursos antes, durante y después de la ejecución de las actividades.
f. El sentido de estas políticas se refiere a que todo lo no está explícitamente permitido está prohibido.

1. Administración de riesgos.

Diseñar una administración de riesgos que permita mitigar los riesgos, implementando los controles pertinentes que aseguren la operación del IIMAS.

Objetivo

Esta política describe las acciones que deben realizarse para llevar a cabo la identificación y monitoreo de amenazas, riesgos y controles de seguridad de los activos informáticos, con la finalidad de desarrollar un análisis de riesgos.

Responsable:

El grupo de administradores de riesgos (GAR) serán los responsables de desempeñar la presente política.

Alcance

Administración de Riesgos.

Generales.

a. Nombrar un grupo de administradores de los sistemas de información que tiene la Dependencia y entre sus actividades se debe encontrar lo siguiente:

- Guía para la administración de riesgos.
- Actividades de administración y análisis de riesgos en la Dependencia.
- Promover la seguridad práctica y la protección de los activos de información tomando como base su confidencialidad, integridad y disponibilidad.

b. Todos los usuarios tienen la responsabilidad de participar en las actividades de administración de riesgos, cuando el grupo de administración se los solicite.

Análisis de Riesgos.

a. El análisis de riesgos debe ser realizarse considerando los siguientes puntos:

- Infraestructura.
- Gente.
- Procesos.

b. Llevar a cabo procesos de identificación y valoración de vulnerabilidades por parte del grupo de administradores.

c. El grupo de administradores debe crear un programa para identificar nuevas amenazas que puedan afectar al Instituto, como amenazas se deben tomar en cuenta las siguientes clases:

- Gente interna.
- Gente Externa.
- Código malicioso.
- Errores humanos.

d. El análisis de riesgos debe considerar la eficacia de las medidas de seguridad implementadas y se deben tomar en cuenta las tendencias de incidentes de seguridad sucedidos.

e. Contar con documentación sobre los análisis de riesgos valorados y debe estar a disposición de los integrantes del grupo de administración.

Determinación y Aceptación de los riesgos.
a. El propósito principal de un análisis de riesgos es identificar los riesgos y tomar medidas para minimizarlos, controlarlos o concluirlos. El resultado de estos riesgos debe ser del conocimiento de los dueños de los activos de información, los cuales tiene la responsabilidad de implementar los controles recomendados.
b. Los dueños de los activos de información deben estar conscientes de los riesgos, cuáles son posibles de controlar y cuáles no, con base en la operación del Instituto.
c. Se tiene que documentar toda la información referente a la administración de riesgos y elaborar un informe.
d. Los resultados del análisis de riesgos deben ser del conocimiento del grupo de administradores.

2.- Roles y responsabilidades

Para el correcto seguimiento de las Políticas de Seguridad, se deben conformar roles y grupos de trabajo los cuales estén encargados de la seguridad del IIMAS.

Objetivo

Esta política establece la creación de roles ejecutivos y operativos, su conformación y funciones para la correcta aplicación de las políticas.

Responsable:

La comisión de seguridad de la información será el responsable de supervisar la política.

Alcance

Esta política contempla tres niveles:

- Los roles y responsabilidades a nivel estratégico, que son los grupos que se encargan de la gestión de la seguridad de la información.
- Los roles y responsabilidades a nivel táctico que tienen la responsabilidad de administrar al personal operativo e informar al nivel estratégico sobre indicadores de desempeño de los controles de seguridad.
- Los roles y responsabilidades a nivel operativo que son los grupos que se encargarán de que se lleven a cabo los controles de seguridad establecidos.

Es importante mencionar que un rol es una función y no una posición dentro de una organización, por lo cual los roles de seguridad no se contraponen con las posiciones dentro de la dependencia.

Roles y Responsabilidades Estratégicos:

Comité de Seguridad de la Información (CSI):
Conformar un Comité de seguridad de la Información, que lleve a cabo las funciones del proceso de administración de riesgos, la validación de la estrategia de seguridad y de supervisar el seguimiento de las Políticas de Seguridad.

Este comité debe estar integrado por el Director, coordinador técnico y administradores de sistemas de información de la Dependencia y debe de contar con las siguientes responsabilidades:

a. Validar la estrategia institucional en materia de seguridad de la información.
b. Establecer la visión corporativa de seguridad así como la dirección para el desarrollo y evolución de la seguridad dentro de la dependencia.
c. Autorizar la disposición de recursos humanos, hardware y software necesarios para la adecuada implantación de las Políticas de Seguridad.
d. Asegurar el soporte a iniciativas en materia de seguridad de la información, acordes con los programas institucionales.
d. Promover la seguridad de la información en la Dependencia
e. Identificar y priorizar los riesgos que puedan afectar la seguridad de la información propiedad del Instituto.
f. Proveer de los medios para capacitar al personal de la Dependencia en materia de Seguridad de la información.
g. Promover las revisiones internas que aseguren la efectividad de las acciones en materia de seguridad de la información.
h. Aprobar iniciativas que promuevan la mejora continua de la seguridad de la información.

Oficial de Seguridad de Información
Nombrar una persona que lleve a cabo las funciones de definir las directrices institucionales de seguridad y aprobar la asignación de recursos materiales, humanos y financieros en materia de seguridad de la información.

A continuación se enumeran sus responsabilidades:
a. Apoyar y generar el plan general de seguridad para la Dependencia.
b. Aprobar y revisar proyectos sobre seguridad de la información.
c. Justificar la definición roles y responsabilidades específicos que se relacionen a la seguridad de la información.
d. Definir el uso de metodología y procesos específicos para la seguridad de la información.
e. Asegurar que se promueva la seguridad de la información en la Dependencia.
f. Revisar las políticas, estándares, procedimientos y lineamientos de seguridad informática para la Dependencia.
h. Representar a la Dependencia, en materia de seguridad de la información en foros, comités, instituciones y entidades publicas y privadas, tanto nacionales como internacionales, y coordinar los grupos de trabajo internos en dicha materia.

Oficial de la Infraestructura de Seguridad de la Información
Nombrar un responsable para coordinar e implementar acciones preventivas para proteger la infraestructura tecnológica y continuidad operativa de los sistemas que soportan los procesos críticos del Instituto, a través de la identificación de riesgos, vulnerabilidades y amenazas externas, considerando su impacto a la Dependencia.

Sus responsabilidades son:
a. Capacitar y crear hábitos de seguridad informática entre el personal.
b. Identificar riesgos externos que puedan impactar a la infraestructura tecnológica (código malicioso, vulnerabilidades) e implementar acciones correctivas minimizarlos apropiadamente.

c. Analizar el comportamiento de los usuarios de la infraestructura tecnológica para poder prevenir incidentes internos de seguridad informática.
d. Interactuar con otros oficiales de seguridad y grupos de trabajo operativos para la administración de la seguridad.

Roles y Responsabilidades Tácticos:

Responsable de Seguridad de información

Nombrar una persona que tenga la función de coordinar las actividades técnicas y operativas para la implantación de las directrices de seguridad de la información establecidas con los oficiales estratégicos. Debe coordinar las labores de monitoreo y respuesta a incidentes de la seguridad en la infraestructura tecnológica junto con el área de seguridad de la UNAM; así como de llevar a cabo el diseño de la normatividad en materia de seguridad. Entre sus responsabilidades se encuentran:
a. Coordinar la implantación de medidas específicas de seguridad de la información cuando aplique.
b. Participar en la planeación de la seguridad junto con los oficiales de seguridad.
c. Desarrollar políticas, estándares, procedimientos y lineamientos de seguridad informática para la Dependencia.
d. Coordinar los esfuerzos para normar la seguridad de la información dentro de las áreas de la Dependencia.
e. Apoyar en el diseño, implementación y mantenimiento del plan/programa de seguridad de la información de la Dependencia.

Grupo de Administración de Riesgos (GAR):

Nombrar un grupo de administración de riesgos, el cual debe de evaluar y analizar los riesgos relacionados con la generación, procesamiento y almacenamiento de la información en los procesos críticos del Instituto. Además de coordinarse y apoyarse con el área de seguridad de la UNAM.

Este grupo debe contar con las siguientes responsabilidades:
a. Definir e implementar la metodología a seguir en la realización del diagnóstico de riesgos apoyándose del área de seguridad.
b. Planear la periodicidad con que se llevará a cabo el diagnóstico de riesgos.
c. Proponer los controles de seguridad acordes a las necesidades de la Dependencia.
d. Generar un reporte ejecutivo de los resultados obtenidos en el diagnóstico de riesgos.

Roles y Responsabilidades Operativos:

Grupo de Monitoreo de Seguridad (GM):

Nombrar un grupo de monitoreo de seguridad que debe implantar los procesos de registro de bitácoras y logs para generar estadísticas que permitan la afinación de indicadores y medidas de seguridad, detectar comportamientos de controles incompletos o posibles violaciones o debilidades de seguridad, definir mejoras a los sistemas y / o a los controles de protección de activos.
Las siguientes responsabilidades son:
a. Ejecutar el proceso de monitoreo de seguridad para identificar incidentes.
b. Realizar el monitoreo de los controles establecidos para el cumplimiento de las políticas de seguridad.
c. Iniciar el proceso de respuesta a incidentes de seguridad al detectarse una desviación dentro de la operación.
d. Llevar la administración de vulnerabilidades.

e. Definir el proceso de registro de eventos (bitácoras) de los sistemas de información.
f. Revisar las bitácoras de los sistemas de información con el objetivo de identificar a los responsables de incidentes.

Responsabilidades de Seguridad en el Desarrollo y Mantenimiento de Sistemas (RDS):
Nombrar un grupo de desarrollo de sistemas, el cual debe verificar que los sistemas de información, cuenten con los lineamientos de seguridad adecuados, durante su desarrollo, adquisición e implantación.
Las responsabilidades deben realizar lo siguiente:
a. Desarrollar, integrar y mantener los controles de seguridad en los sistemas de información.
b. Separar los ambientes de desarrollo y producción.
c. Supervisar que en el desarrollo e implementación de los sistemas se tome en cuenta a la seguridad de la información.

3.- Seguridad en el Personal.

Contar con medidas de seguridad que permitan reducir los riesgos asociados al personal que labora en el Instituto.

Objetivo
Determinar los requerimientos de seguridad informática que el personal que labora en la Dependencia debe cumplir.

Responsable
El Comité, y el oficial de seguridad tendrán la responsabilidad de la seguridad del personal en el Instituto.

Alcance
Esta política contempla los requerimientos que tiene el personal de la Dependencia, sobre la protección de la información. En esta política se deben evaluar los siguientes tópicos:

- Seguridad en las responsabilidades de trabajo.
- Revisión histórica de empleados.
- Contratos.
- Términos y condiciones de los empleados.
- Capacitación.

Seguridad en el Personal
Generales.
1. El personal que labora en la Dependencia tiene la obligación de seguir cualquier normatividad que el IIMAS establezca en materia de seguridad de la información.
2. Considerar dentro de las responsabilidades diarias de trabajo del personal de la Dependencia, la seguridad de la información.

Acuerdos de Confidencialidad.
a. Los empleados y proveedores deben de contar con contratos de confidencialidad que permitan asegurar la información de la Dependencia

Capacitación en seguridad de la información.

Capacitación.

a. Todo el personal del IIMAS debe recibir capacitación periódica (1 vez al año) para concienciar sobre problemas de seguridad de la información.

Cultura de Seguridad.

a. Los usuarios del Instituto deben recibir capacitación periódica (1 vez al año) para conocer sobre cultura de seguridad de la información.

Recordatorios.

a. Estructurar métodos que permitan afianzar la cultura de seguridad en el personal como:

- Correos electrónicos.
- Promover videos institucionales.
- Promover pláticas de seguridad
- Promover carteles o trípticos en materia de seguridad.

4.- Clasificación de la información.

Debido a la importancia de la información en el Instituto, se deben llevar a cabo lineamientos que se encarguen de asegurarla, con base en su manejo y la cual debe ser publicada para conocimiento de los propietarios de activos de información y responsables de seguridad de la información.

Objetivo

El objetivo de esta política es establecer los lineamientos de seguridad para la protección de la información del Instituto, con base en los niveles de clasificación de impacto.

Responsable

La clasificación de la información debe realizarse por los dueños de los activos junto con los demás grupos de seguridad.

Alcance

La clasificación de los activos de información debe llevarse a cabo en función de las siguientes variables, según el marco de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG):

- Confidencial
- Reservado
- Pública

Guía de Clasificación y Valuación de Información.

Generales

a. Se debe contar con una guía de clasificación y valuación de información que soporte los lineamientos de esta política.

b. El propósito de la guía de clasificación y valuación de información, debe ser proporcionar los requerimientos mínimos de seguridad para la protección de la información abarcando los siguientes temas:

- Lineamientos de clasificación.
- Clasificación y manipulación de la información
- Seguridad de los medios transferibles.

Inventario de Activos de Información:

Generales

a. Para la clasificación y valuación de la información se debe llevar a cabo primero un inventario de activos de información, con base en los procesos del Instituto.

Criterios de clasificación y valuación de información.

Generales

a. Todos los activos informáticos deben estar clasificados con base al impacto que representan.
b. Los dueños de los activos de información deben responsabilizarse de las necesidades de la organización para clasificar, valuar y compartir o restringir información, así como del impacto al negocio asociado con estas necesidades.
c. Para la incorporación de activos de información al inventario, se debe asignar una clasificación de seguridad y debe ser proporcionada por el dueño del activo.

Clase de información	Características	Accesos
Pública	Está disponible para quien la solicite (mediante los canales autorizados), sin restricciones.	Todos los usuarios autorizados a los sistemas de información
Reservada	No se debe dar a conocer a los empleados, el hacerlo podría perjudicar a terceros (personas, empresas o instituciones)	Algunos usuarios que tienen algún privilegio o derecho a los sistemas de información dentro del Instituto.
Confidencial	No se debe dar a conocer a los empleados, para proteger datos personales.	El acceso sólo será a -Autorización del dueño de la información. o Información de investigaciones y/o desarrollos. o Información sensible al Instituto.

Clasificación y valuación de Hardware y Software (Aplicaciones, Administradores de TI)

a. En el documento guía, se debe definir la clasificación y valuación de hardware y software, con base en su confidencialidad, integridad y disponibilidad.

Dispositivos que transmiten información.

a. En la guía de clasificación y valuación de la información, se debe definir la clasificación de los dispositivos que transmiten información (VPN, Router, Switch).

Dispositivos que almacenan información.

a. En la guía de clasificación y valuación de la información, se debe definir la clasificación de los dispositivos que almacenan información (discos, unidades de respaldo).

Dispositivos que procesan información.
a. En la guía de clasificación y valuación de la información, se debe definir la clasificación de los dispositivos que procesan información (aplicaciones y servicios).

Reclasificación de la Información.

Generales
a. Se debe llevar a cabo un proceso de reclasificación de la información, con base a los puntos estipulados en la guía de clasificación y valuación de la información.

Envió (Transferencia) de la Información.

Generales
a. En la guía de clasificación y valuación de la información, se debe definir las acciones para el envió de información, de acuerdo a su propiedad de confidencialidad.

Eliminación de la Información.

Generales
a. En la guía de clasificación y valuación de la información, se debe definir las acciones para la eliminación de información, de acuerdo a su propiedad de confidencialidad y medio de almacenamiento.

Etiquetado de la Información.

Generales
b. En la guía de clasificación y valuación de la información, se debe definir las acciones para etiquetar la información, de acuerdo a su propiedad. Es decir, que toda la información debe llevar asociada su clasificación.

5.- Seguridad Física y Ambiental.

Los elementos críticos del Instituto deben estar protegidos en áreas seguras para su operación, a través del uso de barreras físicas para su acceso directo, reglamentos y sanciones. Los bienes informáticos se distribuyen tanto en centros de cómputo, como en oficinas. Las políticas para la seguridad física y ambiental aplican dentro de esos ámbitos.

Objetivo

Proteger la operación de los bienes informáticos del Instituto en un ambiente seguro, y sujetos a reglas para prevenir accesos físicos no autorizados, robos o mal uso de los recursos que afecten la correcta operación de estos bienes.

Responsable

De está política es responsable de su cumplimiento y supervisión el Comité de seguridad de la Información.

Alcance

Esta política contempla las normas y procedimientos utilizados para asegurar edificios, computadoras, información y medios de comunicación. La seguridad física debe proteger los dispositivos de la Dependencia tanto de una violación deliberada (ejemplo: intentos de individuos no autorizados de obtener el acceso a los recursos del sistema) como de interrupciones accidentales que llevan a reducir la disponibilidad del sistema (ejemplo: daño accidental a hardware como resultado imprevisto de otras actividades).

Seguridad Física y Ambiental.

Generales.

a. Definir los criterios para la delimitación de las áreas seguras pertenecientes al IIMAS a las que sólo tendrá acceso el personal autorizado. Las áreas en general serán definidas considerando los diferentes recursos con los que cuenta las áreas de tecnologías de información, de la siguiente forma:

- Área de Administración de servidores.
- Área de Oficinas.
- Área de Equipos de Red.

b. Los accesos a las áreas en las que se procese ó maneje información reservada y confidencial por el Instituto, deben estar estrictamente controlados y vigilados. Deben existir barreras y controles (perímetro seguro, gabinetes) para proteger los dispositivos de la Dependencia, que delimiten el acceso a personal no autorizado.

c. Los visitantes, empleados, prestadores de servicio o cualquier entidad externa que tenga acceso a las áreas seguras de la Dependencia, y cualquier área de trabajo en donde se manipule información y equipos sensibles, deberá identificarse y señalar el motivo de la visita, así como indicar el nombre de la persona responsable de su estancia en las instalaciones y el área a visitar, para posteriormente registrarse en una bitácora de acceso. El acceso podrá ser registrado a través del área de vigilancia, secretaría o personal perteneciente al área de trabajo.

Áreas y Perímetros de Seguridad.

a. Dentro de las áreas seguras se deben de establecer perímetros de seguridad que se encargarán de la protección del entorno de estas áreas.

b. Dentro del perímetro de seguridad establecido, todo el personal debe portar gafete de identificación, no obstruyendo o distorsionando la información del mismo con micas, cintas adheribles o cualquier otro elemento que no permita identificar claramente al portador del mismo.

c. Toda persona que no esté relacionada con la operación de la infraestructura de tecnologías de información del Instituto (de forma directa o indirecta), debe recibir un gafete que lo identifique como visitante.

d. A los empleados que por algún motivo hayan olvidado su gafete de identificación, se les proporcionará un gafete temporal, con el objeto de que todo el personal que tenga acceso a las áreas seguras de la Dependencia pueda ser identificado. Los empleados deberán proporcionar una identificación oficial y registrarse en una bitácora de acceso de empleados para obtener este gafete temporal con validez de un día.

e. En caso de pérdida o robo de un gafete de identificación o tarjeta de acceso, éste debe ser reportado en un lapso de 24 horas

f. Ninguna persona no autorizada podrá acceder a áreas de trabajo, utilizando el mismo acceso de una persona autorizada.

h. Con el objeto de no permitir que información reservada sea extraída de los dispositivos de la Dependencia, todo componente de cómputo o electrónico, únicamente podrá ser retirado de las instalaciones a través de una autorización firmada por el personal pertinente.

Seguridad de equipos.

a. Las áreas seguras deben contar con el equipo apropiado de seguridad física (extinguidores, aire acondicionado, energía regulada, otros) para evitar daños tanto a la información como a los equipos; se deberá instruir al personal sobre el uso y funcionamiento de los equipos.
b. Los equipos que efectúan las operaciones críticas de la organización deben contar con equipo UPS para suministros de energía en caso de falla en la corriente eléctrica.
c. Las estaciones de trabajo y los servidores críticos deben estar protegidos contra el robo de partes, de tal manera que no puedan ser abiertos. Las llaves para las estaciones de trabajo y servidores serán controladas por responsables plenamente identificados.
d. Los medios magnéticos que contienen respaldos de información crítica, deben ser protegidos contra robo.
e. Los servidores centrales y remotos deben estar ubicados en un ambiente seguro.
e. Se deben tomar medidas para limitar el acceso físico a los servidores con misión crítica dentro de la organización, siempre que sea posible el servidor se ubicará en un sitio cerrado y sólo personal autorizado tendrá acceso al mismo.
f. Todos los dispositivos removibles dentro de las áreas seguras, tales como discos o memorias flash deben ser revisados, para asegurar que no contengan información reservada o software con licencia antes de ser desechados.

Seguridad en los Escritorios.

a. Cualquier bien informático utilizado en el lugar del escritorio debe estar resguardo cuando el usuario eventualmente se encuentre fuera de su sitio de trabajo, con condiciones que eviten el acceso y disposición no autorizada.
b. Los equipos de soporte de la Dependencia como copiadoras y faxes deberán estar en sitios seguros, con el fin de minimizar el riesgo de que usuarios no autorizados tengan acceso a información.
c. Todos equipos portátiles y de escritorio deberá contar con dispositivos que eviten el movimiento físico no autorizado de los elementos que almacenan información en los mismos, tales como disco duro, memorias, CPU, etc.
d. Está prohibido que los empleados y visitantes fumen, coman o ingieran bebidas en las áreas donde se encuentran bienes informáticos ya que se corre el riesgo de un daño eléctrico así como de contaminación a los dispositivos de almacenamiento.
e. No se deben dejar documentos con información clasificada como confidencial o reservada en los escritorios, a la vista de todo el personal del Instituto.
f. Los documentos con información crítica deben estar asegurados en un gabinete con llave.

Mantenimiento de Equipos.

a. Los equipos de procesamiento de información deben contar con mantenimientos periódicos de acuerdo a los requerimientos del fabricante.
b. Tener registros sobre las averías a los equipos y los mantenimientos tanto correctivos como preventivos que se efectúen.

6.- Incidentes de Seguridad.

Contar con una respuesta a incidentes de seguridad, que permita mitigar cualquier tipo de incidente y reestablecer lo antes posible la operación normal de los servicios del Instituto.

Objetivo

Esta política contempla los reportes y respuestas ante un incidente de seguridad informática dentro de las instalaciones o activos informáticos del IIMAS y que serán registrados con el área de seguridad de la Dirección General de Servicios de Cómputo Académico (DGSCA) de la UNAM.

Responsable

Un grupo de respuesta Incidentes (conformado por el oficial de seguridad y los administradores de los sistemas de información) serán los responsables de conocer, registrar los incidentes de seguridad que se presenten en el Instituto.

Alcance

Esta política excluye a los clientes y otras entidades externas contemplando solamente los siguientes puntos:

- Mecanismos para reportar un incidente al área de seguridad de la DGSCA.
- Registro del incidente al área de seguridad y apoyarse de dicha área para la respuesta de incidentes
- Investigación de incidentes.
- Comunicación organizacional de incidentes.

Incidentes de Seguridad.

Generales.

a. El grupo de respuesta a incidentes de seguridad, tiene la responsabilidad de tomar y solucionar los incidentes de que afecten la operación del Instituto junto con área de seguridad de la DGSCA.

b. Todos los usuarios tienen la responsabilidad de reportar los incidentes de seguridad que sean de su conocimiento, al grupo de respuesta de incidentes de seguridad por medio de los procedimientos establecidos.

c. Los procedimientos para la notificación de incidentes deben estar fácilmente disponibles para todos los usuarios.

Reporte de respuesta a Incidentes de Seguridad.

a. Todos los incidentes de seguridad se deben reportar al área de seguridad de la DGSCA.

b. Los procedimientos para respuesta a incidentes de seguridad deben permitir dar un seguimiento continuo del estado del incidente.

c. La investigación de los incidentes de seguridad se debe de llevar a cabo con base en los procedimientos de respuesta a incidentes de seguridad del área de seguridad de la DGSCA.

d. Se debe llevar a cabo un informe detallado de los resultados de la investigación de los incidentes de seguridad, antes de que el incidente sea cerrado y se guardaran por un periodo no menor a tres años.

e. Los informes sobre los incidentes de seguridad, deben ser del conocimiento de los usuarios que levantaron el reporte, siempre y cuando la información que contenga el reporte no este clasificada como confidencial.

Respuesta a Incidentes de seguridad.
Los procedimientos para la respuesta a incidentes deben ser:
a. Elaborados junto con el área de seguridad de la DGSCA, tomando en consideración reducir al mínimo el daño potencial a los activos del Instituto.
b. Actualizados como resultado del análisis de un incidente con base en las lecciones aprendidas.
c. Llevarse a cabo sesiones de lecciones aprendidas con base a los incidentes de seguridad presentados.

7.- Monitoreo de Seguridad.

Los sistemas de información deben ser monitoreados para detectar violaciones con respecto a las Políticas de Seguridad, así como guardar los eventos que pueden ser utilizados como evidencia en incidentes de seguridad.

Objetivo
Esta política debe asegurar el monitoreo de los eventos de seguridad relacionados con ataques y mal comportamiento dentro de los sistemas y redes que procesen, almacenen o transmitan información del Instituto.

Responsable
Los responsables de ejecutar la política es el grupo de monitoreo (GM) del Instituto.

Alcance
El alcance de esta política contempla el monitoreo de eventos de seguridad, relacionados con ataques y conductas maliciosas en los sistemas y redes del Instituto. Dicha política no debe contemplarse el monitoreo relacionado con capacidad o rendimiento de sistemas o equipos.

Monitoreo de Seguridad.
Generales.
El monitoreo debe:
a. Proporcionar lo medios para identificar incidentes de seguridad, basado en herramientas de monitoreo (IDS, Firewalls) que proporcionen información sobre tráfico de la red y eventos relacionados con equipos de cómputo y dispositivos de red.
b. Analizar las alertas generadas por las herramientas de seguridad para detectar posibles eventos de seguridad.
c. Identificar e iniciar el proceso de respuesta a incidentes con base al tipo de incidente de seguridad registrado.
d. Llevar acabo escaneo de vulnerabilidades a los equipos del Instituto, en los periodos y a los equipos que se considere necesarios, notificando a los dueños de los activos.

Alcance del Monitoreo.

a. El monitoreo de la seguridad debe contemplar como mínimo los siguientes dispositivos:

- Firewalls.
- Detectores de Intrusos (basados en host y en red).
- Sniffer.
- Sistemas de Antivirus.
- Revisión periódica de bitácoras.
- Dispositivos de Seguridad, entre otros.

b. Debe establecer procedimientos para el monitoreo de utilización de los sistemas de información del Instituto, cubriendo al menos los siguientes puntos:

- Accesos autorizados, incluyendo detalles tales como:
  - Identidad del usuario.
  - Hora y día de eventos clave.
  - Tipo de eventos.
  - Archivos accedidos.
  - Utilidades, programas y herramientas utilizadas.
- Intentos de accesos no autorizados:
  - Intentos fallidos.
  - Alertas de sistemas de detección de intrusiones (IDS).
- Alertas del sistema o fallas detectadas:
  - Alertas o mensajes en consola.
  - Alarmas de administración de red.

c. El monitoreo de la seguridad debe llevarse a cabo en un periodo definido por el GM.

d. El monitoreo de seguridad debe bloquear ataques que afecten la disponibilidad, confidencialidad e integridad de la información de la Dependencia.

Administración de Incidentes.

a. Cuando una alerta de seguridad se activé el administrador debe determinar si se trata de un falso positivo o un ataque real, e iniciar el proceso de respuesta a incidentes de seguridad.

8.- Protección de Redes Internas.

Establecer controles en la red para asegurar la información y los servicios contra accesos no autorizados.

Objetivo

Definir los mecanismos para la protección de las redes internas del IIMAS.

Responsable

El grupo de administradores de los sistemas de información, serán los que lleven a cabo las actividades necesarias para cumplir la política.

Alcance

Indicar los controles para la protección de la red interna (LAN) del Instituto, bajo los siguientes puntos:

- Titulares de las redes.
- Administración de redes.
- Seguridad en redes.
- Administración del direccionamiento.

Seguridad en Redes Internas.

Generales.

a. Los usuarios de los servicios de red del IIMAS, son responsables del uso de la misma y debe ser sólo para efectos de la operación de la Dependencia.
b. Los administradores de la red deben ser lo dueños de los componentes de la red de la Dependencia.

Administración de la red.

a. El grupo responsable debe contar con un inventario de todos los componentes de red y todos los sistemas, aplicaciones y activos de información que estén asociados con la red interna del Instituto.
b. Los servidores, estaciones de trabajo, equipos portátiles, impresoras y todos los equipos que sea conectados a la red interna, deben estar configurados con base a los lineamientos establecidos por los administradores de la red.
c. Tomar las medidas necesarias cuando se lleve a cabo cualquier expansión de la red, para asegurar la protección de la misma y de la información almacenada procesada y transmitida vía red.
d. Realizar un monitoreo constante por parte de los administradores de la red, el cual se encargue de medir el desempeño de la misma.
e. El uso de redes inalámbricas debe ser bajo un estricto control de configuraciones de seguridad, por el riesgo que representan.
f. Llevar a cabo un estricto bloque de sitios Web que no son necesario para la operación del Instituto, ya que consumen recursos de la red.

Seguridad en redes.

a. Los componentes de la red, deben de contar con las configuraciones adecuadas de seguridad, actualización de parches y versiones indicadas por el proveedor.
b. Llevar a cabo mantenimiento periódico de los componentes de red con base a los requerimientos del fabricante.
c. Monitoreo constante, para detectar cualquier incidente de seguridad en los servicios de red de la Dependencia.
d. La información clasificada como confidencial que se transmita por medio de la red interna de la Dependencia debe ser de manera segura, contando con una tecnología de cifrado de información para proporcionar integridad y confidencialidad en la misma, con base en los lineamientos de la política de cifrado de información.
e. Considerar dentro de la seguridad de la red interna de la Dependencia, controles para el correo electrónico en donde se revisen los siguientes puntos:

- Mensajes que puedan provocar negación de servicio de la red.
- Uso de cuentas de correo de Internet por parte de los usuarios.
- Alternativas para envíos de información sensible.
- Información recibida de usuarios desconocidos.

9.- Respaldo y Borrado de Información

Los equipos de procesamiento de información del IIMAS, deben contar con los medios de almacenamiento que aseguren la información contenida en éstos. A fin de evitar pérdidas importantes de datos y las posibles consecuencias asociadas, se deben especificar claramente los tipos de datos que necesitan ser respaldados, los registros de operación críticos y eliminar registros no necesarios.

Objetivo

Establecer los lineamientos de respaldo, recuperación y borrado de información de los sistemas y componentes de red que soportan la operación del IIMAS.

Responsable

El grupo de administradores de los sistemas de información, son los encargados de llevar a cabo el proceso de respaldo de información sobre la infraestructura de tecnologías de seguridad.

Alcance

Indicar los requerimientos de los respaldos y recuperación de información, su calendarización y el resguardo seguro de los mismos, así como los lineamientos de desecho de información.

Respaldo de Información.

Generales.

a. Toda la información clasificada en los sistemas del IIMAS, deben respaldarse periódicamente con base en la criticidad de la información.
b. Los respaldos deben llevarse a cabo fuera de los horarios de operación.

Restauración e Integridad de Respaldos.

a. Los datos críticos que hayan sido respaldados no deben utilizarse directamente para restaurarlos, a menos que exista otra copia de respaldo de los mismos en un medio de almacenamiento diferente (cinta, disco, CD-ROM, etc.). Si se sospecha la existencia de virus u otro problema de software, la copia de respaldo adicional debe realizarse en una computadora diferente. Este lineamiento previene que la única copia de respaldo de datos críticos sea dañada inadvertidamente en el proceso de restauración.
b. Todos los registros de incidentes, alarmas, cambios, configuraciones, etc. deben guardarse por un periodo de al menos 3 años y estar disponibles para su revisión para cuando sea requerido

Almacenamiento de Información.

a. La información clasificada como reservada y confidencial, que se encuentre almacenada en medios magnéticos por periodos prolongados de tiempo, debe ponerse a prueba al menos anualmente para asegurarse que la información aún es recuperable (esto incluye respaldar el sistema o aplicación que la procesa), o copiarse a un medio nuevo.

b. Evitar que los medios magnéticos utilizados para el almacenamiento de información clasificada como reservada y confidencial, se vuelvan obsoletos en cuanto a la tecnología que utilizan. Se debe buscar utilizar tecnologías de punta que permitan reducir el espacio físico que ocupan estos medios.
c. Los procedimientos de respaldo de información en medios magnéticos (CD, cintas magnéticas, etc.) deben asegurar que la información sensible, crítica o valiosa almacenada por periodos prolongados de tiempo, no se pierda por deterioro.
d. Los respaldos de información reservada y confidencial, deben almacenarse en un sitio protegido contra el medio ambiente y con controles estrictos de acceso.

Destrucción de Información.

Generales.

La información del IIMAS debe ser destruida o almacenada en un sitio seguro cuando ya no sea necesaria ni en la operación ni por requerimientos legales. Se debe revisar periódicamente por parte de las áreas correspondientes la continuidad del valor y utilidad de la información.

Los procedimientos deberán considerar los siguientes puntos básicos:

- Toda la información reservada y confidencial, al no ser utilizada, debe ser eliminada o almacenada, de acuerdo a los criterios que establezcan las áreas competentes.
- Los medios que contengan información se podrán encontrar en las siguientes presentaciones:
  - Documentos impresos
  - Papel calca
  - Unidades de almacenamiento magnético removibles (discos duros, discos flexibles, cintas, memorias USB, etc.).
  - Medios de almacenamiento óptico

10.- Antivirus y Código Malicioso

Los equipos del IIMAS deben tener mecanismos de protección para evitar virus y código malicioso, que pueden ocasionar daños o mal funcionamiento en la operación.

Objetivo

Establecer la administración de código malicioso, virus, gusanos, caballos de Troya, etc. que involucren cualquier incidente en los sistemas de información y redes que procesen, almacenen o transmitan información del IIMAS.

Responsable

El oficial de seguridad, debe verificar que se lleve a cabo una adecuada administración del antivirus, coordinando actividades con los demás grupos

Alcance

Indicar los lineamientos para la protección de servidores, equipos portátiles y de escritorio, contra virus y código maliciosos, tomando en consideración los siguientes puntos:

- Responsabilidades de los empleados.
- Archivos y Software.
- Reporte y solución de Incidentes.
- Actualizaciones y mantenimiento.
- Avisos y alerta de virus y código malicioso.
- Correo electrónico.

Antivirus.

Generales.

a. Todos los equipos de escritorio, personales y servidores utilizados en la operación del Instituto, deben manejar un software antivirus que pueda detectar cambios en los archivos de configuración, archivos de sistema, aplicaciones y otros recursos.
b. Los usuarios son responsables de no desactivar o eliminar el software de antivirus en sus equipos y deben notificar cualquier sospecha de contaminación.
c. Los proveedores o personal externo que tengan equipos y que necesiten conectarse a la red del IIMAS, deben contar con un software de antivirus autorizado y actualizado.
d. Cualquier software que sea recibido de entidades externas al IIMAS debe ser revisado en alguna máquina que no comprometa a la red del Instituto. De esta manera, si un virus o software malicioso se presenta, el daño será restringido a la máquina involucrada.

Reporte de Incidentes.

a. Lo usuarios debe canalizar las incidencias de antivirus y código malicioso a su administrador.
b. Debido a que los virus se han vuelto muy complejos, los usuarios no deben pretender eliminarlos por sí solos. Si los usuarios perciben o sospechan que sus equipos están infectados inmediatamente tiene que detener el uso del equipo en cuestión y contactar al administrador de red.

Archivos y Software.

a. Los Archivos de nueva procedencia deben ser revisados por el software de antivirus incluyendo:
- Archivos de correo electrónico.
- Archivos provenientes de medios magnéticos (discos flexibles (floppy), CD y USB).
- Archivos de otras computadoras.
- Contenido Internet.

b. Los archivos de correo electrónico deben ser revisados por el software antivirus utilizado oficialmente, antes de ser accesible para el usuario.
c. El software y archivos provenientes de fuentes externas como Internet pueden contener virus (o similares, como caballo de Troya, gusanos u otros programas similares). Antes de que el software sea descomprimido o los archivos sean abiertos, los usuarios deben revisar la información con el software antivirus. En caso de detectarse algún virus, se debe notificar inmediatamente y no se realizará ningún trabajo sobre el dispositivo infectado hasta que el virus sea eliminado.
d. Antes de distribuir un software o archivo en medio electrónico a terceros, los administradores deben revisarlo con el antivirus para identificar y eliminar la presencia de alguno de ellos.
e. Queda prohibido instalar y ejecutar cualquier programa o proceso no autorizado para la operación del IIMAS
.

Escaneo y Capacidades del Antivirus.

a. El software de antivirus debe estar configurado para desempeñar las siguientes actividades:

- Archivos abiertos.
- Los escaneos de servidores de archivos, de correo y críticos deben hacerse por lo menos una vez al día en horarios fuera de operación, mientras que otros tipo de servidores y equipos de escritorio y portátiles por lo menos una vez por semana.
- Archivos de correo electrónico de entrada y de salida.
- Escaneo de contenidos Web.

b. El software de antivirus debe contar con las siguientes capacidades:

- Escaneo automático, manual o programable.
- Limpiar archivos infectados.
- Mantener en cuarentena los archivos que no pueden ser limpiados.
- Proveer la capacidad de actualizaciones automáticas y programables.
- Registrar los incidentes de virus y contar con la capacidad de análisis de registro.
- Detección de código malicioso.
- Alertas.
- Administración centralizada.

Mantenimiento.

a. Llevar acabo las actualizaciones del software de antivirus con base en los contratos con el fabricante.

b. El software antivirus deber ser actualizado mensualmente o antes, en caso de que exista una nueva versión.

Reportes y Alertas.

a. El software de antivirus debe proporcionar las siguientes tipos de alertas:

- Reportes por medio de correos electrónicos.
- Alertas por medio de mensajes escritos a dispositivos móviles, alarmas visuales o de sonido.

Reportes Históricos.

a. Los reportes mensuales de incidentes de antivirus y código maliciosos se deben guardar para su análisis y tomar futuras acciones sobre incidentes.

11.- Autenticación y Control de Accesos.

El acceso a los servicios de información del IIMAS debe ser controlado. Es necesario asegurar que los usuarios internos, externos o terceros, que tienen acceso a los servicios de información no comprometan la seguridad de los mismos.

Objetivo

Asegurar el uso de tecnologías de autenticación y control de acceso a sistemas de información, servicios o redes del Instituto.

Responsable

El grupo de administradores de la información junto con el oficial de la infraestructura de seguridad serán los responsable de supervisar la política

Alcance

Indicar los requerimientos que tiene el personal interno como externo, para la autenticación y controles de acceso identificando los siguientes elementos:

- Uso de autenticación
  - Requerimientos para la autenticación
  - Métodos de autenticación.
- Uso de control de accesos
  - Implementación y mantenimiento de controles de acceso.
  - Proceso de autorización para acceso a información.
  - Administración de privilegios.

Autenticación

Generales.

a. Formalizar las políticas de acceso a los sistemas de información, servicios y/o red del Instituto, que deberán aplicar tanto a los usuarios internos, externos.
b. Asignar identidades y privilegios de seguridad para establecer los lineamientos de administración para la autenticación de usuarios.
c. Usar canales de autenticación cifrados.
d. Diseñar y establecer esquemas de autenticación para acceso a los sistemas de información, servicios y/o red de la Dependencia de acuerdo al nivel de confidencialidad de la información que se requiera acceder.
e. La información clasificada como confidencial debe ser accedida a través de esquemas de autenticación basados en técnicas de cifrado, tokens de seguridad, o protocolos especiales, controlados y asignados.

Factores de autenticación.

a. Los usuarios deben ser autenticados con base algo que ellos conozcan, tengan o sea parte, como son:

- Algo que el usuario sabe – Contraseña o PIN
- Algo que el usuario tiene – Token o certificados.
- Alguna parte del usuario – Huella Digital (biométricos).

b. La autenticación debe de ser uno o dos factores de acuerdo al tipo de servicios al que se acceda.

- Cuando se trate de un factor de autenticación, el usuario debe proporcionar solo una prueba de identidad.
- Cuando se trate de dos factores de autenticación, el usuario debe proporcionar dos tipos de pruebas de identidad.

Requerimientos de autenticación.

a. El acceso a los recursos informáticos del IIMAS, deben ser bajo los siguientes lineamientos:

Red IIMAS

- Factor de Autenticación

Correo electrónico dentro de la red de la Dependencia

- Factor de Autenticación para la red

Aplicaciones dentro de la red

- Factor de Autenticación para la aplicación.

Internet

- Factor de Autenticación para dispositivo de comunicaciones o seguridad (Router o Firewall).

Controles de Acceso.

Generales.

a. Los controles de acceso a los sistemas de información, servicios y/o red del Instituto se deben llevar a cabo con base en los roles de los empleados.
b. La comunicación entre las estaciones de trabajo (PC´s o equipos móviles) a los sistemas de información, servicios y/o red de la Dependencia deben estar controlados a través de mecanismos distribuidos a lo largo de la ruta que se establezca entre ellos. Algunos de ellos se indican a continuación:

- Utilización de canales de comunicación cifrados.
- Conexión a los servicios de información a través del firewall.
- Prevención de "broadcasts" de información, excepto cuando sea necesario.
- Reforzar la utilización de controles para el acceso de usuarios externos.
- Implantación de equipos y funciones que controlen activamente la comunicación entre la fuente y el destino (firewalls, filtros y otros.)

Controles de Acceso a la información.

a. Contar con los controles para la manipulación de la información, con base en su nivel de clasificación, en donde se verifiquen los siguientes puntos:

- Acceso de solo lectura
- Acceso a escritura (incluyendo lectura)
- Acceso de ejecución (incluyendo lectura)

Implementación y Mantenimiento de Controles de Acceso.

a. La red LAN del IIMAS debe estar distribuida en segmentos o dominios, los cuales deben estar comunicados entre sí a través de elementos que filtren el tráfico entre ellos, bloqueando cualquier acceso no autorizado entre dominios y evitando que cualquier intromisión se divulgue a la totalidad de la red.
b. El grupo de administración debe llevar a cabo los cambios, eliminación y creación de los controles de acceso y privilegios a sistemas, servicios de red y aplicaciones para los usuarios, con previa autorización de los dueños de la información.

Auditoria de Eventos de Acceso.

a. El grupo administradores tiene que llevar un registro de los accesos exitosos y fallidos en los sistemas (periodo de 45 días).
b. Llevar a cabo una revisión de los privilegios de usuarios en los sistemas, por lo menos una vez al año que permitan verificar su integridad, esta auditoria se debe realizar por parte del grupo de administración en coordinación con los dueños de la información.

Manejo y control de Privilegios.

a. Toda la información residente en dispositivos o equipos del IIMAS, que sea sensible, crítica o vulnerable, forzosamente debe manejar un control de accesos para asegurar y minimizar el riesgo de que la información pueda ser modificada, borrada o manipulada. Si un sistema (equipos móviles, aplicación) maneja información restringida, el sistema forzosamente debe utilizar identificador de usuario y contraseñas.
b. Los privilegios de sistemas para los usuarios de la Dependencia, deben ser restringidos o limitados específicamente a lo que les compete saber (lo estrictamente necesario).
c. Los proveedores sólo deben tener acceso a los sistemas con base a las tareas a desarrollar. Estos privilegios deben ser otorgados por periodos de tiempo controlados.

12.- Usuarios y Contraseñas.

Los usuarios deben asumir la responsabilidad sobre el manejo de su cuenta y contraseña para prevenir el acceso no autorizado a la información dentro de los sistemas del IIMAS.

Objetivo

Proteger los activos de Información para que sean utilizados de forma autorizada, evitando acciones que puedan provocar su alteración, borrado o divulgación no autorizada, de forma accidental o intencionada. De tal forma que se pueda asegurar a través de un proceso válido las autorizaciones para añadir, modificar o eliminar privilegios de administración.

Responsable:

El grupo de administradores de los sistemas de información serán los responsables del cumplimento de la presente política.

Alcance

Esta política contempla los lineamientos necesarios para la administración de cualquier sistema de información o componentes de red y cómputo, que sean utilizados para acceder a cualquier tipo de información del Instituto. En este documento también se definirán los lineamientos para la administración de contraseñas asociadas a cuentas que se utilicen en cualquier sistema de información o componentes de red y cómputo de la Dependencia. Esta política se aplica a todo el personal que use equipo de cómputo y que actúen en nombre y para el Instituto.

Lineamientos sobre Cuentas de Usuarios

Generales

a. Los usuarios son responsables de las actividades realizadas a través de su cuenta de usuario.
b. El nombre de usuario (user-ID) debe de ser único por cada sistema de información y/o equipo de cómputo.
c. Las cuentas de usuario para recursos de cómputo deben ser utilizadas sólo por el usuario a quien fue asignada; por lo tanto, quedará estrictamente prohibido el uso compartido de cuentas de usuario.

Cuentas Nuevas

a. Todos los usuarios deben acceder a los recursos de cómputo de la Dependencia a través de una cuenta de usuario asignada en su equipo de cómputo por el grupo de administración.
b. Todos los empleados de la Dependencia deben solicitar por escrito a través del responsable del área al grupo de administración, el alta de cuentas de usuario sobre los recursos de procesamiento de información.
c. En el caso de que no sea posible solicitar por escrito la cuenta o no exista un responsable asignado, la aplicación que genere la cuenta debe dejar un registró de auditoria o notificación vía correo electrónico, para comprobar de que se realizó el alta de la cuenta.

d. Los usuarios que requieran de privilegios especiales para la administración de dispositivos de red, sistemas operativos, bases de datos y aplicaciones, deben contar con dos tipos de cuenta: cuenta de usuario final y cuenta privilegiada; esta última sólo deberá ser utilizadas para tareas de administración.

Controles para las Cuentas

a. Las cuentas de usuario deben de ser restringidas o limitadas específicamente a lo que les compete saber (lo estrictamente necesario). El área que haga uso de un recurso de procesamiento de información, debe especificar claramente y por escrito, la asignación de responsables o propietarios de la información. Tales declaraciones deben indicar para que puedan ser autorizadas a los individuos que se les ha concedido autoridad para originar, modificar o borrar información específica.

b. Notificar las bajas de personal de la Dependencia, al grupo de administración con una periodicidad de 30 días, para inhabilitar y/o dar de baja las cuentas de usuario correspondientes.

c. Las cuentas de administración por omisión con privilegios especiales en los sistemas operativos tales como root, administrador, entre otros; deben ser renombradas, y su utilización deberá restringirse para contingencias.

Eliminación de cuentas

a. Las cuentas de usuario deben ser borradas por el grupo de administración, cuando alguna de las siguientes situaciones se presente:

- Cambio de funciones y/o localidad del responsable de la cuenta de usuario.
- Terminación de la relación laboral con la Dependencia.
- Terminación de la función para la cual fue creada la cuenta del usuario.
- Inactividad de la cuenta de usuario en un periodo mayor a 30 días.

Bloqueo y Desbloqueo de cuentas

a. Las cuentas pueden ser bloqueadas de manera automática o manual por el grupo de administración, y basándose en lo siguientes criterios:

- Tres intentos fallidos de acceso (si el sistema lo permite).
- Cuenta inactiva por 30 días.
- La cuenta se encuentre involucrada en algún incidente de seguridad.

b. Las cuentas que hayan sido bloqueadas por las situaciones arriba mencionadas, tienen que ser desbloqueadas por el grupo de administración, con la aprobación por escrito del mando inmediato superior del usuario afectado.

Revisión de cuentas existentes

a. Llevar a cabo una revisión de todas las cuentas existentes (usuario final, grupo, servicio, usuarios privilegiados), por lo menos una vez al año, que permitan verificar su integridad, esta auditoria se debe realizar por parte del grupo de administración, en coordinación con los dueños de la información.

Lineamientos sobre Contraseñas

Contraseña Inicial

a. Todos los usuarios de recursos de procesamiento de información del Instituto deben ser identificados con un nombre de usuario (user-ID) y una contraseña secreta.

b. En caso de que un usuario tenga necesidad de privilegios especiales para un sistema o aplicación (por ejemplo un administrador), se debe crear un user-ID y contraseña diferente a la ya asignada.

c. La contraseña inicial debe de ser asignada por el grupo de administración a través de los canales de comunicación que se encuentren disponibles para tal efecto en la Dependencia.
d. La Contraseña inicial no debe de ser igual al nombre de usuario, este tiene la responsabilidad de cambiar la contraseña inicial inmediatamente después que le sea asignada, (el sistema debe estar configurado para llevar a cabo este cambio automáticamente si el usuario no lo realiza) y de acuerdo al formato mínimo de contraseñas definido en el siguiente punto.

Cambio de Contraseñas
a. El cambio de contraseñas debe solicitarse con el grupo de administración, con el objeto de que los usuarios y contraseñas sean asignados una vez que se comprueba la identidad del usuario y prevenir que sea revelado a una entidad no autorizada.
b. El sistema de contraseñas, debe de contar con una bitácora de registro en donde se guarden los cambios exitosos y no exitosos.
c. Respecto del cambio de contraseñas en sistemas operativos, dispositivos de red, aplicaciones y sistemas de información debe quedar registrada:

- La cuenta de usuario asociada al cambio de contraseña.
- La fecha y hora del cambio.
- El estatus (fallido o exitoso) del cambio de contraseña.
- Los registros deben quedar almacenados por 45 días

Controles para las contraseñas
a. Las contraseñas no deben ser reveladas ni compartidas, salvo en casos de emergencia, en los cuales se debe contar con la autorización por escrito del Jefe o mando superior. Una vez resuelta la situación de emergencia, se debe cambiar la contraseña de inmediato por parte del responsable directo de la misma.
b. En caso de sospecha de revelación de contraseñas a entidades no autorizadas, estas contraseñas deben ser cambiadas inmediatamente.
c. Las contraseñas no deben ser escritas u olvidadas en un lugar en donde puedan ser del conocimiento de personal no autorizado
d. Si el usuario está utilizando información sensible, clasificada como reservada y/o confidencial, no podrá abandonar su PC, terminal o estación de trabajo sin antes salirse de los sistemas o aplicaciones pertinentes.
e. Si no ha habido actividad en una aplicación durante un lapso de tiempo (3 minutos), el sistema deba suspender la sesión y se reestablezca cuando el usuario introduzca la contraseña adecuada (siempre y cuando la aplicación lo permita en caso de que no lo permita, se debe tener habilitado el protector de pantalla al pasar los 3 minutos antes mencionados).

Integridad de las Contraseñas
a. El grupo de administradores de la Dependencia, deben proporcionar los mecanismos necesarios para verificar la integridad del almacenamiento de contraseñas (por medio del sistema obligar a los usuarios a contar con el formato mínimo de contraseñas)

Estándar de contraseñas para usuarios finales
Las contraseñas para el acceso a los sistemas de información del Instituto deben cumplir con las siguientes características:

a. Una longitud mínima de 8 caracteres
b. Combinar caracteres numéricos (al menos uno) y caracteres especiales (al menos uno) de forma no consecutiva, por ejemplo: s3cr?tbr
c. **No deben** tener como base un nombre propio, por ejemplo: mexico2004
d. **No deben** estar relacionados con números telefónicos o fechas de nacimiento, por ejemplo: perico1970, fiscal56716593
e. Cambiar cada 45 días como mínimo.
f. Los recursos de procesamiento de información de la Dependencia no deben permitir la repetición de contraseñas por al menos 5 iteraciones.
g. Si no es posible seguir con el estándar por que la tecnología no lo permite, se debe reportar al responsable, para que tome medias alternas para la seguridad de esta Infraestructura.

Estándar de contraseñas para administradores

Las contraseñas para el acceso a los recursos de procesamiento de información del Instituto deben cumplir con las siguientes características:
a. Mantener una longitud mínima de 10 caracteres
b. Combinar caracteres numéricos (al menos uno), mayúsculas (al menos uno), y caracteres especiales (al menos uno) de forma no consecutiva, por ejemplo: #s3crtMrvh
c. **No deben** tener como base un nombre propio, por ejemplo: juanramirez2004
d. **No deben** estar relacionados con números telefónicos o fechas de nacimiento, por ejemplo: juliabernuy1980, dgscacoapa56716320
e. Cambiar cada 30 días como mínimo.
f. El grupo de administración no debe permitir la repetición de contraseñas por al menos 10 iteraciones.
g. Las contraseñas deben ser almacenadas en forma cifrada de tal forma que no puedan ser comprometidas con técnicas de análisis criptográfico.
h. Las contraseñas deben viajar cifradas una vez que han sido introducidas en el recurso de procesamiento de información.
i. El proceso de asignación de contraseñas dentro de una aplicación o sistema de información, deberá programarse para que el usuario cambie la contraseña la primera vez que intente acceder a éstos.
j. Las contraseñas nunca deben ser iguales a las cuentas de usuario.
k. Si no es posible seguir con el estándar por que la tecnología no lo permite, se debe reportar al responsable, para que tome medias alternas para la seguridad de esta Infraestructura.

Estándar de tipos de cuentas

Los tipos de cuentas de usuario para acceder a los recursos de procesamiento de información serán:
a. Cuentas de usuario final. Cuentas con privilegios normales, asignados de forma individual; con fines de uso y análisis de la información.
b. Cuentas grupales. Cuenta compuesta de cuentas de usuario final, asignadas de forma grupal; con fines de uso y análisis de la información.
c. Cuenta de servicio. Cuenta asociada al funcionamiento de una aplicación y/o servicio; con fines de administración de elementos de procesamiento de información, y restringida a las áreas de tecnología de información.
d. Cuentas privilegiadas. Cuenta asociada a la administración u operación de un elemento de procesamiento de información.

13.- Protección de equipos de cómputo.

Deben formalizarse las medidas necesarias para el control adecuado de la información sensible alojada en los equipos de cómputo, así como el cuidado de los mismos.

Objetivo

Establecer los requerimientos de seguridad para las computadoras incluidas en el alcance.

Responsable.

Los administradores de los sistemas de información, así como el oficial de seguridad serán los responsables de hacer cumplir está política a los empleados del Instituto.

Alcance

Esta política debe ser para todas las computadoras que procesen, transmitan o almacenen información del IIMAS. Los lineamientos de esta política deben incluir los siguientes puntos:

- Control de Accesos
- Administración del usuario
- Responsabilidades del usuario
- Seguridad de equipos y aplicaciones
- Software no autorizado y Antivirus
- Reportes de mal funcionamiento.

Equipos de Cómputo.

Generales.

a. Los equipos de cómputo deben ser asignados por el área responsable.
b. El área responsable debe llevar un inventario de los equipos de cómputo y de todos los sistemas, aplicaciones instaladas en los mismos.
c. Los usuarios deben reportar cualquier mal funcionamiento de los equipos de cómputo.
d. Todos los equipos del Instituto, deben contar con antivirus de acuerdo a los lineamientos de la política de antivirus y código malicioso.
e. Los usuarios que se les asigne equipos de cómputo deben ser responsables del buen uso de los mismos considerado los siguientes puntos:

- Cuidado físico de los equipos.
- Información contenida.
- Software instalado.
- Hardware.

Autorización de uso de equipos de cómputo.

a. No esta autorizado que los usuarios instalen o configuren el software y hardware, siempre y cuando tengan la autorización para ello.
b. No esta autorizado bajar software de Internet para instalarlo en los equipos de cómputo, a no ser que haya sido autorizado por el jefe inmediato.
c. Todo el software que sea necesario instalar en los equipos debe ser autorizado por los dueños de los activos informáticos.

Instalación y configuración inicial.

a. Es importante que los equipos de cómputo cuenten con controles de acceso para autenticar a los usuarios con base en la política de usuarios y contraseñas.
b. Contar con guías para la configuración de sistemas operativos.
c. Los equipos de cómputo deben contar con las siguientes instalaciones y configuraciones de seguridad:

- Protección para evitar el acceso no autorizado a discos duros y sistema operativo.
- Protección para evitar el remover discos duros de los equipos.
- Protección contra virus.

Áreas Seguras.

a. Las áreas que contengan equipo de cómputo crítico para la operación del Instituto, deben contar con accesos controlados que permitan la protección física de los equipos de amenazas. Tomar en consideración los lineamientos de la política de seguridad física y del ambiente.
b. Para remover equipos y componentes físicamente, es necesario la autorización del área responsable.

Información en los equipos de cómputo.

a. La información clasificada como confidencial de los equipos de cómputo debe ser cifrada.
b. Realizar respaldos de la información alojada en los equipos de cómputo.
c. Revisar periódicamente por parte del área responsable de la operación de las tecnologías de información, las aplicaciones y archivos alojados en los equipos de cómputo, y eliminar cualquier aplicación, programa o archivo sospechoso.

Servidores.

a. Los servidores del Instituto, deben estar protegidos bajo los siguientes lineamientos:

- Los servidores deben estar en áreas seguras.
- Los sitios en donde se encuentren los servidores deben estar en cumplimiento con la política de seguridad física y ambiental.
- En caso de desastre los servidores deben estar dentro de un plan de continuidad del negocio y de acuerdo a la política de administración de la continuidad
- Las consolas de los servidores solo deben ser utilizadas por usuarios autorizados y contar con controles de accesos.

Equipos Portátiles.

a. Los equipos portátiles del Instituto, deben estar protegidos bajo los lineamientos de la política de equipos portátiles.

Mantenimiento de equipos de cómputo.

a. Los equipos de procesamiento de información deben contar con mantenimientos periódicos de acuerdo a los requerimientos del fabricante.
b. Tener registros sobre las averías a los equipos y los mantenimientos tanto correctivos como preventivos que se efectúen.

14.- Equipos portátiles.

Formalizar las medidas necesarias para el control adecuado de la información sensible alojada en las unidades de cómputo portátiles, así como el cuidado de las mismas.

Objetivo

Cuidar la información sensible alojada en los equipos portátiles, así como el cuidado de los mismos.

Responsable

Los administradores de seguridad de la información, es responsable de la instalación, configuración y asignación inicial de los equipos portátiles.

Alcance

Esta política contempla a los equipos portátiles, en donde los lineamientos deben estar enfocados a los siguientes puntos:

- Propiedad y custodia.
- Autorizaciones de uso.
- Protección de información confidencial.
- Intercambio de equipos.

Equipos Portátiles.

Generales.

a. Llevar un inventario de los equipos portátiles y de todos los sistemas, aplicaciones instaladas en los mismos.

b. Los usuarios deben reportar cualquier mal funcionamiento que se presente en los equipos portátiles.

c. A los usuarios que se les asigne equipos portátiles deben ser responsables del uso de los mismos considerado los siguientes puntos:

- Cuidado físico de los equipos.
- Información contenida.
- Software instalado.
- Configuraciones.
- Hardware.

Autorización de uso de equipos portátiles.

a. Proporcionar el entrenamiento necesario a los usuarios para el uso de los mismos, obligando con esto a que los usuarios se responsabilicen de los equipos.

b. Todo el software que sea necesario instalar en los equipos debe ser autorizado por los dueños de los activos informáticos.

Instalación y configuración inicial.

a. Los equipos portátiles deben contar con las siguientes instalaciones y configuraciones de seguridad.

- Protección para evitar el acceso no autorizado a discos duros y sistema operativo.
- Protección para evitar el remover discos duros de los equipos portátiles.
- Protección contra virus.
- Protección contra transmisiones wireless.
- Contar con cifrado de datos.

Información en los equipos portátiles.
a. La información clasificada como confidencial de los equipos portátiles debe ser cifrada.
b. Los usuarios deben contar con el respaldo de toda información alojada en los equipos portátiles que se les asignó.
c. Revisar periódicamente los equipos portátiles para eliminar cualquier aplicación, programa o archivo sospechoso.

Cuidado físico de equipos portátiles.
a. Controlar estrictamente la entrada y salida de equipos portátiles de las instalaciones.
b. Considerar los accesorios necesarios para conservar la integridad física de los equipos portátiles; así como su robo o extravío, a través de candados.
c. Evitar medios de transporte públicos para la transportación de los equipos portátiles.
d. No esta permitido el préstamo o intercambio de equipos portátiles por parte de los usuarios.

Terminación y Reasignación de equipos portátiles.
a. Al reasignarse o al terminar el uso por parte de empleados de los equipos portátiles, el administrador, debe de reinstalar el sistema operativo y aplicaciones pertinentes.

15.- Desarrollo y Mantenimiento de Sistemas.

Deben formalizarse las medidas necesarias para el control adecuado del desarrollo y mantenimiento de sistemas de información.

Objetivo
Definir el ambiente de seguridad para el desarrollo de sistemas dentro del IIMAS.

Responsable
El responsable de seguridad en el desarrollo y mantenimiento de sistemas (RDS) debe verificar que los sistemas de información, cuenten con los lineamientos de seguridad adecuados, durante su desarrollo, adquisición e implantación.

Alcance
Esta política incluye los lineamientos de seguridad para el ambiente de desarrollo y mantenimiento de sistemas, llevado a cabo tanto por personal del IIMAS, como por terceros.

Desarrollo y Mantenimiento de Sistemas.
Generales.
a. Los desarrolladores de sistemas tanto del Instituto como terceros tienen la responsabilidad de llevar a cabo la planeación, desarrollo y mantenimiento de sistemas bajo los lineamientos de seguridad establecidos.
b. Al llevarse a cabo un nuevo proyecto para el desarrollo de sistemas, es necesario que los requisitos de seguridad sean tratados durante la etapa de análisis de dicho proyecto.
c. Los criterios de aceptación del sistema y los sistemas integrados serán establecidos para tratar requisitos de seguridad y para asegurarse que las pruebas apropiadas se llevaron acabo.

d. Todos los sistemas desarrollados por o para el Instituto, tendrán especificaciones documentadas que traten los requisitos de seguridad.
e. Llevar a cabo revisiones sobre los diseños de los sistemas en donde se tomen en consideración lo requerimientos de seguridad.
f. En el proceso de desarrollo de sistemas no esta permito el utilizar puertas traseras o configuraciones que comprometan la seguridad, para el acceso a dichos sistemas.

Controles para herramientas de desarrollo de software.
a. Las herramientas para el desarrollo de software son accesibles solo para los miembros autorizados de desarrollo de sistemas.
b. Las herramientas para el desarrollo de software deben ser eliminadas de cualquier equipo de cómputo que no sea utilizado para el desarrollo de sistemas.

Software de terceros.
a. Cuando se adquiera sistemas de terceros es necesario que se cumplan con los requisitos de seguridad establecidos, además de estar en acuerdo con la política de licenciamiento de software.
b. Al llevarse a cabo cambio de proveedores es necesario tomar en consideración los siguientes puntos:

- Riesgo de incorporar nuevos controles y procesos con los terceros.
- Proyección del tercero a futuro.
- Impacto de los costos de mantenimiento futuros, los cambios en procesos de mantenimiento y el control de versiones.

Ambientes de producción y desarrollo.
a. Los ambientes de desarrollo de sistemas deben estar separados de los de producción. Tomando en consideración la parte física y de redes, al no ser posible esta separación de ambientes por que los sistemas no lo permitan, se debe llevar acabo separaciones lógicas en cuanto a directorios y archivos.
b. Las herramientas de desarrollo no esta permitido instalarlas en los ambientes de producción, en caso de ser necesario, se tendrán los controles adecuados de seguridad aprobados por personal autorizado.
c. El uso de información operacional del Instituto, para el uso de pruebas en el desarrollo de sistemas no esta permitido, si fuera necesario debe estar autorizado por los dueños de los activos de información y con conocimiento del responsable de desarrollo de sistemas.
d. Todo el proceso de desarrollo de sistemas desde su planeación hasta la entrega debe estar documentada.

Controles de Versión.
a. Tener herramientas que permitan el control de versiones del sistema.
b. Debe existir una función de bibliotecario que llevara a cabo el registro y mantenimiento de las bibliotecas de software.
c. Las versiones de software a lanzar a los ambientes de producción deben ser revisadas cuidadosamente para no cometer errores.
d. Diseñar procedimientos y elaborar la documentación de controles para el cambio de versiones.

Mantenimiento de Sistemas.
a. Para mantener la disponibilidad e integridad de los sistemas, se deben desarrollar procedimientos para el mantenimiento de los mismos, los cuales especificara las actividades a realizar con base a la clasificación del sistema.
b. Las modificaciones a los sistemas serán probados antes de entrar ambientes de producción.
c. Todos los cambios a los sistemas se tiene que llevar a cabo bajo procedimientos establecidos y revisados por el responsable del desarrollo de sistemas.

Segregación de funciones.
a. En los diseños de los sistemas se tiene que asegurar que la segregación de funciones sea mantenida en ambientes controlados, tomando en consideración los siguientes puntos:

- La segregación de funciones no puede ser transferida.
- Solo el personal autorizado puede tener accesos a los sistemas desarrollados.
- Un solo individuo no puede tener el control total sobre los activos de información.
- El personal involucrado en el desarrollo de sistemas tiene que hacerse responsable de sus acciones.

b. Los desarrolladores de los sistemas tiene prohibido llevar a cabo las siguientes tareas, a menos que el equipo de desarrollo sea tan pequeño que no permita la segregación de dichas funciones:

- Llevar a cabo las pruebas de aceptación del sistema desarrollado.
- Realizar las tareas del bibliotecario de software.
- Migrar o modificar los sistemas existentes en ambientes no operacionales a ambientes de producción.

Controles de Acceso.
a. Los controles de acceso serán empleados en el desarrollo de sistemas y en los ambientes de pruebas y solo por personal autorizado o por los dueños de los activos de información.

Capacitación
a. Se debe de contar con capacitación y manuales sobre el desarrollo de los sistemas, que permitan asegurar la operación y mantenimiento apropiados.

16.- Licenciamiento de Software.

El Software que se encuentre instalado en los equipos del IIMAS, y que no sea desarrollado internamente, debe de contar con licenciamiento con base en los acuerdos de compra establecidos con los proveedores.

Objetivo
Definir los lineamientos para la adquisición de software dentro de la Dependencia.

Responsable
El oficial de seguridad de la Información será el encargado de supervisar la política de licenciamiento de software.

Alcance

Esta política contempla el licenciamiento de software no desarrollado en el Instituto, que sea utilizado para servidores, equipos de comunicación, seguridad, portátiles y de escritorio.

Licenciamiento.

Generales.

a. Todo el software instalado en los equipos mencionados en el alcance de esta política deben ser desarrollado internamente o estar de acuerdo a los compromisos de licencias, las leyes de protección de copia y los acuerdos de compra establecidos con proveedores.
b. El comité de seguridad junto con el área correspondiente de la Dependencia, debe supervisar el apego al uso de licencias y cumplimiento con los derechos de autor de toda aplicación y herramienta de software utilizada en los equipos, mencionados en el alcance de esta política.
c. Al encontrarse software no autorizado en los equipos, el Oficial de seguridad, cuenta con la capacidad de pedir por medio de los canales de comunicación pertinentes, eliminar el software de dichos equipos.

Acuerdos y Contratos con Proveedores.

a. Establecer en el contrato que se realice con un tercero que el Instituto tiene el derecho de tener el código fuente del software (programa, actualizaciones, mejoras, y remiendos) para saber si hay código malicioso o puertas traseras. (Siempre y cuando se cuente con ello)
b. Conservar los contratos o documentos que proporcionan la prueba de la propiedad del software por parte de la Dependencia, hasta que se deje de utilizar el software.

Contratos de Mantenimiento de Software.

a. El oficial de seguridad debe asegurar que los contratos son actuales y están renovados de una manera oportuna.

Inventario de Software.

a. Cada área del Instituto, además del oficial de seguridad deben contar con un inventario de software (aplicaciones comerciales e institucionales), en donde se incluyan cantidad de licencias, el tipo de software, nombre, un identificador único o número de serie y equipo donde se encuentra instalado.

17.- Seguridad para Terceros.

El acceso a la información y a los recursos del IIMAS por terceros, debe ser estrictamente controlado y deben existir lineamientos que lo aseguren.

Objetivo

Definir los requerimientos de seguridad que el Instituto debe solicitar y verificar con los terceros antes de que éstos cuenten con acceso a su información.

Responsable

El comité de seguridad de la información es el responsable de desempeñar y supervisar la política.

Alcance

Controlar los accesos de terceros a los recursos e información de la Dependencia. Como terceros se entienden todas aquellas entidades que no son parte del Instituto, como pueden ser otros organismos gubernamentales, clientes, proveedores, outsourcing.
Los puntos a tomar en cuenta en esta política son los siguientes:

- Revisión y aprobación de contratos.
- Accesos y autorizaciones.
- Requerimientos con terceros.

Seguridad con Terceros.

Generales.

a. Los terceros en todo momento deben atenerse a las políticas de seguridad de la Institución.
b. Los accesos de terceros a servicios de la Dependencia, (red, aplicaciones, equipos e información) deben estar autorizados por los responsables correspondientes (dueños de información y activos, administradores).
c. El acceso físico a los inmuebles del IIMAS, deben estar restringidos solo para personal autorizado, los terceros deben registrarse en una bitácora de entrada, y verificar vía telefónica el acceso al inmueble, con el responsable correspondiente de la Dependencia o área.
d. El trabajo de terceros en áreas seguras debe estar supervisado por el personal encargado de esa área, con base en la política de seguridad física y ambiental.
e. Al ser detectado un incidente de seguridad por parte de terceros, se debe de notificar a la contraparte correspondiente del Instituto.

Contratos con terceros.

a. El área que necesite la contratación de un tercero, debe considerar y reunir todos los requisitos contemplados en los lineamientos establecidos por el área competente de la Dependencia.
b. Los contratos con terceros deben considerar además de los requisitos contemplados en los lineamientos establecidos por el área competente, los siguientes puntos de seguridad de la información de acuerdo al tipo de contrato:

- Requerimientos de protección de activos (tecnológicos e información).
- Compromiso por parte de los terceros al ocurrir algún incidente con los activos (tecnológicos e información).
- Controles para asegurarse que al ocurrir algún incidente con los activos (tecnológicos e información), se solucionara el problema recobrando la operación normal del Instituto.
- Controles apropiados de disponibilidad e integridad.
- Restricciones para el copiado y acceso a la información clasificada.
- Descripción de los servicios que se lleven acabo.
- Responsabilidades de cada parte.
- Requerimientos para control de accesos y procedimientos de autorización para acceder a los activo de información del Instituto (tecnológicos e información).
- Responsabilidades con respecto al hardware e instalación y mantenimiento de software.
- Métodos de reportes y evaluación.
- Controles para asegurar la protección de virus y código maliciosos.
- Datos de los responsables por parte de la Institución para la atención del tercero.
- Datos del tercero.
- Calendario de actividades y horarios (si aplica).
- Penalizaciones por incumplimiento a las Políticas de Seguridad.

c. Se deben de contar con acuerdos de confidencialidad, que permitan asegurar la información de la Dependencia, durante la duración de la relación laboral y después de mínimo 5 años.

Investigación y entrenamiento para terceros.
a. Las áreas que se encarguen de llevar a cabo contratación de terceros, deben investigar los antecedentes del personal de la empresa contratada tomado en consideración los siguientes puntos:

- Verificar la identidad del candidato.
- Contar con Curriculum Vitae.
- Verificar referencias.
- Determinar si cumplen con los lineamientos que solicita la UNAM.

b. Los terceros deben de contar con el entrenamiento adecuado sobre las políticas y procedimientos de seguridad de la Dependencia.

18.- Administración de la Continuidad.

Contar con planes para recuperar las actividades normales del IIMAS de acuerdo a prioridades definidas. Los planes de continuidad deben estar disponibles para proteger los procesos críticos asociados a la Dependencia después de que las actividades han sido suspendidas a causa de fallas, desastres naturales, accidentes y pérdida del servicio.

Objetivo

Contar con los lineamientos para recuperar las actividades críticas de operación, en caso de interrupciones parciales o totales por causa de fallas mayores, desastres naturales, accidentes y eventos impredecibles que provoquen la pérdida de servicios.

Responsable

El Comité de seguridad de la Información debe definir una estrategia de recuperación para las diferentes plataformas con las que cuenta el IIMAS, así como desarrollar, documentar, probar y mantener el Plan de Continuidad que conduzcan a la restauración de los sistemas críticos de información con el objeto de dar continuidad en el servicio.

Alcance

Esta política contempla los lineamientos que se dictaran en cuestión de:

- Responsabilidades de Administración de continuidad del negocio.
- Plan de continuidad del negocio
- Mantenimiento del plan de continuidad del negocio

Administración de la Continuidad.

Generales.
a. El proceso de administración en la continuidad de la operación deberá incluir los siguientes puntos:

- Concientización del personal de los riesgos potenciales que implican en la operación la interrupción de los servicios por eventos impredecibles, y la necesidad de tomar planes de recuperación para esos casos.

- Identificar los bienes y servicios más importantes a proteger en caso de una contingencia, así como los procesos específicos de recuperación indicados en un documento de fácil acceso a toda la organización.
- Considerar la contratación de seguros para la protección de los equipos de cómputo y divulgar los alcances de éstos, y los procedimientos para hacerlos efectivos.
- Planear pruebas (simulacros) y actualización de los planes de recuperación de la operación.
- Definir y documentar de responsabilidades en funciones de recuperación de la operación, y su integración en el organigrama de la organización.

Disponibilidad de los bienes informáticos.

a. Los sistemas críticos deben tener una alta disponibilidad, donde los usuarios deben tener la capacidad de acceder a los equipos durante el mayor tiempo, con base a los niveles de servicio.

b. Establecer los procedimientos necesarios para proporcionar y mantener sistemas de detección/supresión de incendio, aire acondicionado, alimentación y otros sistemas de protección del ambiente de cómputo necesarios para asegurar la continuidad del servicio para sistemas de cómputo críticos.

c. Los equipos críticos deben ser equipadas con sistemas UPS, supresores de picos de voltaje o reguladores de voltaje que hayan sido aprobados por el Comité.

Preparación de los planes de contingencia.

a. Se deben establecer y usar:

- Un marco de trabajo para segmentar los recursos de información por prioridad de recuperación. Esto permitirá que los recursos de información más críticos se recuperen primero.
- Preparar una evaluación del grado de criticidad de todas las aplicaciones en producción.
- Preparar, actualizar y probar periódicamente planes de respuesta a emergencias, dichos planes deben facilitar la operación continua de sistemas críticos en el evento de una interrupción o degradación del servicio.
- Documentar y mantener un proceso estándar para el desarrollo y mantenimiento de los planes de contingencia que cubran la totalidad de las tecnologías de información.

Prueba de los planes de contingencia.

a. Preparar, actualizar y probar periódicamente un plan de recuperación por desastre, que permita que los sistemas estar disponibles en caso o en eventos de desastres naturales como un incendio, inundación o temblor. Este plan de recuperación debe especificar cómo se proporcionarán instalaciones alternas como oficinas, muebles, teléfonos y copiadoras para que los empleados puedan continuar con las operaciones en caso de una emergencia o desastre.

Responsabilidad de los empleados.

a. Al usar sitios o equipos alternos para planes de contingencias, se debe de considerar el mismo nivel de seguridad que el utilizado para la infraestructura de producción local, aun cuando los niveles de servicio estén degradados.
b. Los miembros del Comité de seguridad de la información, así como de los demás grupos de seguridad que salgan de la ciudad deben proporcionar a su jefe directo, los números de teléfono donde pueden ser localizados. Esta información debe proporcionarse antes de emprender el viaje y se requiere independientemente de la razón del viaje.

SANCIONES

El incumplimiento accidental o deliberado de las políticas descritas en este documento, será considerado una falta administrativa, dependiendo de la gravedad de la falta, la cuál será determinada por las áreas competentes, y/o por el jefe inmediato superior de la persona que cometió la falta; o el responsable del proveedor o tercero que incurriere en falta.

Las sanciones aplicables para violaciones en el contenido serán determinadas por el Comité de seguridad de la información y podrán ser:

1. Para la primera falta menor se hará una amonestación privada (individual)
2. Para la segunda falta menor consecutiva se hará una amonestación al empleado con una notificación al jefe inmediato superior;
3. Para faltas mayores (dependiendo de la gravedad de ésta):
    - Suspensión del empleo, cargo o comisión por un período no menor de tres días ni mayor a un año;
    - Destitución del puesto;
    - Sanción económica.

Apéndice C

Configuración, reglas y comandos de un Firewall transparente

- A continuación se describe las instrucciones necesarias para configurar un firewall transparente:

    a) Editar el archivo de configuración /etc/rc.local

        - Deshabilitar portmap=YES a portmap=NO
        - Deshabilitar check_quotas=YES a check_quotas=NO
        - Deshabilitar ntpd=YES a ntpd=NO
        - Habilitar pf=NO a pf=YES

    b) Editar el archivo sysctl.conf
        - Habilitar:

        net.inet.ip.forwarding=1 # 1=Permit forwarding (routing) of packets

    c) Editar los archivos hostname.xl0 y hostname.xl1

        - Agregar en cada uno de los archivos la palabra “up”

    d) Generar el archivo bridgename.bridge0

        - Con la siguiente sintaxis: “add xl0 add xl1 up”

- Reglas para un firewall transparente

    El archivo de configuración para las reglas en el archivo /etc/pf.conf son:

    - Reglas de tráfico completo

    pass in on xl0 from any to any keep state
    pass out on xl0 from any to any keep state

    pass in on xl1 from any to any keep state
    pass out on xl1 from any to any keep state

    - Reglas para bloquear toda la entrada y permitir la salida.

    block in on xl0 all
    pass out on xl1 from any to any keep state
    pass out on xl0 from any to any keep state

- Comandos para ejecutar reglas en un firewall transparente

pfctl –e *Activar el Packet filter*
pfctl –d *Desactivar el Packet filter*
pfctl -f /etc/pf.conf *Carga el archivo pf.conf*
pfctl -nf /etc/pf.conf *Analiza el archivo, sin cargalo.*
pfctl -Nf /etc/pf.conf *Carga sólo las reglas de NAT del archivo.*
pfctl -Rf /etc/pf.conf *Carga sólo las reglas de filtrado del archivo.*

Apéndice D

Configuración, reglas y comandos de un Firewall NAT

- A continuación se describen las instrucciones necesarias para configurar un firewall NAT:

    a. Editar el archivo de configuración /etc/rc.local

        i. Deshabilitar portmap=YES a portmap=NO
        ii. Deshabilitar check_quotas=YES a check_quotas=NO
        iii. Deshabilitar ntpd=YES a ntpd=NO
        iv. Habilitar pf=NO a pf=YES

    b. Editar el archivo sysctl.conf
        - Habilitar:

        net.inet.ip.forwarding=1 # 1=Permit forwarding (routing) of packets

        Editar el archivo hostname.xl0

        Para la Red del IIMAS la cual tendrá conectividad a la red la UNAM
        - Agregar en el archivo hostname.xl0
            - inet 132.248.51.4 255.255.255.0 NONE

Para la configuración de cada una de las redes internas del IIMAS se deben editar los siguientes archivos de configuración:

Editar el archivo hostname.xl1
Red de Servicios
- Agregar en el archivo hostname.xl1
    - inet 10.10.10.1 255.255.255.0 NONE
    - inet alias 10.10.10.2

Editar el archivo hostname.xl2
Red de Aulas
- Agregar en el archivo hostname.xl2
    - inet 10.10.10.2 255.255.255.0 NONE

Editar el archivo hostname.xl3
Red de Oficinas
- Agregar en el archivo hostname.xl3
    - inet 10.10.10.3 255.255.255.0 NONE

Editar el archivo hostname.xl4
Red de Investigadores
- Agregar en el archivo hostname.xl4
    - inet 10.10.10.4 255.255.255.0 NONE

Editar el archivo hostname.xl5
Red de Servidores DMZ
- Agregar en el archivo hostname.xl5
    - inet 10.10.10.5 255.255.255.0 NONE

- Reglas para Firewall NAT

```
# MACROS DE REDES DEL IIMAS
ext_if = "xl0"
int_if_servicios = "xl1"
int_if_aulas = "xl2"
int_if_oficinas = "xl3"
int_if_investigadores = "xl4"
int_if_dmz = "xl5"
int_if_todas=”{xl1, xl2, xl3, xl4, xl5}”
icmp_types = "echoreq"

priv_nets = "{ 127.0.0.0/8, 10.10.1.0/24, 10.10.2.0/24, 10.10.3.0/24, 10.10.4.0/24, 10.10.5.0/24 }"

table <intrusos> persist file "/etc/tablas/intrusos"

web_ext="132.248.51.2"
web_int="10.10.1.2"
correo_int="10.10.1.2"

# OPCIONES DE SEGURIDAD ANTISPOOF
set block-policy return
set loginterface $ext_if

# ENSAMBLADO DE PAQUETES
scrub in all

# NAT Y REDIRECCIONAMIENTO
nat on $ext_if from {$int_if_todas}  to any -> ($ext_if)
rdr on xl0 proto tcp from any to $web_ext port 80 -> $web_int port 80

# REGLAS DE FILTRADO
block in log all
block out log all
pass quick on log all

# BLOQUE A DIRECCIONES DE INTRUSOS POR MEDIO DE TABLAS
block drop in log quick on $ext_if from <intrusos> to any

block drop in  quick on $ext_if from $intrusos to any
block drop in  quick on $ext_if from $priv_nets to any
block drop out quick on $ext_if from any to $priv_nets

# ENTRADA A SERVICIO DE IIMAS
pass in log on $ext_if proto tcp to $web_int port 80 keep state
```

```
# SALIDA SERVICIO DE CORREO
pass in log  on $int_if inet proto { tcp, udp } from $correo_int to any port { 25, 53 }
keep state
pass out log on $int_if inet proto { tcp, udp } from any to $correo_int  port { 25, 53 }
keep state

# ACCESO COMPLETO PARA ACADEMICOS Y/O INVESTIGADORES
pass in log  on $int_if from $admin to any keep state
pass out log on $int_if from any to $admin keep state

# SALIDA A LA INTERFACE DEL IIMAS
pass out log on $ext_if proto tcp all modulate state flags S/SA
pass out log on $ext_if proto { udp, icmp } all keep state

# OPCION PARA EJECUTAR TRACEROUTE
pass in inet proto icmp all icmp-type $icmp_types keep state
```

- Comandos para ejecutar reglas en Firewall NAT

pfctl –e *Activar el Packet filter*
pfctl –d *Desactivar el Packet filter*
pfctl -f /etc/pf.conf *Carga el archivo pf.conf*
pfctl -nf /etc/pf.conf *Analiza el archivo, pero no lo carga*
pfctl -Nf /etc/pf.conf *Carga sólo las reglas de NAT del archivo.*
pfctl -Rf /etc/pf.conf *Carga sólo las reglas de filtrado del archivo.*

Bibliografía

1. Alexander, Alberto**, Mejora continua y Acción Correctiva,** Prentice Hall 2002, México.
2. Brandon Palmer y Jose Nazario, **Secure Architectures with OpenBSD**, Editorial Addison- 28 Wesley, 2004.
3. Peltier, Thomas R., **Information Security Risk Analysis**, Aurebach Publications, 2001.
4. Peltier, Thomas R, Information **Security, Policies, Procedures, and Standards**, Aurebach Publications, 2001.
5. D. Russell y G.T. Gangemi, **Computer Security Basics**, O'Reilly & Associates.
6. Artymiak, Jacek, **Building Firewalls with OpenBSD and PF**, Second Edition, Editorial Lublin, 2003.

- **Enlaces/URLS**

- Proyecto OpenBSD: http://www.openbsd.org
- OpenBSD Journal: http://undeadly.org
- Proyecto FreeBSD: http://www.freebsd.org
- Proyecto NetBSD: http://www.netbsd.org
- Onlamp BSD: http://www.onlamp.com/bsd
- Pf, OpenBSD packet filter: http://www.benzedrine.cx/pf.html
- OpenBSD FAQ, http://www.openbsd.org/faq/pf/index.html
- TCP rfc: http://www.faqs.org/rfcs/rfc793.html
- http://www.faqs.org/rfcs/rfc3168.html
- Google: http://www.google.com
- ISACA: http://www.isaca.org.mx
- CERT: http://www.cert.org
- IIMAS http://www.iimas.unam.mx
- ISO 17799: Made Easy: http://17799.macassistant.com/
- BSI América: http://www.bsiamericas.com/Mexico/index.xalter
- ISO 20000: http://20000.fwtk.org/
- ISO 27000: http://www.iso27000.es/iso27000.html
- RFC 2196 : http://www.faqs.org/rfcs/rfc2196.html
- NIST: http://csrc.nist.gov/publications/nistpubs/
- ISO: http://www.iso.com/
- ITIL: http://www.itil-officialsite.com/home/home.asp

- **Guías y estándares**

1.BS ISO/IEC 17799:2005 (BS 7799-1:2005) **Information technology. Security techniques. Code of practice for information security management**.
2.Draft BS 7799-2:2005 (ISO/IEC FDIS 27001:2005) **Information technology. Security techniques. Information security management systems. Requirements**
3.Information technology – **Security techniques – Information security management systems – Requirement.** BS ISO/ IEC 27001:2005 BS 7799-2:2005.
4.COBIT 4.0, Obejtivos de Control 4a. Edición. IT Governance Institute.