PROYECTO

METODOLOGIA
PARA LA ELABORACION DEL PLAN DE SEGURIDAD INFORMATICA

Propósitos de este documento

El objetivo del presente documento es establecer una metodología para la elaboración del Plan de Seguridad Informática de una entidad, mediante la descripción de los controles de seguridad que deben ser implementados, de forma que permita la interpretación clara y precisa de las políticas, medidas y procedimientos que se definan en la misma, con el objetivo de alcanzar niveles aceptables de seguridad.

En el mismo se describen los elementos fundamentales que deben ser incluidos en el Plan de Seguridad Informática de una entidad (contenido) y el modo en que pueden ser estructurados (formato). Como metodología al fin, tiene un carácter general, o sea, no está orientado a un tipo determinado de entidad o sistema informático, debiendo ser considerado como una guía de trabajo y no como un cuestionario que haya que seguir al pie de la letra, por lo que el equipo designado para su elaboración desarrollará los aspectos que considere necesarios a partir del Sistema de Seguridad Informática que previamente se haya diseñado para la entidad en cuestión, de modo que aquellos aspectos que no correspondan a las necesidades de protección identificadas podrán ser excluidos y por supuesto, se adicionará cualquier elemento que se considere importante para los requerimientos de seguridad, con independencia de que no esté contemplado en este documento.

Auditorio

Esta metodología está dirigida en primer lugar a aquellas personas que están responsabilizadas con el diseño e implementación de un sistema de Seguridad Informática, entre las cuales pueden incluirse distintas categorías de personal, pero en ningún caso deben faltar los dirigentes y funcionarios relacionados con la información que se procesa, por la responsabilidad que tienen para con la misma; los especialistas en informática, debido a los conocimientos técnicos que poseen y los profesionales de la seguridad y protección, por su experiencia y conocimientos generales de esta especialidad.

Documentos relacionados

Este documento es un complemento de la Metodología para el Diseño de un Sistema de Seguridad Informática elaborado por la Dirección de Protección del Ministerio del Interior, que profundiza en los aspectos que preceden a la confección del Plan de Seguridad Informática.

Aproximación básica

Un **Sistema de Seguridad Informática** es un conjunto de medios administrativos, medios técnicos y personal que de manera interrelacionada garantizan niveles de seguridad informática en correspondencia con la importancia de los bienes a proteger y los riesgos estimados.

El **Plan de Seguridad Informática** es la expresión gráfica del Sistema de Seguridad Informática diseñado y constituye el documento básico que establece los principios organizativos y funcionales de la actividad de Seguridad Informática en una Entidad y recoge claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo.

Durante el proceso de diseño de un Sistema de Seguridad Informática se distinguen tres etapas:

1) Determinar las necesidades de protección del sistema informático objeto de análisis, que incluye:
   - Caracterización del sistema informático.
   - Identificación de las amenazas y estimación de los riesgos.
   - Evaluación del estado actual de la seguridad.

2) Definir e implementar el sistema de seguridad que garantice minimizar los riesgos identificados en la primera etapa.
   - Definir las políticas de seguridad.
   - Definir las medidas y procedimientos a implementar.

3) Evaluar el sistema de seguridad diseñado.

El contenido de cada una de estas etapas se describe en la "Metodología para el diseño de un sistema de Seguridad Informática" elaborada por el Ministerio del Interior.

Una vez cumplidas estas etapas se elabora el Plan de Seguridad Informática.

Para la elaboración del Plan de Seguridad Informática se tendrán en cuenta las consideraciones siguientes:

- Serán confeccionados tantos ejemplares como se determine en cada lugar, numerando las paginas consecutivamente.
- Se determinará su clasificación, parcial o total, de acuerdo a la información que contenga, en correspondencia con las categorías que expresa el Decreto-Ley No. 199 de 1999 sobre la Seguridad y Protección de la Información Oficial.
- Contendrá las tablas y gráficos que se consideren necesarios y contribuyan a su mejor interpretación.
- Tendrán acceso a este documento, o a parte de él, las personas que en cada área requieran de su conocimiento.
- Se mantendrá permanentemente actualizado sobre la base de los cambios que se produzcan en las condiciones que se consideraron durante su elaboración.

Al elaborar el Plan se deberá evitar repetir aspectos que ya han sido señalados anteriormente, en todo caso se puede hacer referencia a ellos.

Tabla de contenido

	Presentación del documento.	6
1.	Alcance.	7
2.	Caracterización del Sistema Informático.	7
3.	Resultados del Análisis de Riesgos.	8
4.	Políticas de Seguridad Informática.	9
5.	Sistema de Seguridad Informática.	10
5.1.	Medios humanos.	10
5.2.	Medios técnicos.	10
5.3.	Medidas y Procedimientos de Seguridad Informática.	11
5.3.1.	De protección física.	13
5.3.1.1.	A las áreas con tecnologías instaladas.	13
5.3.1.2.	A las tecnologías de información.	13
5.3.1.3.	A los soportes de información.	14
5.3.2.	Técnicas o lógicas.	14
5.3.2.1.	Identificación de usuarios.	14
5.3.2.2.	Autenticación de usuarios.	15
5.3.2.3.	Control de acceso a los activos y recursos.	15
5.3.2.4.	Integridad de los ficheros y datos.	16
5.3.2.5.	Auditoria y alarmas.	16
5.3.3.	De seguridad de operaciones.	16
5.3.4.	De recuperación ante contingencias.	17
6.	Anexos.	18
6.1.	Programa de Seguridad Informática	18
6.2.	Listado nominal de usuarios con acceso a redes de alcance global.	18
6.3.	Registros.	18

Presentación del documento.

La página inicial (portada) contendrá el siguiente título: "**PLAN DE SEGURIDAD INFORMATICA**" seguido de la denominación de la entidad.

En la segunda página se consignarán los datos referidos a la elaboración, revisión y aprobación del Plan de Seguridad Informática, de acuerdo al siguiente formato:

REV. ___	ELABORADO	REVISADO	APROBADO
NOMBRE			
CARGO			
FIRMA			
FECHA			

En la columna "elaborado" se consignan los datos del jefe del equipo que confeccionó el Plan de Seguridad Informática, en la columna "revisado" los de la persona designada para su revisión antes de presentarlo a aprobación y en la columna "aprobado" se reflejan los datos del jefe de la entidad en la que el Plan será implementado.

A partir de la página No. 2, cada una de las páginas que conforman el Plan tendrán el encabezamiento siguiente:

Clasificación Del Documento	**Nombre de la Entidad**	**Pag. ___ de ___**

En la casilla "clasificación del documento" se pondrá la que le fue otorgada de acuerdo a lo establecido para la seguridad y protección de la información oficial.

1. Alcance.

El Alcance expresará el radio de acción que abarca el Plan, de acuerdo al Sistema Informático objeto de protección, para el cual fueron determinados los riesgos y diseñado el Sistema de Seguridad. La importancia de dejar definido claramente el alcance del Plan (y de ahí su inclusión al comienzo del mismo) estriba en que permite tener a priori una idea precisa de la extensión y los límites en que el mismo tiene vigencia.

2. Caracterización del Sistema Informático.

Se describirá el resultado de la caracterización realizada al sistema informático de la entidad, con el objetivo de determinar **qué se trata de proteger**, especificando sus principales componentes y considerando entre otros:

- Bienes informáticos, su organización e importancia.
- Redes instaladas, estructura, tipo y plataformas que utilizan.
- Aplicaciones en explotación.
- Servicios informáticos y de comunicaciones disponibles, especificando si son en calidad de clientes o servidores.
- Características del procesamiento, transmisión y conservación de la información, teniendo en cuenta el flujo interno y externo y los niveles de clasificación de la misma.
- Otros datos de interés.

Al describirse el sistema informático se hará uso, en los casos que lo requieran, de diferentes tipos de esquemas, tablas, gráficos, etc; a fin de facilitar una mejor comprensión. Estos medios auxiliares pueden ser insertados, lo mismo dentro de esta propia sección que al final, como anexos a los cuales debe haber una obligada referencia.

3. Resultados del Análisis de Riesgos.

A partir de que el Plan de Seguridad Informática es la expresión gráfica del Sistema de Seguridad Informática diseñado y de que la esencia de ese diseño es la realización de un análisis de riesgos, no se concibe seguir adelante en la elaboración del Plan sin dejar claramente precisados cuales fueron los resultados obtenidos en el análisis de riesgos realizado, por lo que en este acápite deberán relacionarse las principales conclusiones obtenidas en ese proceso, entre las cuales no pueden faltar:

a) Cuales son los activos y recursos más importantes para la gestión de la entidad y por lo tanto requieren de una atención especial desde el punto de vista de la protección, especificando aquellos considerados de importancia crítica por el peso que tienen dentro del sistema.
b) Que amenazas actúan sobre los activos y recursos a proteger y entre ellas cuales tienen una mayor probabilidad de materializarse (riesgo) y su posible impacto sobre la entidad.
c) Cuales son los activos, recursos y áreas con un mayor peso de riesgo y que amenazas lo motivan.

En la medida en que las conclusiones del análisis de riesgos sean más precisas se logrará una visión más acertada de hacia donde pueden ser dirigidos los mayores esfuerzos de seguridad y por supuesto los recursos disponibles para ello, lográndose que la misma sea más rentable.

4. Políticas de Seguridad Informática

En esta sección se definen los aspectos que conforman la estrategia a seguir por la Entidad sobre la base de sus características propias y en conformidad con la política vigente en el país en esta materia y el sistema de seguridad diseñado, mediante el establecimiento de las normas generales que debe cumplir el personal que participa en el sistema informático, las cuales se derivan de los resultados obtenidos en el análisis de riesgos y de las definidas por las instancias superiores en las leyes, reglamentos, resoluciones y otros documentos rectores. Al definir las políticas de Seguridad Informática se considerarán, entre otros, los aspectos siguientes:

a) El empleo conveniente y seguro de las tecnologías instaladas y cada uno de los servicios que éstas pueden ofrecer.
b) El tratamiento que requiere la información oficial que se procese, intercambie, reproduzca o conserve a través de las tecnologías de información, según su categoría.
c) La definición de los privilegios y derechos de acceso a los activos de información para garantizar su protección contra modificaciones no autorizadas, pérdidas o revelación.
d) Los principios que garanticen un efectivo control de acceso a las tecnologías, incluyendo el acceso remoto, y a los locales donde éstas se encuentren.
e) La salva y conservación de la información.
f) La conexión a redes externas a la Entidad, en especial las de alcance global y la utilización de sus servicios.
g) Los requerimientos de Seguridad Informática a tener en cuenta durante el diseño o la adquisición de nuevas tecnologías o proyectos de software.
h) La definición de los principios relacionados con el monitoreo del correo electrónico, la gestión de las trazas de auditoría y el acceso a los ficheros de usuario.
i) El mantenimiento, reparación y traslado de las tecnologías y el personal técnico que requiere acceso a las mismas por esos motivos.
j) Las regulaciones con relación a la certificación, instalación y empleo de los Sistemas de Protección Electromagnética.
k) Las regulaciones relacionadas con la certificación, instalación y empleo de los Sistemas Criptográficos, en los casos que se requiera.
l) Los principios generales para el tratamiento de incidentes y violaciones de seguridad.

5. SISTEMA DE SEGURIDAD INFORMATICA

En esta sección se describe **cómo** se implementan, en las áreas a proteger, las políticas generales que han sido definidas para toda la entidad, en correspondencia con las necesidades de protección en cada una de ellas, atendiendo a sus formas de ejecución, periodicidad, personal participante y medios**.**

Se sustenta sobre la base de los recursos disponibles y, en dependencia de los niveles de seguridad alcanzados se elaborará un Programa de Seguridad Informática, que incluya las acciones a realizar por etapas para lograr niveles superiores.

Se describirán por separado los controles de seguridad implementados en correspondencia con su naturaleza, de acuerdo al empleo que se haga de los medios humanos, de los medios técnicos o de las medidas y procedimientos que debe cumplir el personal.

5.1. Medios Humanos: Aquí se hará referencia al papel del personal dentro del sistema de seguridad implementado, definiendo sus responsabilidades y funciones respecto al diseño, establecimiento, control, ejecución y actualización del mismo.

Se describirá la estructura concebida en la Entidad para la gestión de la Seguridad Informática, especificando las atribuciones y funciones de las distintas categorías de personal, que incluyen: dirigentes a los distintos niveles (Jefe de la entidad, Jefes de departamentos, áreas y grupos de trabajo o estructuras equivalentes); Jefes y especialistas de informática; Administradores de redes, sistemas y aplicaciones; Especialistas de Seguridad y Protección; Responsables de Seguridad Informática y Usuarios comunes de las tecnologías de Información.

5.2. Medios Técnicos de Seguridad: Se describirán los medios técnicos utilizados en función de garantizar niveles de seguridad adecuados, tanto al nivel de software como de hardware, así como la configuración de los mismos. Para lo cual se tendrá en cuenta:

- Sistemas Operativos y nivel de seguridad instalado,
- Tipo de redes utilizadas y topología de las mismas,
- Conexiones a redes externas a la entidad,
- Servidores de uso interno y externo,
- Configuración de los servicios,
- Barreras de protección y su arquitectura,
- Empleo de Firewall, de Hosts Bastiones, Sistemas Proxy, etc.
- Filtrado de paquetes,
- Herramientas de administración y monitoreo,
- Habilitación de trazas y subsistemas de auditoría,
- Establecimiento de alarmas del sistema,
- Sistemas de protección criptográfica,
- Dispositivos de identificación y autenticación de usuarios,
- Protección contra programas no deseados,
- Software especiales de seguridad,
- Medios técnicos de detección de intrusos,
- Cerraduras de disqueteras,
- Dispositivos de protección contra robo de equipos y componentes,
- Sistemas de aterramiento,
- Protección electromagnética,
- Fuentes de respaldo de energía eléctrica,
- Medios contra incendios,
- Medios de climatización,
- Otros.

5.3. Medidas y Procedimientos de Seguridad Informática

En esta parte del Plan se relacionarán las acciones que deben ser realizadas en cada área específica por el personal a que se hace referencia en el apartado 5.1, en correspondencia con las políticas generales para toda la entidad establecidas en el apartado 4 y con la ayuda, en los casos que lo requieran, de los medios técnicos descritos en el 5.2, adecuando las mismas a las necesidades de protección de cada una de ellas de acuerdo con el peso del riesgo estimado para cada bien informático objeto de protección.

Las medidas y procedimientos de Seguridad Informática que de manera específica (no deben ser confundidas con las políticas que tienen un carácter

general) sean requeridas en las distintas áreas, serán definidas de manera suficientemente clara y precisa, evitando interpretaciones ambiguas por parte de quienes tienen que ejecutarlas y son de obligatorio cumplimiento por las partes implicadas.

Un procedimiento de seguridad es una secuencia predeterminada de acciones dirigida a garantizar un objetivo de seguridad. Los procedimientos que se definan serán descritos en los acápites que correspondan o si se desea se hará referencia a ellos agrupándolos al final del Plan en un anexo.

Su redacción deberá hacerse lo más clara y sencilla posible, precisando de manera inequívoca los pasos a seguir en cada caso para evitar posibles interpretaciones incorrectas, de forma tal que puedan ser ejecutados fielmente por las personas responsabilizadas para ello, sin necesidad de alguna otra ayuda adicional. En caso de agruparse todos como un anexo, el formato a utilizar será el siguiente:

- Denominación del procedimiento (título).
- Secuencia de las acciones a realizar.

Especificando en cada caso: **qué** se hace, **cómo** se hace y **quién** lo hace, así como los recursos que sean necesarios para su cumplimiento.

Algunos procedimientos a considerar son los siguientes:

- Otorgar (retirar) el acceso de personas a las tecnologías de información y como se controla el mismo.
- Asignar (retirar) derechos y permisos sobre los ficheros y datos a los usuarios.
- Autorizar (denegar) servicios a los usuarios. (Ejemplo: Correo Electrónico, Internet)
- Definir perfiles de trabajo.
- Autorización y control de la entrada/salida de las tecnologías de información.
- Gestionar las claves de acceso considerando para cada nivel el tipo de clave atendiendo a su longitud y composición, la frecuencia de actualización, quién debe cambiarla, su custodia, etc.
- Realización de salva de respaldo, según el régimen de trabajo de las áreas, de forma que las salvas se mantengan actualizadas, y las acciones que se

adoptan para establecer la salvaguarda de las mismas, de forma que se garantice la compartimentación de la información según su nivel de confidencialidad.

- Garantizar que los mantenimientos de los equipos, soportes y datos, se realicen en presencia y bajo la supervisión de personal responsable y que en caso del traslado del equipo fuera de la entidad la información clasificada o limitada sea borrada físicamente o protegida su divulgación.
- Salva y análisis de registros o trazas de auditoria, especificando quien lo realiza y con qué frecuencia.

5.3.1. De protección física.

5.3.1.1. A las áreas con tecnologías instaladas

Se precisarán, a partir de las definiciones establecidas en el Reglamento sobre la Seguridad Informática, las áreas que se consideran vitales y reservadas en correspondencia con el tipo de información que se procese, intercambie, reproduzca o conserve en las mismas o el impacto que pueda ocasionar para la Entidad la afectación de los activos o recursos que en ellas se encuentren, relacionando las medidas y procedimientos específicos que se apliquen en cada una. (**Ejemplo:** restricciones para limitar el acceso a los locales, procedimientos para el empleo de cierres de seguridad y dispositivos técnicos de detección de intrusos, etc.)

5.3.1.2. A las Tecnologías de Información

- Se especificarán las medidas y procedimientos de empleo de medios técnicos de protección física directamente aplicados a las tecnologías de información que por las funciones a que están destinadas o por las condiciones de trabajo de las áreas en que se encuentran ubicadas lo requieran. (**Ejemplo:** utilización de cerraduras de disquetera, anclaje de chasis, cerradura de encendido del procesador etc.)
- Posición de las tecnologías de información destinadas al procesamiento de información con alto grado de confidencialidad o sensibilidad en el local de forma que se evite la visibilidad de la información a distancia, minimice la posibilidad de captación de las emisiones electromagnéticas y garantice un mejor cuidado y conservación de las mismas.
- Medidas y procedimientos para garantizar el control de las tecnologías de información existentes, durante su explotación, conservación, mantenimiento y traslado.

5.3.1.3. A los soportes de información

Se describirá el régimen de control establecido sobre los soportes magnéticos de información refiriéndose entre otros aspectos a:

- Lo relacionado con la identificación de los soportes removibles autorizados a utilizar dentro de la entidad, incluyendo su identificación física y lógica.
- Las condiciones de conservación de los soportes, especificando las medidas que garanticen la integridad y confidencialidad de la información en ellos recogida.
- Las medidas y procedimientos que se establecen para garantizar el borrado o destrucción física de la información clasificada o limitada contenida en un soporte una vez cumplida su finalidad.
- Las medidas y procedimientos que se establecen para garantizar la integridad y confidencialidad de la información clasificada o limitada durante el traslado de los soportes.

5.3.2. Técnicas o Lógicas

Se especificarán las medidas y procedimientos de seguridad que se establezcan, cuya implementación se realice a través de software, hardware o ambas.

5.3.2.1. Identificación de usuarios

Se explicará el método empleado para la identificación de los usuarios ante los sistemas, servicios y aplicaciones existentes, especificando:

- Como se asignan los identificadores de usuarios.
- Si existe una estructura estándar para la conformación de los identificadores de usuarios.
- Quien asigna los identificadores de usuarios.
- Como se eliminan los identificadores de usuarios una vez que concluya la necesidad de su uso y como se garantiza que estos no sean utilizados nuevamente.
- Proceso de revisión de utilización y vigencia de los identificadores de usuarios asignados.

5.3.2.2. Autenticación de usuarios.

Se explicará el método de autenticación empleado para comprobar la identificación de los usuarios ante los sistemas, servicios y aplicaciones existentes.

Cuando se utilice algún dispositivo específico de autenticación se describirá su forma de empleo. En el caso de empleo de autenticación simple por medio de contraseñas se especificará:

- Como son asignadas las contraseñas.
- Tipos de contraseñas utilizadas (Setup, Protector de pantalla, Aplicaciones, etc.)
- Estructura y periodicidad de cambio que se establezca para garantizar la fortaleza de las contraseñas utilizadas en los sistemas, servicios y aplicaciones, en correspondencia con el peso de riesgo estimado para los mismos.
- Causas que motivan el cambio de contraseñas antes de que concluya el plazo establecido.

5.3.2.3. Control de acceso a los activos y recursos

En esta parte del Plan se describirán las medidas y procedimientos que aseguran el acceso autorizado a los activos de información y recursos informáticos que requieren la imposición de restricciones a su empleo, especificando:

- A que activos y recursos se le implementan medidas de control de acceso.
- Métodos de control de acceso utilizados.
- Quien otorga los derechos y privilegios de acceso.
- A quien se otorgan los derechos y privilegios de acceso.
- Como se otorgan y suspenden los derechos y privilegios de acceso.

El control de acceso a los activos y recursos deberá estar basado en una política de “mínimo privilegio”, en el sentido de otorgar a cada usuario solo los derechos y privilegios que requiera para el cumplimiento de las funciones que tenga asignadas.

5.3.2..4. Integridad de los ficheros y datos

Se describirán las medidas y procedimientos establecidos con el fin de evitar la modificación no autorizada, destrucción y pérdida de los ficheros y datos, así como para impedir que sean accedidos públicamente, especificando:

- Medidas de seguridad implementadas a nivel de sistemas operativos, aplicación o ambos para restringir y controlar el acceso a las bases de datos.
- Medidas para garantizar la integridad del software y la configuración de los medios técnicos.
- Empleo de medios criptográficos para la protección de ficheros y datos.
- Medidas y procedimientos establecidos para la protección contra virus y otros programas dañinos que puedan afectar los sistemas en explotación, así como para evitar su generalización, especificando los programas antivirus utilizados y su régimen de instalación y actualización.

5.3.2.5. Auditoría y Alarmas

Se describirán las medidas y procedimientos implementados para el registro y análisis de las trazas de auditoría en las redes y sistemas instalados, con el fin de monitorear las acciones que se realicen (acceso a ficheros, dispositivos, empleo de los servicios, etc.), y detectar indicios de hechos relevantes a los efectos de la seguridad que puedan afectar la estabilidad o el funcionamiento del sistema informático.

En caso de empleo de software especializado que permita la detección de posibles errores de configuración u otras vulnerabilidades se describirán los procedimientos requeridos.

Se describirán además las medidas que garanticen la integridad de los mecanismos y registros de auditoría limitando su acceso solo a las personas autorizadas para ello.

5.3.3. Seguridad de operaciones

En esta parte del Plan se incluirán las medidas y procedimientos relacionados con los siguientes aspectos:

- ♦ Identificación y control de las tecnologías en explotación, en particular aquellas donde se procese información clasificada.
- ♦ Control sobre la entrada y salida en la entidad de las tecnologías de información (máquinas portátiles, periféricos, soportes, etc.).
- ♦ Metodología establecida para las salvas de la información, especificando su periodicidad, responsabilidades, cantidad de versiones, etc.)
- ♦ Acciones específicas durante las conexiones externas a la entidad.
- ♦ Autorizar (denegar) servicios a los usuarios. (Ejemplo: Correo Electrónico, Internet)
- Gestión de las claves de acceso considerando para cada nivel el tipo de clave, la frecuencia de actualización, quién debe cambiarla, su custodia, etc.
- Gestión de salvas de respaldo, según el régimen de trabajo de las áreas, incluyendo las acciones que se adoptan para establecer la salvaguarda de las mismas.
- Mantenimientos de los equipos, soportes y datos en presencia y bajo la supervisión de personal responsable y en caso del traslado de equipos fuera de la entidad.
- Salva y análisis de registros o trazas de auditoria, especificando quien lo realiza y con qué frecuencia.

5.3.4. De recuperación ante contingencias

Se describirán las medidas y procedimientos de neutralización y recuperación ante cualquier eventualidad que pueda paralizar total o parcialmente la actividad informática o degraden su funcionamiento, minimizando el impacto negativo de éstas sobre la entidad.

A partir de los resultados obtenidos en el análisis de riesgos, se determinarán las acciones a realizar para neutralizar aquellas amenazas que tengan mayor probabilidad de ocurrencia en caso de materializarse, así como para la recuperación de los procesos, servicios o sistemas afectados, precisando en cada caso:

- Que acciones se deben realizar.
- Quién las realiza.
- En que momento debe realizarlas.
- Como debe realizarlas.
- De qué recursos debe disponer.

6. ANEXOS

6.1. Programa de Seguridad Informática

En esta parte del Plan se incluirán aquellos aspectos cuya realización requiera de un tiempo adicional, ya sea porque necesitan algún tipo de recursos con que no se cuenta, la realización de gestiones complementarias u otras causas, señalando los plazos para su cumplimiento y el personal responsabilizado con su ejecución. Los aspectos que lo requieran deben ser considerados dentro del Plan de Inversiones de la entidad. Algunos aspectos a considerar pudieran ser los siguientes:

- La implementación a mediano y largo plazo de aquellos aspectos que así lo exijan para lograr un nivel de seguridad óptimo, como por ejemplo la introducción de medios técnicos de seguridad, modificación de locales, etc.
- La preparación y capacitación del personal en materia de seguridad informática, según su participación en el sistema diseñado, ya sea a través de cursos específicos, mediante la impartición de materias relacionadas con el tema u otras medidas de divulgación.
- La organización y ejecución de pruebas, inspecciones y auditorías (internas y externas) para asegurar la continuidad de la integridad funcional del Sistema de Seguridad Informática existente, mencionando con que frecuencia se realizan, quienes participan y el contenido de las mismas.

6.2. Listado nominal de Usuarios con acceso a redes de alcance global

Si la entidad tiene acceso a redes de alcance global se anexará un Listado de Usuarios autorizados, especificando Nombre, Apellidos y Cargo que ocupa en la entidad, así como los Servicios para los que está autorizado.

6.3. Registros

Se definirán los documentos de registro que se requieran para el control de la actividad, de acuerdo a los requerimientos del sistema de seguridad diseñado, pudiéndose considerarse entre otros los siguientes:

- Registro de inspecciones.
- Registro y control de los soportes.
- Registro de software de nueva adquisición.
- Registro de entrada, salida y movimiento de tecnologías de información.
- Registro de incidencias de la Seguridad Informática.