Planificación de Políticas de Seguridad

María E. Díaz Valle [(1)] José A. Navarro Maspons [(2)] Ignacio Marín García [(3)]
Facultad de Ingeniería en Electricidad y Computación [(1) (2) (3)]
Escuela Superior Politécnica del Litoral [(1) (2) (3)]
Campus Gustavo Galindo, Km 30.5 Vía Perimetral, Apartado 09-01-5863. Guayaquil, Ecuador [(1) (2) (3)]
maesdiaz@espol.edu.ec [(1)] josanava@espol.edu.ec [(2)] imaringa@fiec.espol.edu.ec [(3)]

Resumen

El presente trabajo consiste en la planificación de las Políticas de Seguridad para Empresas de tamaño medio y que se dedican en especial a brindar algún tipo de servicio de telecomunicaciones.

Para el éxito en el desarrollo de este documento seguimos las recomendaciones que sugieren los estándares ISO/IEC 17799:2005, ISO/IEC 27000:2009, el manual de Políticas de Seguridad Informática- Mejores Prácticas Internacionales y otros adjuntos. Logrando así considerar todos los aspectos de seguridad que se deben analizar en las empresas y consiguiendo además orden y aceptación de las propuestas que exponemos.

Presentamos propuestas que ayudan a realizar una mejora continua de los documentos de Políticas de Seguridad que se han decidido aplicar y de como mejorar la manera en que se integran estas políticas en el ambiente laboral a través de un conjunto de sugerencias que cubren la manera en que deben aplicarse las políticas, darles seguimiento y lo más importante aún conseguir que el personal de la empresa acepte y cumpla con las Políticas.

Palabras Claves: *Políticas de Seguridad, Seguridad en Redes, matriz de cobertura, normas, áreas, audiencias*.

Abstract

The present works consist in planning security policies for medium-sized Companies dedicated specially to give any type of telecommunication services.

For the success in the develop of this document we follow the recommendations that suggest the standards like ISO/IEC 17799:2005, ISO/IEC 27000:2009, "Manual de Políticas de Seguridad Informática-Mejores Prácticas Internacionales and others listed in reference. Considering with this all the security aspect that must analyze in companies and also getting order and acceptance for the exposed proposals.

We present proposals that help to realize a continuous improvement of the security policies documents that have decided to applied and how to increase the way they are integrated in a workplace through a set of suggestion that cover the way the policies must be applied, follow them and more importance to achieve that the personnel accept and respect with the policies.

1. Introducción

A medida que la infraestructura de las empresas crece, se producen un aumento del personal y divisiones departamentales. Esto presenta nuevas dificultades para proteger la información y mantener correctas relaciones laborales entre el personal. Surge así la importancia de implementar mecanismos de seguridad que permitan proteger y dar un orden a la continua expansión de la infraestructura a través del tiempo. El correcto funcionamiento del crecimiento de los sistemas empresariales va ligado de una buena definición de normas, lineamientos, procedimientos y controles que permitan cuidar y alcanzar los intereses gerenciales.

Con la finalidad de definir estas guías adecuadas, se presenta en este documento un manual de reglamentos conocido como "Políticas de Seguridad". Las políticas de seguridad brindan a la empresa la oportunidad de lograr alcanzar los estándares internacionales tanto en seguridad como calidad de sus servicios ofrecidos, otorgando así una buena imagen que permite incrementar la confianza y aceptación de sus clientes.

Quedando claro entonces, la necesidad inmediata de definir un esquema de políticas que aseguren a la empresa de los riesgos que pudieran presentarse.

2. Planteamiento del Problema

Toda empresa necesita de políticas, normas o procedimientos que le permitan llevar un mejor control en las acciones que realiza. Pero, para esto es primordial identificar las áreas en donde se va implementar la seguridad, antes de dar inicio a la escritura del documento. El identificar las áreas claramente, nos permitirá redactar mejor las políticas, porque, desde un principio, las estaremos enfocando directamente al lugar donde se va a dar la seguridad, sabiendo con lo que ya se cuenta y como se lo va a mejorar.

2.1 Áreas de Seguridad

Hay que tener en cuenta que no siempre es necesario o posible para las empresas cubrir todas sus áreas que se puedan identificar con un elevado nivel de seguridad. Las áreas a seleccionar y el nivel de seguridad correspondiente dependerá en gran medida de los intereses primordiales que presenten la gerencia. Podemos distinguir en forma general algunas áreas que las empresas tendrían que tener en cuenta al implementar su seguridad. Entre estas tenemos:

- Seguridad Física y Dispositivos
- Gestión de Riesgo
- Seguridad de Red y Perimetral
- Seguridad de Software y sus aplicaciones
- Seguridad en la Información
- Seguridad en el Desarrollo

2.2 Definición de Política de Seguridad

Las políticas de seguridad son las directrices y objetivos generales de una empresa relativos a la seguridad, expresados formalmente por la dirección general. Éstas forman parte esencial de la seguridad en las empresas y por esta razón deben ser aprobadas por la alta gerencia.

Las Políticas de Seguridad de una empresa son documentos auditables tanto para los auditores internos de la organización, como por los externos y que a su vez facilitan la obtención de nuevas certificaciones.

Es por este motivo que las políticas de seguridad son documentos **que deben ser comprendidos más que aprendidos en todos los niveles**; desde el personal operativo/operador como por los altos mandos (directivos, gerentes, etc.).

2.3 Importancia de la Implementación de Políticas de Seguridad

Con la gran cobertura que brindan hoy en día los medios noticiosos a la seguridad de la información, uno pensaría que los altos mandos de todas las empresas saben de qué se trata esto, lamentablemente en muchos casos no es así. Por eso, antes de empezar a redactar políticas de seguridad, hay que llevar el caso y explicarle detalladamente a la gerencia de que se trata este tema y que beneficios dará a su organización.

La importancia de la implementación de las políticas queda inmediatamente aclarada cuando analizamos problemas comunes que pueden ser resueltos o evitados con la implementación de dichas políticas. Podemos mencionar como ejemplo lo siguiente, una empresa puede adquirir una serie de productos de seguridad, pensando que estos resolverán todas sus dificultades y amenazas, pero a la hora de su implementación descubren que no alcanzan los resultados que esperaban y todo ello debido a que no poseían un conjunto de políticas que aclararan las necesidades de la organización. Es por esto que decimos que los documentos de políticas forman parte primordial de una infraestructura de seguridad que debe tener la empresa.

3. Diseño del Desarrollo de las Políticas

Las políticas de seguridad son documentos que permitan a la empresa obtener un mayor grado de credibilidad y valoración hacia sus clientes; es por esto que se deben desarrollar las políticas basándose en procedimientos y definiciones estandarizadas por organismos internacionales, tales como: la norma ISO/IEC 17799:2005 y la norma ISO/IEC 27000:2009, las cuales nos ayudan con definiciones y estructuración en el documento que se elabora.

3.1 Herramientas Disponibles

Entre un sin número de herramientas existentes para la elaboración de los documentos de políticas de seguridad, tenemos la norma ISO 17799, la norma ISO 27000 y la matriz de cobertura, que sin duda alguna son tres de las herramientas más fáciles de entender y comprender su uso, facilitando de igual manera la elaboración de los documentos de seguridad. Por esta razón son las herramientas utilizadas en el presente documento y que a continuación detallaremos que son y cómo las utilizaremos.

3.1.1 Norma ISO/IEC 17799:2005. El estándar nos indica una serie de consideraciones que debemos tener tanto para la elaboración o selección de las políticas, los riesgos que se deberían analizar, como el contenido que debería tener el documento final que se presentará a la empresa.

Entre las consideraciones más importantes que se siguen en este trabajo tenemos:

- Identificación clara de los objetivos comerciales de la gerencia, obtención de su apoyo y compromiso
- Elaboración de un documento que reciba la aprobación por parte de la gerencia y que permita ser publicado y comunicado a todos los empleados y las partes externas relevantes.
- Asignación de recursos y/o responsabilidades que se presenten debido a las políticas asignadas.

El estándar también nos ofrece un listado claro de las categorías de seguridad principales que se deben analizar en toda organización. Como son:

- Política de seguridad.
- Organización de la seguridad de la información.
- Gestión de activos

3.1.2 Norma ISO/IEC 27000:2009. El objetivo de la norma es la de proveer términos y definiciones. Esta provee una descripción general de los sistemas de gestión sobre la seguridad de la información. Menciona sobre las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Las organizaciones que implementen esta norma podrán obtener: una descripción general de las familias de los estándares SGSI, una introducción a la SGSI, una descripción resumida del proceso PLANIFICAR-HACER-VERIFICAR-ACTUAR (PDCA).

3.1.3 Matriz de Cobertura. La Matriz de Cobertura es muy útil cuando las políticas han de dirigirse a más de dos públicos, a través de documentos diferentes separados. La preparación de esta matriz, es recomendable hacerla antes de la elaboración del primer borrador de las políticas.

Describiendo de una manera sencilla, la matriz de cobertura es solo una tabla de dos dimensiones. Dado que seguramente habrá muchas columnas y pocas filas, se recomienda una matriz de cobertura con títulos de fila para las audiencias definidas en la empresa, los títulos de columnas en blanco para las áreas a cubrir de políticas y finalmente celdas en blanco en el medio para las políticas específicas.

En el siguiente Gráfico, se puede visualizar el modelo de la matriz de cobertura utilizada en este documento para el ordenamiento de las políticas.

	AREAS				
AUDIENCIA	S1	S2	S3	S4	S5
A1					
A2					
A3					

Gráfico 3. 1 Modelo de la Matriz de Cobertura

3.2 Información recaudada de las empresas

La encuesta se elaboró con el fin de determinar un perfil de seguridad actual de la empresa, para luego poder seleccionar y elaborar políticas que resuelvan y mejoren el grado de seguridad.

La encuesta comprende tres partes principales: 1) Información general de la empresa, 2) Información acerca de las políticas de seguridad, e 3) Información detallada de la seguridad de la empresa.

- **Información general de la empresa:** La idea principal aquí, es conocer la información que maneja la empresa, que desea cuidar dentro de la misma, cuáles son sus objetivos en temas de seguridad.
- **Información acerca de las políticas de seguridad:** Con esta parte se desea saber si la empresa posee algún conjunto de políticas o si siguen políticas especificadas en alguna norma estandarizada.
- **Información detallada de la seguridad de la empresa:** Si la empresa posee políticas, las preguntas serán contestadas en base a ellas, caso contrario serán contestadas en base al documento donde establezcan las obligaciones y comportamiento de todos los individuos de la empresa.

4. Formalización de las Políticas de Seguridad

Las políticas que se presentan aquí siguen un modelo general, es decir, sobre un problema se enuncia

una política con una perspectiva amplia de la solución, de tal manera que sea después fácil de modificar si se desea detallar más o dividirlas en varias políticas más específicas. También aplicaremos la elaboración de una matriz de cobertura con el objetivo de lograr un mayor ordenamiento y a su vez entendimiento del listado de política seleccionado.

4.1 Evaluación de Riesgo

A continuación se presenta una lista de factores que en el caso de ocurrir, fallar, o alterarse presentaría una amenaza que perjudicaría a las empresas y sobre la cual se realiza una evaluación de riesgo basada en la opinión y nivel de interés indicado por las personas entrevistadas en las empresas y los resultados obtenidos de las encuestas realizadas.

Activos Organizativos	Amenazas de seguridad	Vulnerabilidades
- Información - Equipos - Personal	- Naturales -Intencionales - Involuntarias	- Físicas - Naturales - Por Hardware - Por Software - En Medios de Almacenamiento - En Comunicación - Humanas

Tabla 4. 1 Listado de factores de posibles riesgos de interés.

Controles Actuales	Controles propuestos
- Utilización de Guardias - Controles de temperaturas - Monitoreo electrónico - Administración de cuentas de usuarios	- Servicios integrados para administración y comunicación. - Circuitos cerrados de televisión - Protección electrónica - Sistemas biométricos - Sistemas de Verificación Automática de Firmas (VAF)

Tabla 4. 1 Listado de factores de posibles riesgos de interés (continuación)

Se observa en la tabla 4.2, que para las empresas las amenazas que involucran: la información, los equipos, el estado de los medios de almacenamiento, los procesos de comunicación en general y la administración sobre los usuarios, es en temas de seguridad una necesidad que se debe resolver con mayor prioridad.

Tipos de Riesgos	Probabilidad	Criticidad	Valor
Sobre Activos de Información	ALTA	ALTA	25
Sobre Activos de Equipos	ALTA	MEDIA	15
Sobre Activos de Personal	MEDIA	BAJA	15
Amenazas Naturales	BAJA	MEDIA	15
Amenazas Intencionales	MEDIA	MEDIA	9
Amenazas Involuntarias	BAJA	BAJA	1
Vulnerabilidades Físicas	BAJA	MEDIA	3
Vulnerabilidades Naturales	BAJA	MEDIA	3
Vulnerabilidades por Hardware	MEDIA	MEDIA	9
Vulnerabilidades por Software	MEDIA	MEDIA	9
Vulnerabilidades en Medios de Almacenamiento	ALTA	BAJA	5
Vulnerabilidades en Comunicación	ALTA	MEDIA	15
Vulnerabilidades Humanas	MEDIA	BAJA	3
Utilización de Guardias	BAJA	BAJA	1
Controles de temperaturas	MEDIA	MEDIA	9
Monitoreo electrónico	MEDIA	BAJA	3
Administración de cuentas de usuarios	ALTA	BAJA	5
Servicios integrados para administración y comunicación	MEDIA	MEDIA	9
Circuitos cerrados de televisión	BAJA	BAJA	1
Protección electrónica	MEDIA	MEDIA	9
Sistemas biométricos	MEDIA	MEDIA	9
Sistemas de Verificación Automática de Firmas (VAF)	BAJA	MEDIA	3

Tabla 4. 2 Se muestra los diferentes Tipos de Riesgos, junto con su factor de probabilidad según la Tabla 4.1

4.2 Listado General de las Políticas

Haciendo uso de las políticas de alto nivel propuestas en el manual de "Políticas de Seguridad Informática" [1], se hará un listado general de políticas que más se acomoden al perfil de las empresas entrevistadas e ir cubriendo de esta manera sus requerimientos y necesidades. La ventaja que presenta la selección de políticas que siguen un modelo general es que en caso de requerir cambios, estas se prestan para ser

modificadas en políticas más específicas si se lo requiere.

A continuación, se enlistan por título cada política y según el orden en que aparecen en el manual de "Políticas de Seguridad Informática" [1]. En el Anexo A se encuentran la lista de todas estas políticas y sus características.

1. Rol de la Información y los Sistemas informáticos.
2. Esfuerzo de Equipo.
3. Personas Involucradas.
4. Propiedad de Archivos y Mensajes.
5. Principales Departamentos que Trabajan en Seguridad de la Información.
6. Tres Categorías de Responsabilidad.
7. Responsabilidades del Propietario.
8. Responsabilidades del Custodio.
9. Responsabilidades del Usuario.
10. Manejo Consistente de la Información.
11. Designaciones para la Clasificación de la Información.
12. Etiquetado de la Clasificación de la Información.
13. Necesidad de Conocer.
14. Identificadores de Usuario y Contraseñas.
15. Identificadores de Usuarios Anónimos.
16. Contraseñas Difíciles de Adivinar.
17. Contraseñas Fáciles de Recordar.
18. Patrones Repetitivos en Contraseñas.
19. Restricciones de las Contraseñas.
20. Almacenamiento de las Contraseñas.
21. Compartir Contraseñas.
22. Declaración de Conformidad.
23. Divulgación de Información a Terceros.
24. Solicitud de Terceros de Información de la empresa.
25. Seguridad Física para Controlar el Acceso a la Información.
26. Conexiones Internas de Red.
27. Conexiones Externas de Red.
28. Modificaciones a las Redes.
29. Teletrabajo.
30. Acceso a Internet.
31. Correo Electrónico.
32. Software antivirus.
33. Erradicación de Virus.
34. Respaldos Limpios.
35. Fuentes de Software.
36. Especificaciones Escritas para los Propietarios.
37. Requisito de Autorización por Seguridad.
38. Control Formal de Cambios.
39. Convenciones para Desarrollo de Sistemas.
40. Licencias Adecuadas.
41. Copias No Autorizadas.
42. Responsabilidad de Respaldar.
43. Protección Antirrobo.
44. Divulgación de la Información de Seguridad.
45. Derechos sobre el Material Desarrollado.
46. Derecho a Investigar y Monitorear.
47. Uso Personal.
48. Conducta Inapropiada.
49. Herramientas que Comprometen la Seguridad.
50. Actividades Prohibidas.
51. Informes Obligatorios.
52. Plan de Seguridad Física.
53. Ubicación del Centro de Computación y Comunicaciones.
54. Distintivos de Identificación.
55. Distintivos Personales.
56. Entradas Individuales.
57. Documentación de las Aplicaciones de Producción.
58. Implementación de Sistemas Multiusuario.
59. Análisis del Impacto sobre la Seguridad Informática.
60. Comité de Gestión de Seguridad Informática.

4.3 Elaboración de la Matriz de Cobertura

La matriz de cobertura no es más que una herramienta que nos permitirá ordenar las políticas según unas áreas y audiencias establecidas previamente.

La asignación de las audiencias es un proceso muy importante, porque serán las personas a la cuales van a estar dirigidas las políticas y a quienes se les asignará los permisos y negaciones para hacer uso de los bienes e información de la empresa.

AUDIENCIAS	DEFINICIÓN
Gerencia	Audiencia encargada de tomar las decisiones en la empresa. (Encargadas de aprobar las políticas).
Departamento Técnico o de IT	Audiencia encargada de administrar, instalar y cuidar los sistemas dentro de la empresa.
Usuarios Finales	Audiencia que hacen usos de los servicios y activos de la empresa.

Tabla 4. 3 Lista de Audiencias y sus definiciones

La definición de las áreas es un proceso primordial para la elaboración del documento de políticas, una correcta definición del área logra que la implementación de las políticas sea más certera al permitir a las audiencias a quienes se les dirige las políticas, entender el objetivo y el alcance que se desea conseguir con las mismas.

ÁREAS	DEFINICIÓN
Ordenadores	Área que relaciona todos los computadores personales de la empresa.
Seguridad Física	Todo lo que concierne al ambiente donde se ubican los equipos y se labora.
Comunicación y Manejo de Datos	Todo lo que concierne a los procesos de comunicación, administración de la información, etc.
Gestión de Riesgo	Se contempla todo lo relacionado a las medidas y contramedidas que se presenten o se llegaran a presentar por causas físicas o legales.
Equipos de Comunicación de Datos	Todo lo referente a equipos que forman parte de la red de comunicación de datos de la empresa.

Tabla 4. 4 Lista de las Áreas junto con sus definiciones

4.4 Planteamiento de la Matriz de Cobertura.

Una vez definidas las audiencias y áreas a las cuales será orientado el documento de las políticas, se procede a armar la matriz de cobertura como paso esencial para la presentación final y general de las políticas.

En la siguiente tabla, se presenta el diseño general de la matriz de cobertura, donde se ha colocado ya las políticas divididas y que cubran la seguridad de cada área establecida.

	AREAS				
AUDIENCIA	ORDENADORES	SEGURIDAD FISICA	COMUNICACIÓN Y MANEJO DE DATOS	GESTION DE RIESGO	EQUIPOS DE COMUNICACIÓN DE DATOS
GERENCIA	N.A.	25-52-53	1-4-11-23-24-45-59-60	3-5-6-7-8-9-28-29-40-46-48	N.A.
DEPARTAMENTO TECNICO	15-16-17-18-19-20-21-27-32-33-35-38-39	14-25-26-43-53-56	1-10-11-13-23-42-47-57-58-59	2-3-5-6-7-8-9-28-29-30-31-34-36-37-41-44-46-48-49	15-16-17-18-19-20-21-22-27-35-38-39
USUARIOS FINALES	15-16-17-18-19-20-21-32-33	25-43-54-55	1-4-11-12-13-23-24-42-45-47-58	2-3-9-28-29-30-31-37-41-46-48-49-50-51	N.A.

Tabla 4.5 Matriz de Cobertura con todas las políticas divididas según el área y audiencia requerida

Ahora, con la matriz de cobertura formada se puede elaborar un índice del listado de las políticas diferente para cada audiencia y ordenado por las áreas, logrando así que el público objetivo pueda concentrarse más en las políticas que les conciernen.

5. Aprobación y Diseño de Proceso de Mejoramiento Continuo de las Políticas.

Como ya se habló anteriormente, no basta implementar algo y pensar que esto funcionará por siempre, es necesario, por no decir obligatorio, seguir un proceso de seguimiento del documento de políticas implementado, que permita mantener siempre las políticas acorde con el crecimiento de la empresa. Y es por esto, que aquí se presenta unos breves pasos que resuman como debería realizarse de manera efectiva este seguimiento.

5.1 Seguimiento de las Políticas de Seguridad

Los procesos de mejoramiento continuo recomiendan que después de toda implementación se realice un seguimiento que evalué y recopile todos los cambios que se produzcan. La mejora continua del proyecto va ligada estrechamente al incremento de la seguridad dentro de la organización.

A continuación se enlista una serie de pasos que se pueden seguir para lograr mejores resultados del documento de políticas de seguridad.

1) Se debe colocar el documento al alcance de todos los usuarios y asegurándose además que se pueda desplazar cómodamente a través de este. Se podría lograr esto colocándolo en un sitio web para uso interno de la empresa, con enlaces hacia las políticas, uso de motores de búsqueda de palabras claves. Debe estar elaborado de tal manera que los usuarios solo se concentren en las políticas de interés para ellos.
2) Se debe ofrecer la oportunidad que los usuarios opinen sobre las políticas, es importante conocer desde el punto de vista del usuario su impresión de las políticas. Los usuarios podrían incluso mediante sus opiniones identificar ciertos requerimientos que las políticas no cubren, y que consideran que deberían. Esto se puede conseguir mediante la elaboración de cuestionarios que se los pueden hacer llegar en pequeños bancos de preguntas que no les tomen más de un minuto o dos cooperar, también este mecanismo puede permitir que el personal se integre con las políticas.
3) La elaboración de un documento legal que permita reflejar el cumplimiento y conocimiento de las políticas por parte del empleado, se debe requerir. El personal de esta manera no tendrán otra opción más que informarse de las políticas y acatarse a ellas.
4) Es importante conocer si el usuario entiende las políticas, principalmente aquellas que se

encuentran dirigidas a sus funciones, equipos e información que maneja. Para esto no basta con tener a alguien que explique, ya que muchas veces la actitud más común que se toma cuando no se entiende es no prestar atención, por esto una solución más correcta es la de elaborar formularios breves sobre los puntos esenciales de un documento de políticas de seguridad.

5) Se puede impartir cursos sobre seguridad dirigida para diferentes audiencias (las que se observan en el documento de políticas, por ejemplo). De esta manera el personal pueden adaptarse mejor a las nuevas medidas que establecen las políticas.
6) Con el objetivo de supervisar las iniciativas que se han tomado sobre seguridad, se debe conformar un comité con supervisores o gerentes de nivel medio. Estos deben encargarse de garantizar que las actividades vigentes de seguridad están en línea con los objetivos del negocio. También tienen que preparar resúmenes de las propuestas que se presentaran a la alta gerencia acerca de los cambios que se debieran hacer sobre el documento de políticas.
7) Cada cierto tiempo se debe analizar todas las propuestas reunidas hasta este momento, y en base a estas comenzar a actualizar el documento de políticas para mantenerlo al día con los requerimientos y objetivos de la empresa. Todos los cambios que se realicen sobre el documento de políticas es importante que se den inmediatamente a conocer a todo el personal de la empresa y que nuevamente se realicen todos pasos de seguimiento sugeridos y quizás esta vez se podrían enfocar más en los cambios.

5.2 Concientización de los Documentos de Políticas.

Concientizar a las audiencias es importante en el proceso de la puesta en marcha de los documentos de políticas. La importancia que la gerencia brinda a la seguridad se ve reflejada en los tópicos que se organizan dentro de la empresa para concientizar. Es difícil esperar que el personal opere según los dictámenes que las políticas determinan si no se ha dado a conocer de manera correcta las políticas.

Las siguientes acciones consideradas serán divididas según la vía que se utilice para su distribución, en la mayoría de los casos es muy necesario distribuir la información por todos los medios aquí sugeridos, como son: En Persona, Por Escrito, En Sistemas y Por Otras Vías; ya que de esta manera no habrá excusas de que las Políticas no fueron distribuidas correctamente y puestas al conocimiento a todo el personal de la organización.

Por escrito:

- Requiera la firma en una declaración de responsabilidad personal que indique que el empleado considera el cumplimiento de las políticas como condición para mantenerse empleado.
- Escriba artículos sobre seguridad para periódicos internos, boletines informativos y revistas.
- Coloque anuncios y señales en las oficinas para recordar a las personas acerca de la seguridad.
- Prepare un documento de la arquitectura de la seguridad informática o integre la seguridad en los planes tecnológicos de la organización.

Sistemas Electrónicos:

- Conduzca evaluaciones de riesgo en seguridad informática, especialmente al hacer entrevistas y utilice otros métodos para comprometer al personal al proceso.
- Solicite al departamento Legal que realice un inventario de propiedad intelectual y una evaluación de riesgos pertinente.
- Emita advertencias que reflejen infracciones a las políticas.
- Integre el adiestramiento de seguridad con otros materiales de adiestramiento en computación, como cursos para teletrabajadores, obligatorio antes de comenzar el trabajo a distancia.

En persona:

- Añada instrucciones de seguridad a programas de aplicaciones y pantallas de ayuda en los sistemas.
- Antes de otorgar a los usuarios acceso a ciertas aplicaciones o facilidades en el sistema, exíjales que asistan a un breve programa de adiestramiento en línea.
- Utilice software especial de identificación de vulnerabilidades para verificar los parámetros de seguridad, alertando al personal de seguridad que existen problemas.

Otras Vías:

- Resuma mensajes de seguridad en bloques de notas que se suministre gratuitamente al personal.
- Establezca una línea caliente con una máquina contestadora donde se puedan reportar problemas de seguridad informática de manera anónima.

7. Conclusiones

Se pudo comprobar que con un buen análisis de riesgo, con las encuestas adecuadas, pero sobre todo con la gran colaboración del personal de las empresas, se logran definir todas las falencias que existían con respecto a la seguridad y así poder diseñar las políticas que ayuden a minimizar esas debilidades y con esto mejorar gran parte la seguridad y los procesos dentro de la empresa.

Con las entrevistas realizadas se comprobó que algunas empresas que recién entran al mercado de la tecnología, hablando de empresas pequeñas y/o medianas, carecen gran parte del conocimiento sobre los beneficios que brindan las políticas de seguridad y el impacto que se produce sobre el crecimiento adecuado de la empresa al no ser implementadas a tiempo.

Se demostró que la definición de las áreas y audiencias a las cuales estarán dirigidas las políticas desde un principio, facilita totalmente la escritura y distribución de las mismas. Logrando el entendimiento general de las políticas en todo el personal de la empresa y con ello su aceptación definitiva.

Se comprobó que teniendo como base los criterios de las normas ISO 17799, ISO 27000 y los del manual de "Políticas de Seguridad Informática", se desarrollaron las políticas con las adecuadas medidas legales, evitando caer en la redundancia y politiquería por la falta de seriedad al momento de su redacción. Consiguiendo además con esto, un documento que se puede ajustar a los requerimientos de las empresas medianas.

Se demostró que llevando un adecuado cronograma de trabajo, donde se describan objetivos específicos a alcanzar, se logra más fácilmente culminar con éxitos el proyecto propuesto. Teniendo siempre presente separar algunos días de gracia, para algún contratiempo que pueda surgir y así no perder el objetivo planteado.

8. Referencias Bibliográficas

[1] Charles Cresson Wood, CISA, CISSP. *Políticas de Seguridad Informática – Mejores Prácticas Internacionales, Conjunto Complejo de Políticas de Seguridad Informática*, Versión 9. Publicado por NetIQ, Inc, Septiembre 2002, pág. 6

[2] Subsecretaría de Tecnologías Informáticas – Secretaría de la Función Pública. *Manual de Seguridad en Redes*, Coordinación de Emergencia en Redes Teleinformática. http://www.arcert.gov.ar/webs/manual/manual_de_seguridad.pdf. Consultado el 14 de Enero del 2011, pág. 1-1

[3] Antonio Villalón Huerta, *El Sistema de Gestión de Seguridad de la Información*, La Nueva Norma UNE 71502. Grupo S2, Septiembre 2004. http://www.shutdown.es/ISO17799.pdf. Consultado el 16 de Enero del 2011.

[4] Microsoft-TechNet, *Guía de administración de riesgos de seguridad de Microsoft*. Octubre 2004. http://www.microsoft.com/spain/technet/recursos/articulos/srsgch00.mspx . Consultado el 20 de Enero del 2011.

[5] Organización Internacional para la Estandarización, *Abstracto del ISO/IEC 27000:2009*. Junio 2010. http://www.iso.org/iso/catalogue_detail?csnumber=41933. Consultado el 16 de Enero del 2011.

[6] Scott Barman, *Writing Information Security Policies*, Publishing by New Riders, First Edition, November 2001.