UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

IMPLEMENTACION DE POLITICAS DE SEGURIDAD BASADAS EN LA NTP ISO/IEC 17799:2004

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

JAVIER ANDRES POLTI FIGALLO

PROMOCIÓN

1983 - II

LIMA – PERÚ

2007

IMPLEMENTACION DE POLITICAS DE SEGURIDAD BASADAS EN LA NTP ISO/IEC 17799:2004

SUMARIO

El presente trabajo pretende describir la implementación práctica de la norma ISO11199 a través de la norma técnica peruana en una mediana empresa, la cual se ha impuesto como estándar de la industria en lo que a seguridad de la información se refiere.

El Capítulo I, describe la historia de la Norma ISO/IEC 17799: 2000 Information Technology – Code of practice for information security Management y su adecuación a la realidad peruana a través del Proyecto de Tecnología de la Información, llevado a cabo por la Presidencia del Consejo de Ministros el año 2004.

El Capítulo II, se enfoca en las metodologías de análisis de riesgo, la herramienta utilizada para realizar el análisis de brecha de la institución ha ser evaluada, así como la comparación de dicha brecha con el estándar de la industria.

El Capítulo III, describe la implementación de la norma en una compañía mediana de seguros que debido a los requerimientos de seguridad necesita desarrollar e implantar dichas normas en su plataforma de hardware y software así como comunicar las políticas administrativas.

INDICE

PRÓLOGO

Hoy en día los sistemas de información constituyen uno de los activos más importantes para las empresas en un entorno tan competitivo y completo. La información administrada por todos los niveles de la organización es fundamental para gestionar las empresas en forma eficiente. De ahí que la importancia en la seguridad de la información se torna critica para poder competir en el mercado actual.

Por tal motivo es de suma importancia establecer las políticas de seguridad hacia dicho activo, "la información", de lo contrario estaremos gestionando la información en forma ineficiente y con posibilidades de error, fraude y otros que pueden devenir en situaciones de perdida de competitividad y problemas legales.

Las normas ISO17799 y la BS-7799 dan las pautas generales para gestionar la seguridad de información. Generalmente se asocia la implementación de dichas normas a grandes inversiones y empresas con grandes volúmenes de información.

El presente trabajo muestra como una mediana empresa que se ve en la necesidad de controlar y gestionar su información puede implementar los mecanismos de seguridad de la información con costos accesibles.

El trabajo se centrara en la aplicación de las políticas de seguridad a los capítulos que contengan un alto componente tecnológico tales como sistemas de acceso, comunicaciones IP, virus, redes virtuales, etc. Estas tecnologías al aplicarse en las empresas tienen un alto componente de seguridad que muchas veces no se toman en cuenta y que generalmente su implementación se percibe con altos costos.

CAPITULO I
DESCRIPCIÓN GENERAL DE LA NORMA

1.1 Introducción

La información es un activo que, como otros activos importantes del negocio tiene un valor para la organización y requiere en consecuencia una protección adecuada. La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio minimizar los daños de la organización y maximizar el retorno de las inversiones y las oportunidades del negocio.

La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La siguiente figura caracteriza los tres componentes principales de la seguridad de información:

Figura 1.1: Componentes de la Seguridad de Información

La seguridad de la información se caracteriza aquí como la preservación de:

a) **Su confidencialidad**, asegurando que solo quienes estén autorizados pueden acceder a la información;

b) **Su integridad**, asegurando que la información y sus métodos de proceso son exactos y completos;
c) **Su disponibilidad**, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

La seguridad de la información se consigue implantando un conjunto adecuado de controles que pueden ser políticas, practicas, procedimientos, estructuras organizativas y funciones de software. Estos controles deberían establecerse para asegurar que se cumplen los objetivos específicos de seguridad de la organización.

¿Por que es necesaria la seguridad de la información?

La información y los procesos que la apoyan, sistemas y redes son importantes activos de la organización. La disponibilidad, integridad y confidencialidad de la información pueden ser esenciales para mantener su competitividad, Tesorería, rentabilidad, cumplimiento de la legalidad e imagen comercial.

Las organizaciones y sus sistemas de información se enfrentan, cada vez mas, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La dependencia de los sistemas y servicios de información implica que las organizaciones son más vulnerables a las amenazas a su seguridad. La dificultad de conseguir el control de los accesos se incrementa al interconectar las redes públicas con las privadas y al compartir los recursos de información. La tendencia hacia la informática distribuida debilita la eficacia de un control central y especializado.

Muchos sistemas de información no se han diseñado para ser seguros, La seguridad que puede lograrse a través de los medios técnicos es limitada, y debería apoyarse en una gestión y unos procedimientos adecuados. La identificación de los controles que deberían instalarse requiere una planificación cuidadosa y una atención al detalle. La gestión de la seguridad de la información necesita, como mínimo, la participación de todos los empleados de la organización. También puede requerir la participación de los proveedores, clientes o accionistas. La asesoría especializada de organizaciones externas también puede ser necesaria.

Los controles sobre seguridad de la información son considerablemente más baratos y eficaces si se incorporan en la especificación de los requisitos y en la fase de diseño.

¿Cómo establecer los requisitos de seguridad?

Es esencial que la organización identifique sus requisitos de seguridad. Existen tres fuentes principales.

La primera fuente procede de la valoración de los riesgos de la organización. Con ella se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia y se estima su posible impacto.

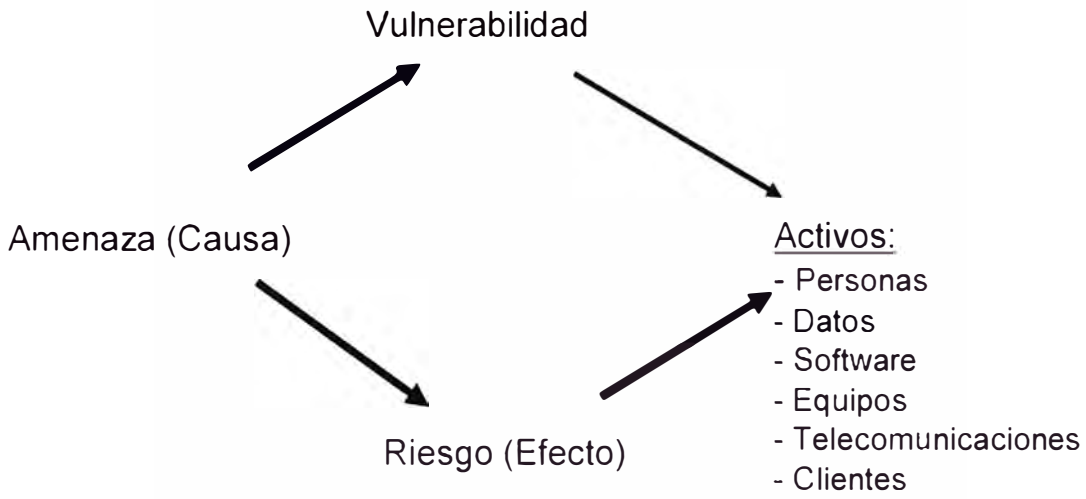

Figura 1.2: Análisis de Amenazas a los Activos de Información

La segunda fuente es el conjunto de requisitos legales, estatutos, regulaciones y contratos que debería satisfacer la organización, sus socios comerciales, los contratistas y los proveedores de servicios.

La tercera fuente esta formada por los principios, objetivos y requisitos que forman parte del tratamiento de la información que la organización ha desarrollado para apoyar sus operaciones.

Evaluación de los riesgos de seguridad

Los requisitos de seguridad se identifican mediante una evaluación metódica de los riesgos. El gasto en controles debería equilibrarse con el posible impacto económico, resultante de los fallos de seguridad. Las técnicas de evaluación de riesgos pueden

aplicarse a toda la organización, solo a partes de ella o incluso a sistemas de información individuales, a componentes específicos de sistemas o a servicios donde sea factible, realista y útil.

La evaluación del riesgo es una consideración sistemática:

a) Del impacto económico que probablemente resulte de un fallo de seguridad, teniendo en cuenta las posibles consecuencias de perdida de confidencialidad, integridad o disponibilidad de la información y otros activos;
b) De la probabilidad realista de que ocurra dicho fallo a la luz de las amenazas y vulnerabilidades existentes, así como de los controles implantados.

Los resultados de esta evaluación ayudaran a encauzar y determinar una adecuada acción gerencial y las prioridades para gestionar los riesgos de seguridad de la información, y la implantación de los controles seleccionados para protegerse contra dichos riesgos. El proceso de evaluación de riesgos y selección de controles, pude requerir que sea realizado varias veces para cubrir partes diferentes de la organización o sistemas de información individuales.

Es importante efectuar revisiones periódicas de los riesgos de seguridad y de los controles implantados para:

a) Tener en cuenta los cambios de los requisitos y las prioridades de negocio de la organización;
b) Considerar nuevas amenazas y vulnerabilidades
c) Confirmar que las medidas de control siguen siendo eficaces y apropiadas

Deberían realizarse estas revisiones con distintos niveles de detalle dependiendo de los resultados de las evaluaciones previas y de los umbrales de riesgo que la gerencia esta dispuesta a aceptar. Su suelen realizar las evaluaciones de riesgo primero a alto nivel, como un medio de priorizar recursos en áreas de alto riesgo, y después en un nivel mas detallado para enfocar riesgos específicos.

Selección de controles

Una vez que los requisitos de seguridad han sido identificados, deberían elegirse e implantarse los controles que aseguren la reducción de los riesgos a un nivel aceptable. Pueden elegirse los controles partiendo de este documento, de otros conjuntos de

controles o de nuevos controles que puedn diseñarse para cubrir adecuadamente las necesidades específicas. Hay muchas formas distintas de gestionar los riesgos y este documento proporciona ejemplos de enfoques habituales. Sin embargo hay que reconocer que ciertos controles no son aplicables para todos los sistemas o entornos de información y pueden no ser de aplicación en todas las organizaciones. Por ejemplo, pueden segregarse ciertas tareas para evitar fraudes y errores. Las organizaciones pequeñas podrían no segregar todas las tareas y necesitarían otras formas para conseguir el mismo objetivo de control. Por poner otro ejemplo, se puede hacer el seguimiento del uso del sistema y recogerse evidencias. Las medidas de control descritas como el registro de eventos podrían entrar en conflicto con la legislación aplicable, como la referente a la protección de la intimidad de los datos de carácter personal de los clientes o de los datos laborales.

Los controles deberían elegirse por su costo de implantación en relación con los riesgos a reducir y con las posibles perdidas si se materializa la ruptura de seguridad. También es conveniente tener en cuenta factores no económicos como la perdida de reputación.

Ciertos controles expuestos en este documento, pueden considerarse como principios que guían la gestión de la seguridad de la información, aplicables a la mayoría de las organizaciones. Estos se explican en más detalle en el siguiente inciso denominado “Punto de partida de la seguridad de la información”.

Punto de partida de la seguridad de la información.

Cierto número de controles se consideran principios orientativos que proporcionan un punto de partida adecuado para implantar la seguridad de la infamación. Se apoyan en requisitos legislativos esenciales o se considera la mejor práctica habitual para conseguir dicha seguridad.

Los controles que se consideran esenciales para una organización desde un punto de vista legislativo comprenden:

a) La protección de los datos de carácter personal y la intimidad de las personas;
b) La salvaguardia de los registros de la organización;
c) Los derechos de la propiedad intelectual.

Los controles que se consideran la mejor práctica habitual para conseguir la seguridad de la información comprenden:

- La documentación de la política de seguridad de la información;
- La asignación de responsabilidades de seguridad;
- La formación y capacitación para la seguridad de la información;
- El registro de las incidencias de seguridad;
- La gestión de la continuidad del negocio.

Estos controles pueden aplicarse a la mayoría de las organizaciones y los entornos. Es conveniente señalar que pese a la importancia dada a los controles en este documento, la importancia de cualquier control debería determinarse a la luz de los riesgos específicos que afronta la organización. Por tanto y aunque el enfoque anterior se considere un buen punto de partida, no sustituye a la selección de controles basada en una evaluación de riesgo.

Factores críticos de éxito

La experiencia muestra que los siguientes factores suelen ser críticos para el éxito de la implantación de la seguridad de la información en una organización:

a) Una política, objetivos y actividades que reflejen los objetivos del negocios de la organización;
b) Un enfoque para implantar la seguridad que sea consistente con la cultura de la organización;
c) El apoyo visible y el compromiso de la alta gerencia;
d) Una buena comprensión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo;
e) La convicción eficaz de la necesidad de la seguridad a todos los directivos y empleados;
f) La distribución de guías sobre la política de seguridad de la información de la organización y de normas a todos los empleados y contratistas;
g) La formación y capacitación adecuadas;
h) Un sistema integrado y equilibrado de medida que permita evaluar el rendimiento de la gestión de la seguridad de la información y sugerir mejoras.

Desarrollo de directrices propias

Este código de buenas prácticas puede verse como punto para desarrollar la gestión especifica de la seguridad en una organización. Pueden no ser aplicables todas las recomendaciones y controles de este código. Incluso pueden requerirse controles adicionales que este documento no incluye. Cuando esto sucede puede ser útil mantener referencias cruzadas que faciliten la comprobación de la conformidad a lo auditores y otros asociados de la organización.

1.2 Términos y Definiciones

Para los fines de la aplicación de la Norma son de aplicación las definiciones siguientes:

Seguridad de la información

Preservación de la confidencialidad, integridad y disponibilidad de la información.

Confidencialidad

Aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.

Integridad

Garantía de la exactitud y el contenido completo de la información y los métodos de su procesamiento.

Disponibilidad

Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados,

Evaluación del Riesgo

Proceso de evaluación de las amenazas, impactos y vulnerabilidades de la información y de los medios de tratamiento de la información y de su probable ocurrencia.

Gestión del Riesgo

Proceso de Identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos que afecten a los sistemas de información.

1.3 Política de Seguridad

El Objetivo es dirigir y dar soporte a la gestión de la seguridad de la información. La gerencia debe establecer de forma clara y precisa las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización.

La gerencia deberá aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información. Debería establecer el compromiso e la gerencia y el enfoque de la organización para gestionar la seguridad de la información. El documento debería contener como mínimo la siguiente información:

a) Una definición de la seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo que permite compartir la información (véase capitulo de introducción);
b) El establecimiento del objetivo de la gerencia como soporte de los objetivos y principios de la seguridad de la información;
c) Una breve explicación de las políticas, principios, normas y requisitos de conformidad mas importantes para la organización, por ejemplo :

- Conformidad con los requisitos legislativos y contractuales
- Requisitos de formación en seguridad
- Prevención y detección de virus y otro software malicioso
- Gestión de la continuidad del negocio
- Consecuencias de las violaciones de la política de seguridad

d) Una definición de las responsabilidades generales y especificas en materia de gestión de la seguridad de la información, incluida la comunicación de las incidencias de seguridad;
e) Las referencias a documentación que pueda sustentar la política: por ejemplo, políticas y procedimientos mucho más detallados para sistemas de información específicos o las reglas de seguridad que los usuarios deberían cumplir.

Esta política debería distribuirse por toda la organización, llegando hasta a todos los destinatarios en una forma que sea apropiada, entendible y accesible.

La política debería tener un propietario que sea responsable de su mantenimiento y revisión conforme a un proceso de revisión definido. Este proceso debería asegurar que la revisión responde a todo cambio que afecte a las bases de la evaluación original de riesgo, por ejemplo, incidencias de seguridad significativas, nuevas vulnerabilidades o cambios a la infraestructura organizacional o técnica. También deberían programarse revisiones periódicas de:

a) La efectividad de la política, demostrada por la naturaleza, numero e impacto de las incidencias de seguridad registradas;
b) El costo y el impacto de los controles en la eficiencia del negocio;
c) Los efectos de los cambios a la tecnología.

1.4 Capítulos de la Norma

1.4.1 Política de Seguridad

a) **Política de seguridad de la información,** dirigir y dar soporte a la gestión de la seguridad de la información.

1.4.2 Aspectos Organizativos de la Información

a) **Estructura para la seguridad de la información**
   Gestionar la seguridad de la información dentro de la organización
b) **Seguridad en los accesos de terceras partes**
   Mantener la seguridad de que los recursos de tratamiento de la información y de los activos de información de la organización sean accesibles por terceros.
c) **Outsourcing**
   Mantener la seguridad de la información cuando la responsabilidad de su tratamiento se ha externalizado a otra organización.

1.4.3 Clasificación y Control de Activos

a) **Responsabilidad sobre los activos**
   Mantener una protección adecuada sobre los activos de la organización

b) **Clasificación de la información**

Asegurar un nivel de protección adecuado a los activos de la información

1.4.4 Seguridad Ligada al Personal

a) **Seguridad en la definición del trabajo y los recursos**

Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios.

b) **Formación de usuarios**

Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo.

c) **Respuesta ante incidencias y malos funcionamientos de la seguridad**

Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos

1.4.5 Seguridad Física y del Entorno

a) **Áreas Seguras**

Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización.

b) **Seguridad de los equipos**

Evitar perdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización.

c) **Controles generales**

Prevenir las exposiciones a riesgo o robos de información y de recursos de tratamiento de información

1.4.6 Gestión de Comunicaciones y Operaciones

a) **Procedimientos y responsabilidades de operación**

Asegurar la operación correcta y segura de los recursos de tratamiento de información.

b) **Planificación y aceptación del sistema**

Minimizar el riesgo de fallos de los sistemas

c) **Protección contra software malicioso**

Proteger la integridad del software y de la información

d) **Gestión interna de respaldo y recuperación**

Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicaciones

e) **Gestión de redes**

Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo

f) **Utilización y seguridad de los medios de información**

Evitar daños a los activos e interrupciones de las actividades de la organización

g) **Intercambio de información y software**

Evitar la perdida, modificación o mal uso de la información intercambiada entre organizaciones.

1.4.7 Control de Accesos

a) **Requisitos de negocio para el control de accesos**

Controlar los accesos a la información

b) **Gestión de acceso de usuarios**

Evitar accesos no autorizados a los sistemas de información

c) **Responsabilidades de los usuarios**

Evitar el acceso de usuarios no autorizados

d) **Control de acceso a la red**

Protección de los servicios de la red

e) **Control de acceso al sistema operativo**

Evitar accesos no autorizados a los computadores

f) **Control de acceso a las aplicaciones**

Evitar el acceso no autorizado a la información contenida en los sistemas.

g) **Seguimiento de accesos y usos del sistema**

Detectar actividades no autorizadas

h) **Informática móvil y tele trabajo**

Garantizar la seguridad de la información cuando se usan dispositivos de informativa móvil y tele trabajo.

1.4.8 Desarrollo y Mantenimiento de Sistemas

a) **Requisitos de seguridad de los sistemas**

Asegurar que la seguridad este imbuida dentro de los sistemas de información.

b) **Seguridad de las aplicaciones del sistema**

Evitar perdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.

c) **Controles criptográficos**

Proteger la confidencialidad, autenticidad o integridad de la información.

d) **Seguridad de los archivos del sistema**

Para asegurar que los proyectos de Tecnología de la Información (TI) y las actividades complementarias sean llevadas a cabo de una forma segura. El acceso a los archivos del sistema debería ser controlado.

e) **Seguridad en los procesos de desarrollo y soporte**

Mantener la seguridad del software de aplicación y la información

1.4.9 Gestión de Continuidad del Negocio

a) **Aspectos de la gestión de continuidad del negocio**

Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a grandes fallos o desastres.

1.4.10 Cumplimiento

a) **Cumplimiento con los requisitos legales**

Evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de todo requisito de seguridad.

b) **Revisiones de la política de seguridad y de la conformidad técnica**

Asegurar la conformidad de los sistemas con las políticas y normas de seguridad

c) **Consideraciones sobre la auditoria de sistemas**

Maximizar la efectividad y minimizar las interferencias en el proceso de auditoria del sistema.

1.5 Estructura Jerárquica.

Los capítulos descritos en el punto anterior contienen una estructura jerárquica en la medida que cada uno se descompone en campos de aplicación por cada acápite de la norma.

La siguiente es la estructura de la Norma y sus campos de aplicación:

Tabla 1.1: Estructura Jerárquica de la Norma de Seguridad

3 POLITICA DE SEGURIDAD

3.1 Política de seguridad de la información

3.1.1 Documento de política de seguridad de la información
3.1.2 Revisión y evaluación

4. ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

4.1 Estructura para la seguridad de la información

4.1.1 Comité de gestión de seguridad de la información
4.1.2 Coordinación de la seguridad de la información
4.1.3 Asignación de responsabilidades para la seguridad de la información
4.1.4 Proceso de autorización de recursos para el tratamiento de la información
4.1.5 Asesoramiento de especialista en seguridad de la información
4.1.6 Cooperación entre organizaciones
4.1.7 Revisión independiente de la seguridad de la información

4.2 Seguridad en los accesos de terceras partes

4.2.1 Identificación de riesgos por el acceso de terceros
4.2.2 Requisitos de seguridad en contratos con terceros

4.3 Outsourcing

4.3.1 Requisitos de seguridad en contratos de outsourcing

5. CLASIFICACIÓN Y CONTROL DE ACTIVOS

5.1 Responsabilidad sobre los activos

5.1.1 Inventario de archivos

5.2 Clasificación de la información

5.2.1 Guías de clasificación
5.2.2 Marcado y tratamiento de la información

6. SEGURIDAD LIGADA AL PERSONAL

6.1 Seguridad en la definición del trabajo y los recursos

6.1.1 Inclusión de la seguridad en las responsabilidades laborales
6.1.2 Selección y política de personal
6.1.3 Acuerdos de confidencialidad
6.1.4 Términos y condiciones de la relación laboral

6.2 Formación de usuarios

6.2.1 Formación y capacitación en seguridad de la información

6.3 Respuesta ante incidencias y malos funcionamientos de la segu

6.3.1 Comunicación de las incidencias de seguridad
6.3.2 Comunicación de las debilidades de seguridad
6.3.3 Comunicación de los fallos del software
6.3.4 Aprendiendo de las incidencias
6.3.5 Procedimiento disciplinario

7. SEGURIDAD FÍSICA Y DEL ENTORNO

7.1 Áreas seguras

7.1.1 Perímetro de seguridad física
7.1.2 Controles físicos de entrada
7.1.3 Seguridad de oficinas, despachos y recursos
7.1.4 El trabajo en las áreas seguras
7.1.5 Áreas aisladas de carga y descarga

7.2 Seguridad de los equipos

7.2.1 Instalación y protección de equipos
7.2.2 Suministro eléctrico
7.2.3 Seguridad del cableado
7.2.4 Mantenimiento de equipos
7.2.5 Seguridad de equipos fuera de los locales de la organ
7.2.6 Seguridad en el reuso o eliminación de equipos

7.3. Controles generales

7.3.1 Política de puesto de trabajo despejado y bloqueo de
7.3.2 Extracción de pertenencias

8. GESTION DE COMUNICACIONES Y OPERACIONES

8.1 Procedimientos y responsabilidades de operación

8.1.1 Documentación de procedimientos operativos
8.1.2 Control de cambios operacionales
8.1.3 Procedimientos de gestión de incidencias
8.1.4 Segregación de tareas
8.1.5 Separación de los recursos para desarrollo y para producción
8.1.6 Gestión de servicios externos

8.2 Planificación y aceptación del sistema

8.2.1 Planificación de la capacidad
8.2.2 Aceptación del sistema

8.3 Protección contra software malicioso

8.3.1 Medidas y controles contra software malicioso

8.4 Gestión interna de respaldo y recuperación

8.4.1 Recuperación de la información
8.4.2 Diarios de operación
8.4.3 Registro de fallos

8.5 Gestión de redes

8.5.1 Controles de red

8.6 Utilización y seguridad de los medios de informaci

8.6.1 Gestión de medios removibles
8.6.2 Eliminación de medios
8.6.3 Procedimientos de manipulación de la información
8.6.4 Seguridad de la documentación de sistemas

8.7 Intercambio de información y software

8.7.1 Acuerdos para intercambio de información y software
8.7.2 Seguridad de medios en tránsito
8.7.3 Seguridad en comercio electrónico
8.7.4 Seguridad del correo electrónico
8.7.5 Seguridad de los sistemas ofimáticos
8.7.6 Sistemas públicamente disponibles
8.7.7 Otras formas de intercambio de información

9. CONTROL DE ACCESOS

9.1 Requisitos de negocio para el control de accesos
- 9.1.1 Política de control de accesos

9.2 Gestión de acceso de usuarios
- 9.2.1 Registro de usuario
- 9.2.2 Gestión de privilegios
- 9.2.3 Gestión de contraseñas de usuario
- 9.2.4 Revisión de los derechos de acceso de los usuarios

9.3 Responsabilidades de los usuarios
- 9.3.1 Uso de contraseña
- 9.3.2 Equipo informático de usuario desatendido

9.4 Control de acceso a la red
- 9.4.1 Política de uso de los servicios de la red
- 9.4.2 Ruta forzosa
- 9.4.3 Autenticación de usuarios para conexiones externas
- 9.4.4 Autenticación de nodos de la red
- 9.4.5 Protección a puertos de diagnóstico remoto
- 9.4.6 Segregación en las redes
- 9.4.7 Control de conexión a las redes
- 9.4.8 Control de enrutamiento en la red
- 9.4.9 Seguridad de los servicios de red

9.5 Control de acceso al sistema operativo
- 9.5.1 Identificación automática de terminales
- 9.5.2 Procedimientos de conexión de terminales
- 9.5.3 Identificación y autenticación del usuario
- 9.5.4 Sistema de gestión de contraseñas
- 9.5.5 Utilización de las facilidades del sistema
- 9.5.6 Protección del usuario frente a coacciones
- 9.5.7 Desconexión automática de terminales
- 9.5.8 Limitación del tiempo de conexión

9.6 Control de acceso a las aplicaciones
- 9.6.1 Restricción de acceso a la información
- 9.6.2 Aislamiento de sistemas sensibles

9.7 Seguimiento de accesos y usos del sistema
- 9.7.1 Registro de incidencias
- 9.7.2 Seguimiento del uso de los sistemas
- 9.7.3 Sincronización de relojes

9.8 Informática móvil y teletrabajo
- 9.8.1 Informática móvil
- 9.8.2 Teletrabajo

10. DESARROLLO Y MANTENIMIENTO DE SISTEMAS

10.1 Requisitos de seguridad de los sistemas
- 10.1.1 Análisis y especificación de los requisitos de seguridad

10.2 Seguridad de las aplicaciones del sistema
- 10.2.1 Validación de los datos de entrada
- 10.2.2 Control del proceso interno
- 10.2.3 Autenticación de mensajes
- 10.2.4 Validación de los datos de salida

10.3 Controles criptográficos
- 10.3.1 Política de uso de los controles criptográficos
- 10.3.2 Cifrado
- 10.3.3 Firmas digitales
- 10.3.4 Servicios de no repudio
- 10.3.5 Gestión de claves

10.4 Seguridad de los archivos del sistema
- 10.4.1 Control del software en producción
- 10.4.2 Protección de los datos de prueba del sistema
- 10.4.3 Control de acceso a la librería de programas fuente

10.5 Seguridad en los procesos de desarrollo y soport
- 10.5.1 Procedimientos de control de cambios
- 10.5.2 Revisión técnica de los cambios en el sistema opera
- 10.5.3 Restricciones en los cambios a los paquetes de soft
- 10.5.4 Canales encubiertos y código Troyano
- 10.5.5 Desarrollo externo del software

11 GESTIÓN DE CONTINUIDAD DEL NEGOCIO

11.1 Aspectos de la gestión de continuidad del negocio

11.1.1 Proceso de gestión de la continuidad del negocio
11.1.2 Continuidad del negocio y análisis de impactos
11.1.3 Redacción e implantación de planes de continuidad
11.1.4 Marco de planificación para la continuidad del negocio
11.1.5 Prueba, mantenimiento y reevaluación de los planes de continuidad

12. CUMPLIMIENTO

12.1 Cumplimiento con los requisitos legales

12.1.1 Identificación de la legislación aplicable
12.1.2 Derechos de propiedad intelectual (DPI)
12.1.3 Salvaguarda de los registros de la organización
12.1.4 Protección de los datos y de la privacidad de la información personal
12.1.5 Evitar el mal uso de los recursos de tratamiento de la información
12.1.6 Regulación de los controles criptográficos
12.1.7 Recopilación de pruebas

12.2 Revisiones de la política de seguridad y de la conformidad técnica

12.2.1 Conformidad con la política de seguridad
12.2.2 Comprobación de la conformidad técnica

12.3 Consideraciones sobre la auditoria de sistemas

12.3.1 Controles de auditoría de sistemas
12.3.2 Protección de las herramientas de auditoría de sistemas

1.6 Conclusión y Alcance

El presente trabajo tiene como marco conceptual la NTP ISO/IEC 17799:2004 y la norma BS 7999.2:2002.

El presente informe esta compuesto por los capítulos de la norma asociados a tecnología aplicada, los cuales se han descrito en el presente capítulo.

La NTP ISO/IEC 17799:2004, contiene 10 grandes capítulos de seguridad:

1. Política de seguridad
2. Aspectos organizativos para la seguridad
3. Clasificación y control de activos
4. Seguridad ligada al personal
5. Seguridad física y del entorno
6. Gestión de comunicaciones y operaciones
7. Control de accesos
8. Desarrollo y mantenimiento de sistemas
9. Gestión de continuidad
10. Cumplimiento

La implementación de la norma en algunos capítulos son procedimientos y políticas y no mencionan los ítems o herramientas tecnológicas asociadas que se deben gestionar en su adecuación a la norma.

Por tal motivo se ha procedido ha agrupar los capítulos respectivos:

- Grupo 1: Capítulos correspondientes a la gestión de la seguridad.
- Grupo 2: Capítulos correspondientes a tecnología aplicada a la seguridad.

Grupo 1: Capítulos correspondientes a la gestión de la seguridad.

Los siguientes capítulos desarrollan políticas y procedimientos escritos para aplicar la norma. Estos capítulos, tienen pocos aspectos tecnológicos, su objetivo principal es la gestión de la seguridad.

- Capítulo 1: Política de seguridad
- Capítulo 2: Aspectos organizativos para la seguridad
- Capítulo 3: Clasificación y control de activos
- Capítulo 9: Gestión de Continuidad.
- Capítulo 10: Cumplimiento

Grupo 2: Capítulos correspondientes a tecnología aplicada a la seguridad.

Los siguientes capítulos desarrollan y describen la tecnología implementada en la empresa.

Capitulo 4: Seguridad ligada al personal

Capitulo 5: Seguridad física y del entorno

Capitulo 6: Gestión de comunicaciones y operaciones

Capitulo 7: Control de accesos

Capitulo 8: Desarrollo y mantenimiento de sistemas

Como veremos más adelante al utilizar la herramienta de benchmarking (análisis de brecha) la empresa se plantea la estrategia de desarrollar los capítulos de 5, 6 y 7.

CAPÍTULO II
ANÁLISIS Y EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

2.1 Herramienta de Administración de Riesgos

Para tal fin se desarrolló una herramienta a fin de medir el estado actual de la seguridad de información de cada subsidiaria contra el objetivo planteado.

La herramienta se denomina Cuestionario de Metas de Seguridad (ISAAQ por su siglas en ingles) dicha herramienta muestra claramente la relación entre los riesgos y los controles de seguridad de la información, del mismo modo sus resultados sirven como elemento principal para desarrollar los planes de acción para implementar la seguridad de información en la empresa.

2.2 Desarrollo del Benchmarking de Seguridad

2.2.1 Completando el ISSAQ:

El llenado del ISSAQ se hizo siguiendo las siguientes 4 etapas:

1. Completar el Registro de Riesgos (Risk Register), haciendo cambios donde fueron necesarios.
2. Evaluación de la organización contra la hoja de Control de Dominios (desde la hoja 3-Políticas a la 12-Cumplimiento)
3. Revisión de los resultados obtenidos y haciendo los cambios que sean necesarios.
4. Firma de los resultados por la Gerencia General

El principal responsable de utilizar esta herramienta y completar los datos fue el Gerente de TI, apoyado por sus jefes de área y otros miembros de la organización según lo requiera cada control. Por ejemplo, el Gerente de Recursos Humanos, el Gerente de Administración, entre otros.

Esta herramienta incluye una hoja de control de avance, la cual figura como primera hoja y tiene por objetivo facilitar las labores de seguimiento del progreso de desarrollo de la evaluación de riesgos. Esta hoja muestra cuantas respuestas se han completado por cada dominio de la norma ISO. Si existe algún error en la hoja de Control de Políticas, esta también se reflejara en esta área de progreso.

2.2.2 Area de Resultados:

Existen 3 hojas que permiten evaluar los resultados obtenidos en el llenado del ISSAQ. Se describe a continuación su significado y como deben ser interpretadas:

a) **Hoja de Resultado de Riesgos**

Es una lista de todos los riesgos de seguridad de la información que la organización plantea gestionar.

Los gráficos muestran de que forma los controles aplicados están mitigando los riesgos según las categorías definidas en esta hoja (hoja de categoría de riesgos o BRAP Category). Es importante resaltar que de todos los riesgos definidos y categorizados por la empresa, solo se están controlando bajo esta herramienta, aquellos relacionados a la seguridad de la información., por ejemplo, si se alcanza un puntaje de 100% en la categoría de riesgo legal, esto no quiere decir que la empresa no esté expuesta a ningún riesgo legal, sino que se tiene controlada la seguridad de información relacionada al riesgo legal.

b) **Hoja de Resultado de Políticas:**

Este gráfico resume el logro alcanzado en el cumplimiento de las políticas pero agrupadas por cada Dominio del ISO17799. Recuérdese que cada política está relacionada a uno de los 10 dominios del ISO.

c) **Hoja de Resultado detallado de Políticas:**

Esta hoja muestra el grado de cumplimiento alcanzado por dominios pero subdivididos por objetivos de control. Esto permitirá ver que políticas se están cumpliendo y cuales necesitan mas trabajo para ser cubiertas. Esta es una herramienta valiosa para el desarrollo de los planes de seguridad.

Las hojas de “Resultado de Riesgos” y “Resultado de Políticas” están semaforizados (Rojo, Amarillo y Verde) para facilitar su lectura e identificación de nivel de progreso.

A continuación se detalla la definición de cada estado:

- Rojo (Zona inaceptable): El % de los controles implementados es menor de 51%
- Amarillo (Zona en proceso): El % de los controles implementados se encuentra entre 51% y 85%
- Verde (Zona aceptable): El % de los controles implementados es mayor de 85%

2.3 Resultado del Análisis de Brecha

Realizados los cálculos se obtiene el siguiente gráfico en donde se puede observar las áreas que cumplen con las políticas de seguridad según la norma, las áreas que están en situaciones no aceptables y las áreas que son susceptibles de mejoras para pasar al estado aceptable.

En estado aceptable se encuentra la Política de Seguridad de Información de la Empresa, en estado que requieren mejoras se encuentran los capítulos de Seguridad Personal, Administración de Operaciones y Comunicaciones y el de Control de Acceso.

2.4 Planeamiento

Una vez que se completó el ISSAQ y se analizaron los resultados, se procedió a realizar planes de acción para controlar las brechas (gaps). Los resultados de la herramienta sirven para:

1. Establecer donde se encuentran las mayores brechas de seguridad.
2. Establecer que políticas de seguridad tienen los menores valores.
3. Establecer las prioridades por área para ejecutar los planes de seguridad.
4. Desarrollar el plan de las secciones priorizadas.
5. Definir actividades dentro de cada sección.

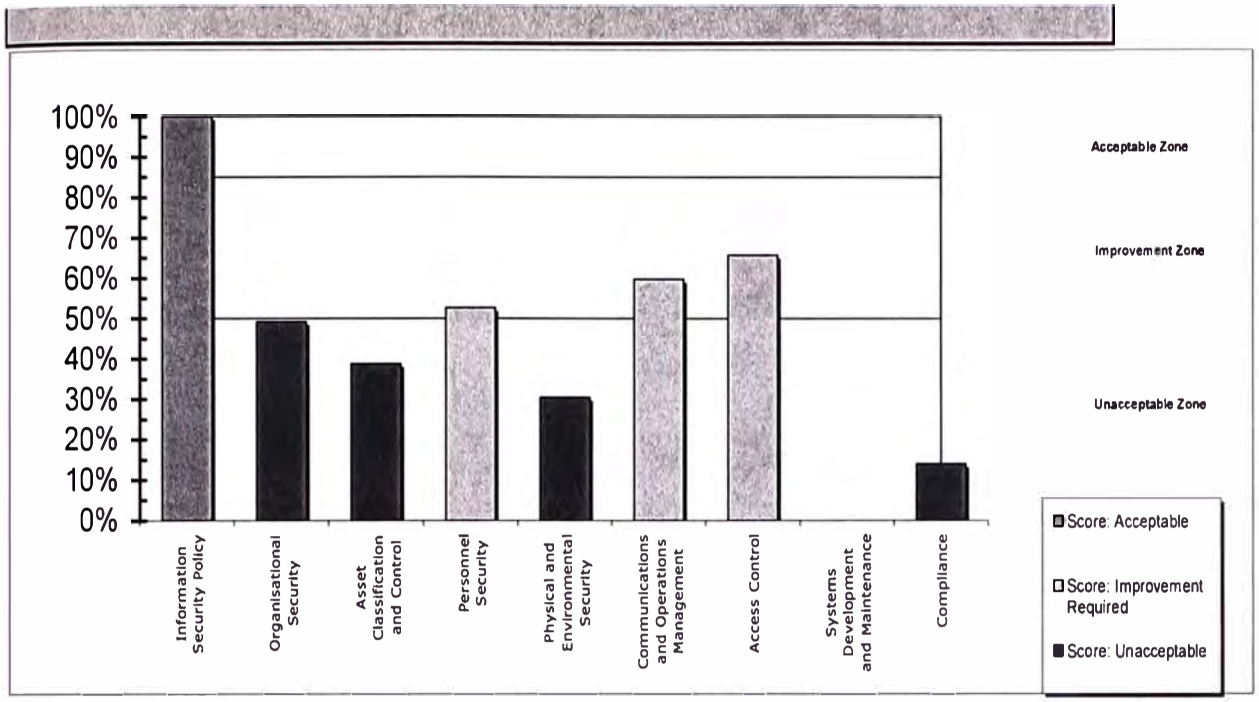

Figura 2.1: Resultados de Aplicación de la Herramienta para Evaluación de la Brecha de Seguridad

Tabla 2-1 Resultados de Aplicación de la Herramienta para Evaluación de la Brecha de Seguridad

(ISSAQ) : Policy Results

Country: PERU | **03-Mar-04**

	Policy Area	%		RATING
3	Information Security Policy	100%		Acceptable
4	Organisational Security	49%		Unacceptable - Compliance Risk
5	Asset Classification and Control	39%		Unacceptable - Compliance Risk
6	Personnel Security	53%		Improvement Required
7	Physical and Environmental Security	31%		Unacceptable - Compliance Risk
8	Communications and Operations Management	60%		Improvement Required
9	Access Control	66%		Improvement Required
10	Systems Development and Maintenance	0%		Unacceptable - Compliance Risk
12	Compliance	14%		Unacceptable - Compliance Risk
	OVERALL ASSESSMENT	43%		Unacceptable - Compliance Risk

2.5 Conclusiones y alcance.

- El uso de una herramienta para evaluar la brecha entre la norma y la situación de la empresa fue fundamental debido a lo extenso de la Norma. La herramienta nos permitió con suma facilidad y rapidez encontrar las áreas de la Norma con problemas potenciales y las áreas que podrían mejorarse inmediatamente.
- A través de la herramienta de Análisis de Brecha se pudo detectar los campos de aplicación de la norma que se encontraban en estado no aceptable y en estado para mejoras.
- La empresa decidió enfocarse en los capítulos que se encontraron para mejoras, capítulos de Seguridad de Personal, Administración de Operaciones y Comunicaciones y de Control de Acceso; lo cual hace que en forma rápida cuatro (4) de los diez (10) capítulos pasen a estado “aceptable”, mejorando las condiciones de seguridad de la información en la empresa.

CAPÍTULO III
APLICACIÓN DE LA NORMA

3.1 La empresa

ROYAL & SUNALLIANCE Seguros Fénix, Compañía de Seguros y Reaseguros, especializada en brindar seguros generales y de vida, con una facturación anual de US$ 30M. Subsidiaria de Royal & Sun Alliance UK. La empresa se fijo la meta de implementar una administración eficiente de la seguridad de la información que tenga como marco conceptual el estándar ISO 17799.

Al ser una empresa multinacional, las diferentes subsidiarias poseían diferentes normas y aplicaciones de seguridad en su plataforma informática por lo cual era muy difícil administrar y controlar la seguridad de la información en forma global.

En el Perú, ROYAL & SUNALLIANCE compró la empresa Seguros Fénix y adquirió sistemas y plataforma informática de diferentes proveedores, sin estándares, con tecnología antigua y sobre todo sin normas y procedimientos de seguridad.

Así mismo la empresa a nivel internacional había sufrido ataques de virus en subsidiarias, hackkers habían penetrado los sistemas contables y se tenía problemas de complejidad de las redes que administraban y volvía insegura la información de la empresa.

3.2 Situación de la redes en ROYAL & SUNALLIANCE Seguros Fénix.

A continuación se muestra la situación y problemas de seguridad en la plataforma informática en la empresa:

1. IBM AS/400

Equipo principal de la empresa de seguros generales. En este equipo se implementaban las aplicaciones "core" (principales) del negocio.

- Este computador tenía habilitado el puerto FTP.
- Los perfiles de usuarios no estaban definidos
- Los objetos de las base de datos estaban sin seguridad.
- Al 21 de enero de 2003 se habían cubierto 23 recomendaciones, avanzado 2 y 7 pendientes con lo cual se tenía un 72% de avance, con respecto a las seguridades de computador central. El detalle se muestra en el anexo 1.

2. IIS (Internet Information Server)

El IIS es el conjunto de servicios (FTP, SMTP, NNTP y HTTP/HTTPS así como los módulos de Microsoft -ASP Active Server Pages y ASP.NET-) que vienen integrados con los sistemas operativos de Microsoft, con el propósito de permitir poder utilizarlos como servidores Web, motivo por el cual su uso está mas su orientado a los MS Windows Servers.

3. Identificar laptops a ser encryptado.

Ninguna laptop que manejaba información confidencial estaba encriptado su password y su información.

4. Seguridad Perimetral

La empresa no poseía ningún Firewall estándar del mercado. Como consecuencia no había una DMZ no se tenía un diseño y configuración del perímetro.

La empresa estaba supeditada a accesos no autorizados o tráfico sospecho hacia la red interna de la organización.

Los equipos que brindaban conexión al exterior, casos de Web Server y accesos desde las clínicas y centros autorizados no estaban protegidos por el Firewall.

5. Antivirus.

La red de la empresa no poseía un software estándar de antivirus.

6. Spams

La empresa debido a su exposición mundial dado el rubro que se desempeña estaba constantemente atacada por troyanos, spams, programas espías y gusano.

7. Control de Acceso:

La empresa no contaba con políticas de acceso y password para los principales sistemas de información. El ingreso a la red no tenía estándares y mecanismos de monitoreo.

8. Filtrado en el Correo Electrónico.

La red del correo electrónico estaba "abierta" al ingreso de cualquier tipo de correo desde el exterior así como se permitía "salir" todo tipo de información a través del correo electrónico.

La red no poseía filtros, ni bloqueos para virus y spams.

A través de la red del correo electrónico no se podía bloquear correos obscenos y /o de carácter ofensivos.

9. Navegación Internet.

El rendimiento y tiempo de respuesta en el acceso de páginas Web dentro de la empresa era lento y no eficiente, las páginas mas visitadas y visitadas necesitaban rapidez y ser descongestionas del enlace Internet de la organización y proporcionar un

servicio de navegación mas rápido.

Todo empleado y funcionario que tenía acceso a Internet podía navegar sin restricciones comprometiendo la seguridad y productividad de la empresa.
No existía labores de auditoria y control a fin de evaluar los accesos y perdida de tiempo por parte del personal.

10. Monitoreo

No se tenía identificado que dispositivos de la red se debían monitorear.
Esto es sumamente importante para la empresa toda vez que los incidentes de seguridad y la recopilación de dicha información puede ser usada para decidir alguna acción legal dado el rubro que se encuentra la empresa.

11. Plan de continuidad del Negocio.

La empresa al estar en el rubro de seguros debía contar con un plan de continuidad del negocio exigido por las autoridades peruanas de la SBS y las autorizadas del grupo Royal de UK.
La empresa no contaba un plan integral de continuidad del negocio y por ende tampoco se había realizado prueba alguna de su funcionamiento, requisito indispensable para toda red de seguridad de la información.

12. Inventario de Hardware y Software

Finalmente la empresa no contaba con un inventario general de Hardware y Software.
No se contaba con una política de control de activos, así como de la adquisición de licencias de software.

3.3 Campos de Aplicación en la Empresa

Los capítulos escogidos para realizar las mejoras conllevan desarrollo e implementación de políticas de seguridad en el Hardware y Software de la empresa, los cuales se detallan a continuación.

Los capítulos restantes, están relacionados a procedimientos y políticas administrativas las cuales se señalan, no siendo parte del presente trabajo su desarrollo y descripción.

3.4 Aplicación en la Infraestructura de Hardware

3.4.1 Infraestructura de Hardware de la Empresa.

La infraestructura de la empresa esta compuesta por una serie de componentes, los cuales se encuentran dispuestos de acuerdo a las normas de seguridad según el gráfico adjunto.

Los componentes de de la infraestructura son:

a) Acceso a Internet:
b) Acceso de Usuarios Remotos a través de Infovía.
c) Acceso de Usuarios de Sucursales a través de Speedy WAN.
d) Red Interna de Servidores y usuarios internos de la Empresa.

a) Acceso a Internet:

Los usuarios de la empresa pueden comunicarse a Internet de acuerdo a las políticas de seguridad a través del Router CISCO 2611 y un enlace de 128Kbps a InfoInternet de TdP. Dicho router esta aislado de la red interna a través del Firewall One de Check Point.

b) Acceso de Usuarios Remotos a través de Infovía.

Los usuarios remotos pueden conectarse de acuerdo a las políticas de seguridad a través del Router CISCO 2610 y un enlace de 512Kbps a Infovia de TdP. El router está asignado a la DMZ Privada a fin de cumplir con las normas de seguridad de interconexión.

La DMZ (zona desmilitarizada por sus siglas) es el conjunto de servidores que se encuentra entre la red de computadoras interior de la organización y la red de computadoras del exterior, principalmente Internet. Esta separación fue implementada a través del Firewall de Checkpoint y permitió que los servidores Antivirus, Gateway de correo y Web interiores interactúen con el exterior mientras se protege la red interior de accesos no autorizados.

c) Acceso de Usuarios de Sucursales.

Los usuarios de sucursales pueden conectarse de acuerdo a las políticas de seguridad a través del Router ADSL y un enlace de 256Kbps a la red Speedy de TdP. En cada sucursal se implementó un router ADSL para la conexión respectiva a Speedy de TdP. El router esta asignado a la DMZ Privada a fin de cumplir con las normas de seguridad de interconexión.

El ADSL (Asymmetric Digital Suscribe Line o Línea de Cliente Digital Asimétrica) es una tecnología de transmisión que permite a los hilos de cobre convencionales, usados inicialmente para telefonía, transmitir datos a alta velocidad, lo cual le da una gran ventaja en velocidad y economía en comparación con las limitaciones que presentan líneas de transmisión de datos convencionales bajo MODEM y RDSI (Red Digital de Servicios Integrados), las cuales pasaron a formar parte de los enlaces de contingencia.

El servicio ADSL fue contratado a Telefónica del Perú quien además proporcionó en calidad de alquiler los ruteadores ADSL en la Oficina Principal de Comandante Espinar y en la red de Agencias a nivel nacional.

Para los casos descritos el RADIUS presenta la siguiente configuración NAT:

Tabla 3-1 : Configuración NAT de la Empresa

NAT RADIUS		
NAT INTERNET	200.60.123.XX	
NAT INFOVIA	192.168.10.XX	
NAT INTERNO	10.141.192.XX	

El RADIUS (acrónimo en inglés de Remote Access Dial-In User Server) es un protocolo de autentificación, autorización y contabilización para aplicaciones de acceso a la red.

El servidor RADIUS fue utilizado para la autenticación de los enlaces de transmisión de datos de las agencias de Piura, Iquitos y Huancayo, puesto que se conectaban a la oficina principal a través del servicio INFOVIA.

La forma como trabaja el servidor RADIUS para dar acceso a las agencias es la siguiente: Cuando la agencia realiza la conexión con el ISP (Internet Service Provider, en este caso Telefónica del Perú) mediante módem (INFOVIA) se envía un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Servidor de Acceso a la Red) sobre el protocolo PPP, quien redirige la petición al servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autentificación como PAP, CHAP o EAP. Si es aceptado, el servidor autoriza el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características mas importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos. Esta información era utilizada a menudo para monitorear los enlaces y contabilizar mensualmente los periodos de conexión de las agencias con la Oficina Principal. Cuando inicialmente todas las agencias se conectaban a través de INFOVIA, la información de contabilidad del RADIUS fue utilizada como base para sustentar la migración de aquellos enlaces que hacían mas uso del servicio hacia la red Speedy WAN.

El RADIUS fue implementado en una PC dedicada ubicada en el centro de cómputo corriendo el sistema operativo Linux RedHad.

El NAT (Network Address Translation - Traducción de Dirección de Red) es un estándar que utiliza una o más direcciones IP para conectar varios computadores a otra red (normalmente a Internet), los cuales tiene una dirección IP completamente distinta (normalmente una IP no válida de Internet definida por el RFC 1918). También es utilizado para dar salida a redes públicas a computadores que se encuentran con direccionamiento privado o para proteger máquinas públicas.
En el cuadro de direcciones NAT mostrado mas arriba se observa el rango de direcciones configuradas en el Firewall Checkpoint utilizados para las translaciones NAT.

d) Red interna de Servidores y usuarios internos de la empresa:

La red interna de servidores de la empresa esta compuesta por servidores:

- **Servidor IBM RS6000 modelo S40**
  Computador principal donde corren las aplicaciones de producción de la Compañía de Seguros de Vida y Rentas Vitalicias.

- **Servidor IBM RS6000 modelo S10**
  Computador de desarrollo y contingencia de la Compañía de Seguros de Vida y Rentas Vitalicias. Este computador se ubica en el COT de GMD conforme el DRP (Disaster Recovery Plan/Plan de Recuperación de Desastre) de la empresa y conectado a la Oficina Principal mediante un enlace dedicado contratado con Telefónica del Perú.

- **Servidor IBM AS400 modelo 820**
  Computador principal donde corren las aplicaciones de producción de la Compañía de Seguros Generales.

- **Servidor IBM AS400 modelo 620**
  Computador de desarrollo y contingencia de la Compañía de Seguros Generales. Este computador se ubica en el COT de GMD conforme el DRP (Disaster Recovery Plan/Plan de Recuperación de Desastre) de la empresa y conectado a la Oficina Principal mediante un enlace dedicado contratado con Telefónica del Perú.

- **Servidor Terminal Server**
  El servicio de "Terminal Services" es lo opuesto a Cliente/Servidor, puesto que es una solución de procesamiento centralizado, en la cual todo el procesamiento se realiza

en el servidor y las estaciones que se conectan solo reciben las pantallas a manera de terminales tontas.

Si bien el servicio de "Terminal Services" viene integrado en el sistema operativo Windows Server de Microsoft, esta es limitada, motivo por el cual la empresa decidió utilizar la solución de la empresa CITRIX Metaframe.

El Terminal Services implementado en el Servidor CITRIX fue una gran solución para las Agencias remotas a nivel nacional, puesto que ofreció los siguientes beneficios:

- ✓ Mejoró el tiempo de respuesta de las aplicaciones Cliente/Servidor desarrolladas en PowerBuilder y que interactuaban con la base de datos SQL de Microsoft. Esto se logró gracias a que el volumen de información ya no era transferido del servidor en Lima a las estaciones cliente en provincias para su procesamiento, sino tan solo las pantallas con los resultados, ya que el procesamiento se realizaba en el propio servidor CITRIX.
- ✓ Solucionó las caídas de las sesiones de emulación al AS/400, truncas por cortes en los enlaces. Cuando había un microcorte en el enlace las sesiones de emulación no las percibían y si el corte se prolongaba, las Agencias retomaban sus sesiones donde las dejaron al momento de conectarse nuevamente a la oficina principal. Esto gracias a que ahora las sesiones de emulación corrían localmente sobre el servidor CITRIX y ya no en las estaciones remotas de las agencias.
- ✓ Facilitó los servicios de soporte remoto a las agencias, puesto que permite capturar y controlar las pantallas de las agencias para resolver problemas operativos o realizar labores de capacitación.

- **Servidor Lotus Domino (eMail)**

  El Sistema de mensajería bajo Lotus Notes fue el estándar establecido en toda la organización a nivel mundial, por su seguridad, herramientas incorporadas, facilidad de uso y administración.

  Una de las características que incluye el Lotus Notes y que la diferencia del resto de soluciones de mensajería, es su capacidad de desarrollo de aplicaciones en una diversidad de lenguajes de programación (Lotus Script, Funciones y Java Script) que al integrarse con los servicios de mensajería permite implementar soluciones de

Workflow de manera muy fácil y rápida. Estas aplicaciones pueden trabajar en modo Cliente Notes o en Web desde cualquier navegador Internet.

La empresa supo aprovechar esta solución de Lotus Notes para mensajería, desarrollo de Intranet departamentales y aplicaciones de Workflow para la gestión y control de flujos documentarios integrados al sistema AS/400.

- **Servidor Lotus Sametime (Mensajería instantánea –Chat-)**
  Este servicio implementado redujo costos de comunicación "on-line" con el resto de Oficinas del Grupo a Nivel Regional, puesto que a diferencia del email, este medio de comunicación es en tiempo real y ayudó a realizar charlas y conferencias sin necesidad de viajar o realizar costosas llamadas telefónicas.
  Este sistema también reducía la carga de archivos del servidor de correos, al ser reemplazados por comunicaciones Chat.

- **Servidor MS Windows Server**
  Utilizado como Servidor de Archivos e impresión. En este servidor se almacenan los datos de los usuarios en sus respectivas carpetas personales. Asimismo, se utiliza como servidor de backup para los fuentes y objetos de las aplicaciones Cliente/Servidor desarrollados bajo PowerBuilder.
- **Servidor WEB Interno**
  Este servidor brinda los servicios de información de los asegurados y su siniestralidad a las áreas de Call Center y Asistencia Médica.

- **Servidor WEB Externo**
  Este servidor brinda servicios de información a los Clientes (datos del asegurado y siniestralidad) y Brokers (cartera de Clientes y siniestralidad)

- **Servidor TEN**
  Este servidor es utilizado como plataforma de comunicación con las Clínicas, las cuales a través de un módulo cliente consultaban los datos del asegurado, cobertura, % de coaseguro y su estado de cuenta cada vez que una persona solicitaba servicio por el seguro.

- **Servidor MS SQL**

  Servidor de base de datos de Microsoft, el cual era utilizado por las aplicaciones Cliente/Servidor en PowerBuilder.

  El MS SQL Server se seleccionó como plataforma estándar para el desarrollo del Datawarehouse del Grupo a nivel regional. Para la explotación de datos (Data Mining) se utilizó la herramienta Cristal Reports.

  El MS SQL se montó sobre un servidor IBM xSeries con doble procesador Xeon y 2 Gb de memoria RAM.

- **Servidor Proxy**
- **Usuarios internos.**

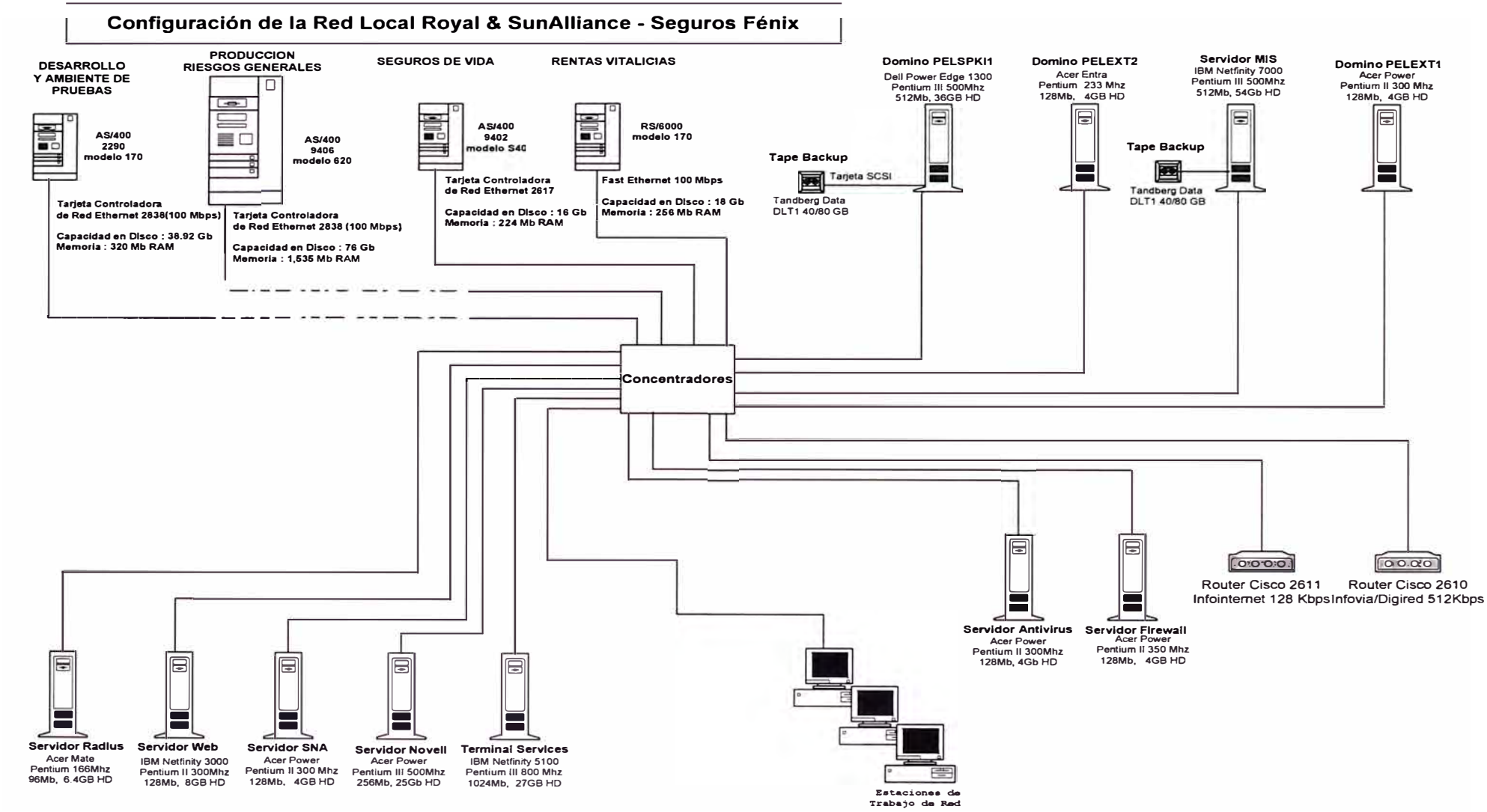

Figura 3.1: Configuración de la Red Local de la Empresa

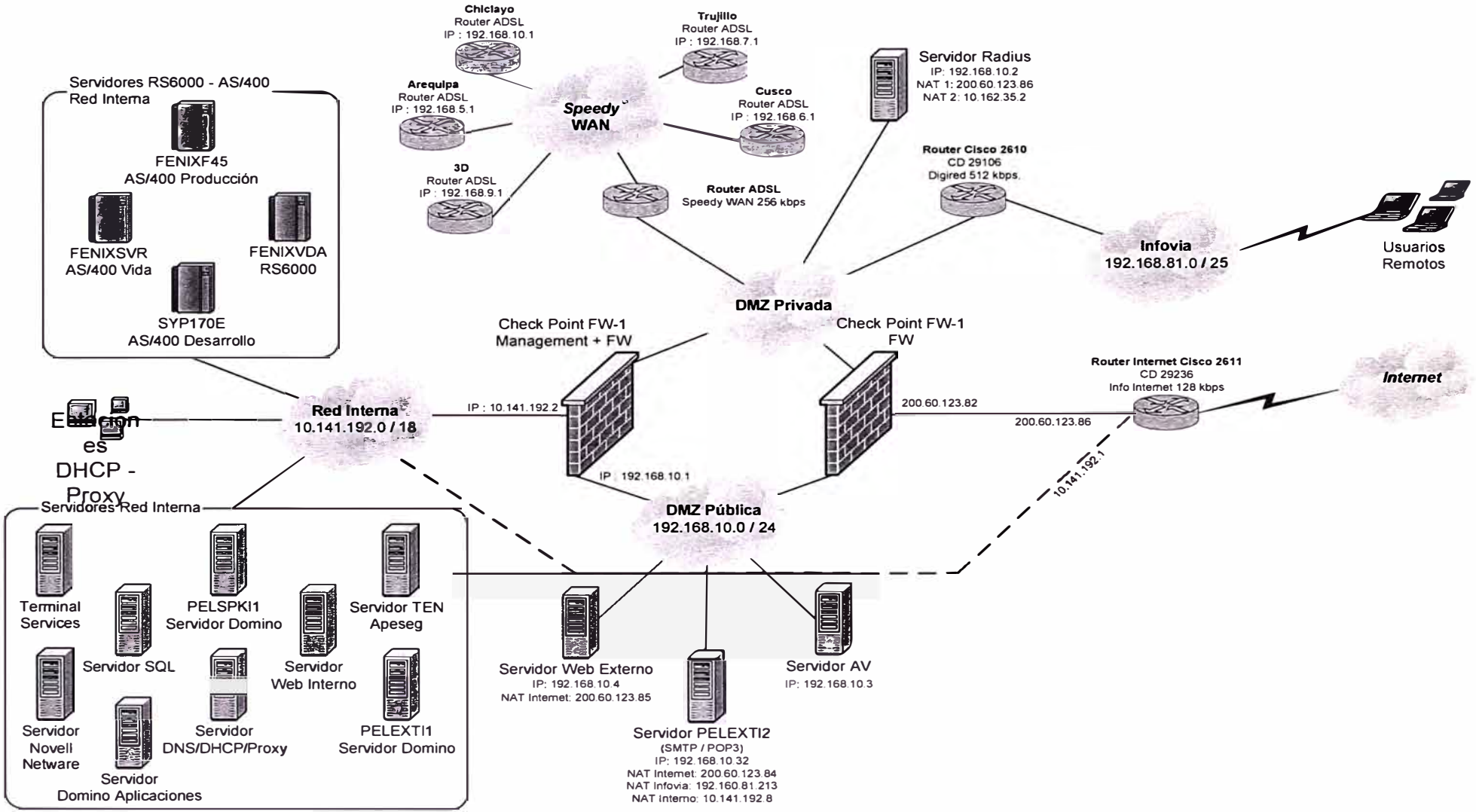

Figura 3.2: Infraestructura de Seguridad de Hardware y Software de la Empresa

3.4.2 Seguridad en la Infraestructura de Hardware de la Empresa.

Se implementó los niveles de seguridad en todo el hardware de la empresa. Los aspectos que se consideraron fueron la configuración y parches de todos los servidores, la encriptación de laptops, y la implementación de la seguridad perimetral a través de la adquisición de los Firewalls respectivos y su incorporación a las definiciones de seguridad.

Tabla 3.2: Acciones de Seguridad en el Hardware

I. Configuración y Parches (Implementación de los estándares de configuración en los principales sistemas operativos)
1. IBM AS/400. Un IBM AS/400 (denominado ahora como iSeries) modelo 820 es el computador principal de la empresa de seguros generales. En este equipo se implementaban las aplicaciones "core" del negocio. Las políticas de seguridad aplicadas al sistema operativo OS/400 de este equipo fueron agrupadas en : a) Configuración básica de seguridad b) FTP c) Acceso a autorizaciones especiales d) Perfiles de usuario e) Autorización sobre objetos f) Continuidad y disponibilidad g) Misceláneas
2. IIS (Internet Information Server) Se definieron 21 controles de seguridad para el IIS. El IIS es el conjunto de servicios (FTP, SMTP, NNTP y HTTP/HTTPS así como los módulos de Microsoft -ASP Active Server Pages y ASP.NET-) que vienen integrados con los sistemas operativos de Microsoft, con el propósito de permitir poder utilizarlos como servidores Web, motivo por el cual su uso está mas su orientado a los MS Windows Server, puesto que las versiones Cliente de MS Windows XP vienen con una versión limitada del IIS. Los controles fueron aplicados sobre el Servidor Web transaccional ubicado en la DMZ de la empresa como en el Hosting de páginas estáticas contratado con la empresa QNet.

3. Security Expressions para MS Windows

Con la finalidad de asegurar la aplicación automática de las políticas de seguridad sobre la plataforma de servidores MS Windows Server y poder gestionarlas y auditarlas fácilmente de forma centralizada, es que se seleccionó el software Security Expressions de la empresa Pedestal. Se aplicó el software en toda la plataforma Windows.

4. Unix (Genérico)

Se aplicaron 21 controles de seguridad al sistema operativo AIX del equipo IBM RS/6000, el cual daba servicio a la empresa de seguros de Vida.

5. CISCO Routers

El estándar de equipamiento de comunicaciones WAN para la empresa fue los ruteadores CISCO. Estos ruteadores son los encargados de la conexión a Internet y Casa Matriz.

Los controles de seguridad aplicados fueron sobre el sistema operativo de estos equipos, los cuales fueron llevados a cabo de forma remota por la propia casa matriz. El principal control fue la actualización a la última versión del sistema operativo de dichos Routers.

II. Encriptación de Laptops

1. Identificar laptops a ser encryptado con Safeboot

Con la finalidad de proteger la información sensible y confidencial de la organización almacenada en equipos portátiles, por su alto riesgo de ser extraviados o sustraídos, es que se seleccionó el software Safeboot de la empresa del mismo nombre para la autentificación de Pre-Booteo de dos factores. La autenticación de Pre-booteo se refiere a que esta autenticación se realiza sobre el usuario y la máquina antes del arranque del sistema. Además provee de las herramientas necesarias para establecer y/o forzar la utilización de políticas de password rigurosas.

El doble factor de autenticación pre-boot, se refiere a que el usuario debe "saber algo" y "tener algo" para que SafeBoot permita arrancar a la PC portátil.

2. Se revisaron los procedimientos de configuración de W2k/XP encryption

3. Se instaló la consola para Safeboot

4. Se implementó el sistema de encriptación de archivos (EFS) en laptops acordadas.

Para reforzar la seguridad de acceso a la información sensible y confidencial almacenada en equipos portátiles, se decidió activar las funciones EFS de los sistemas operativos MS Windows 2000 de las laptops. El Sistema de Archivos Encriptado (Encrypted File System - EFS) proporciona la tecnología principal de encriptación para almacenar archivos del sistema NTFS de Windows NT de forma cifrada en el disco. Con esta medida se pretende resolver las preocupaciones de seguridad que surgen en relación con herramientas disponibles que permiten acceder a archivos desde un volumen NTFS sin una verificación de acceso, puesto que los encontrarán cifrados. Esta solución no afecta al real usuario, puesto que una vez autenticado el uso de sus archivos es transparente.

5. Se procedió a confirmar que no hay problemas operacionales con EFS

6. Se establecieron Políticas formales de Encriptación para las laptops que se incorporan a la empresa.

III. Seguridad PERIMETRAL

1. Migrar firewalls a Nokia / Checkpoint

Se estableció como estándar dentro de la organización la utilización del firewall One de la empresa Checkpoint, con la intención de impedir el acceso no autorizado que pueda ser originado desde Internet a la red local de la empresa. Los pasos que se siguieron para su implementación fueron los siguientes:

1.1. Diseño técnico

1.2. Compra de H-W y S-W

1.3 Configuración y instalación del consola

1.4 Reconfiguración del DMZ (Privado, publico, interno)

1.5 Comprobar la configuración

1.6 Implementación

1.7 Tunning

2. IDS

Se estableció el requerimiento de implementación de un "Sistema de Detección de Intrusos", conocido en sus siglas en inglés como IDS, el cual tiene por objetivo identificar accesos no autorizados o tráfico sospechoso hacia la red interna de la

organización.

3. Implementación de software SNORT

La solución de IDS seleccionada e implementada fue el SNORT. El Sistema de Detección de Intrusos (IDS por sus siglas en ingles), sirve para detectar los ataques a la red informática de la empresa. A través de dicha herramienta se monitorea los puertos que están siendo atacados a fin de prevenir dichos ataques.

4. Routeadores del Perímetro

Se identificaron y evaluaron los ruteadores CISCO que permitían la interacción de la empresa con el exterior, con la finalidad de garantizar cubran los requerimientos de seguridad de la organización.

4.1 Localizar los links existentes

4.2 Racionalizar los links existentes

4.3 Comprobar configuración

5. Conexiones a Terceros

5.1 Identificar Conexiones

5.2 Mudar cada conexión atrás del Router/FW

Se determinó que todo equipo que brinde servicio al exterior, deberá estar siempre detrás de una protección de firewall.

3.5 Aplicación en la Infraestructura de Software

Se implementó las normas de seguridad a través de los diferentes componentes de Software que se adquirió e instaló. Los principales componentes de seguridad fueron el Antivirus, las políticas de control de acceso en los servidores, la implementación de seguridades en el correo electrónico, las normas de navegación de Internet y los controles de monitoreo de la red de la empresa.

Tabla 3.3 Acciones de Seguridad en el Software de la Empresa

I. Anti-Virus
1. Implementar EPO En conjunto con el software antivirus VirusScan, se seleccionó la solución ePolicy Orchestrator de McAfee para gestionar, mantener actualizada, configurar, auditar y distribuir de forma centralizada y automatizada el software antivirus de McAfee en todos los computadores personales y servidores MS Windows de la organización. Esta herramienta se empleó para la generación de reportes de control de incidentes de seguridad por virus informáticos a Casa Matriz.
2. Se aseguró continuamente que el Antivirus esta siendo distribuido a todos servidores y PCs
3. Se implementó el Software Sophos en el puerto SMTP Como parte de la política de robustecimiento de la infraestructura de seguridad de la organización (hardening) se consideró la implementación de un dispositivo de hardware (appliance) aplicado para los servidores SMTP Gateways hacia Internet para la protección de mensajes entrantes y salientes contra virus, programas espía, troyanos y gusanos. Además de permitir la detección de correo spam y protección contra engaños y ataques de captura de información por email. Esta solución trabajaría de forma complementaria al McAfee, trabajando anticipadamente antes de que lleguen los correos a los servidores de email y clientes de Lotus Notes. Asimismo, evitando el uso del servidor gateway SMTP como spam.
4. Se aseguró que estén siendo reportados los incidentes de Virus.

5. Se Implementó procesos para monitorear los reportes EPO

II. Control de Acceso

1. Actualizar Políticas

1.1. Actualizar parámetros de los sistemas:

a) Midrange (AS/400, Unix etc.)

b) Servidores/Redes

1.2 Publicar políticas para usuarios:

a) Nuevas definiciones

b) Política de un buen password

2. Establecer procedimientos/chequeos de administradores

3. Establecer mecanismos de monitoreo

III. Filtrado

1. Email

1.1 MailSweeper

Como complemento a las medidas de seguridad aplicadas a los correos electrónicos bajo Lotus Notes, se aplicó una seguridad de segunda capa sobre el servidor Internet gateway de correos, mediante la instalación del software MailSweeper, el cual analiza los emails de entrada y salida sobre este servidor para bloquear el spam, virus, contenido inapropiado y cumplir con las políticas de seguridad de la empresa.

a) Identificar servidor para MailSweeper

b) Comunicar filtros al personal

c) Instalar MailSweep

d) Revisar operaciones para manejar mail bloqueado

e) Implementar configuración estándar del Grupo

f) Activar MailSweep

g) Definir Reglas para MailSweeper para Spanish/Portuguese

h) Implementar y Probar Reglas Spanish/Portuguese Rules

i) Definir y acordar procedimientos operacionales y niveles de servicio

1.2 Watchdog

Se seleccionó el software Watchdog como solución de filtro para el sistema de mensajería Lotus Notes, el cual permitió bloquear mensajes de correo por su contenido (mensajes obscenos, raciales, ofensivos, etc.) y/o anexos adjuntos no

autorizados (.EXE, .COM, .VBS, entre otros)

a) Revisar procedimientos operacionales para manejar mail bloqueado

b) Implementar Configuración estándar del Grupo

c) Activar Watchdog

2. Navegación Internet

2.1 Web (Proxy & Content Filter)

a) Construir ISA Proxy

Se seleccionó la solución ISA Proxy de Microsoft principalmente para mejorar el rendimiento y tiempo de respuesta en el acceso de páginas Web dentro de la empresa, puesto que las páginas mas visitadas y visitadas recientemente son almacenadas en memoria cache con la intención evitar conexiones externas innecesarias, descongestionar el enlace Internet de la organización y proporcionar un servicio de navegación mas rápido.

Si bien el ISA Proxy también ofrece servicios de seguridad de acceso y contenido, debido a que son limitados, se decidió utilizar para este propósito herramientas especializadas y robustas.

2.2 Instalar SurfControl

El software SurfControl ayuda a detener el contenido no deseado de los servicios de navegación dentro de la empresa de acuerdo a la política de seguridad definida. Asimismo, mediante esta herramienta se implementó los diferentes tipos y niveles de restricciones de acceso a páginas Internet y sistemas de correo Webmail (Hotmail, Yahoo, etc.) para los empleados, reduciendo significativamente los riesgos a la seguridad y productividad.

Se empleó esta herramienta también para las labores de auditoria y control, remitiéndose mensualmente reportes estadísticos y de control de sites visitados y bloqueados.

2.3 Asegurar que el servidor esta configurado, realizar un scaneo de vulnerabilidades

2.4 Confirmar que esta funcionando bien

2.5 Revisar procedimientos para manejar sitios bloqueados

2.6 Comunicar filtros al personal

2.7 Migrar usuarios hacia el nuevo Proxy

IV. Monitoring, Logging

1. Identificación de dispositivos para monitorear

2. Instalación de agentes de monitoreo en Servidores

Para efecto de llevar a cabo las labores de control y monitoreo en el cumplimiento de las políticas de seguridad, se procedió a instalar un software que corre como un agente en los servidores seleccionados. Si bien las tareas de monitoreo pueden ser realizadas dentro de cada organización, el control se realiza de forma centralizada mediante una consola de monitoreo en UK ubicada en Corporate Centre, allí se seguirán los eventos de los respectivos servidores.

Se muestra a continuación una pantalla de del software de monitoreo, en la cual se puede observar mediante semáforos las alarmas respectivas para cada país de la organización R&SA:

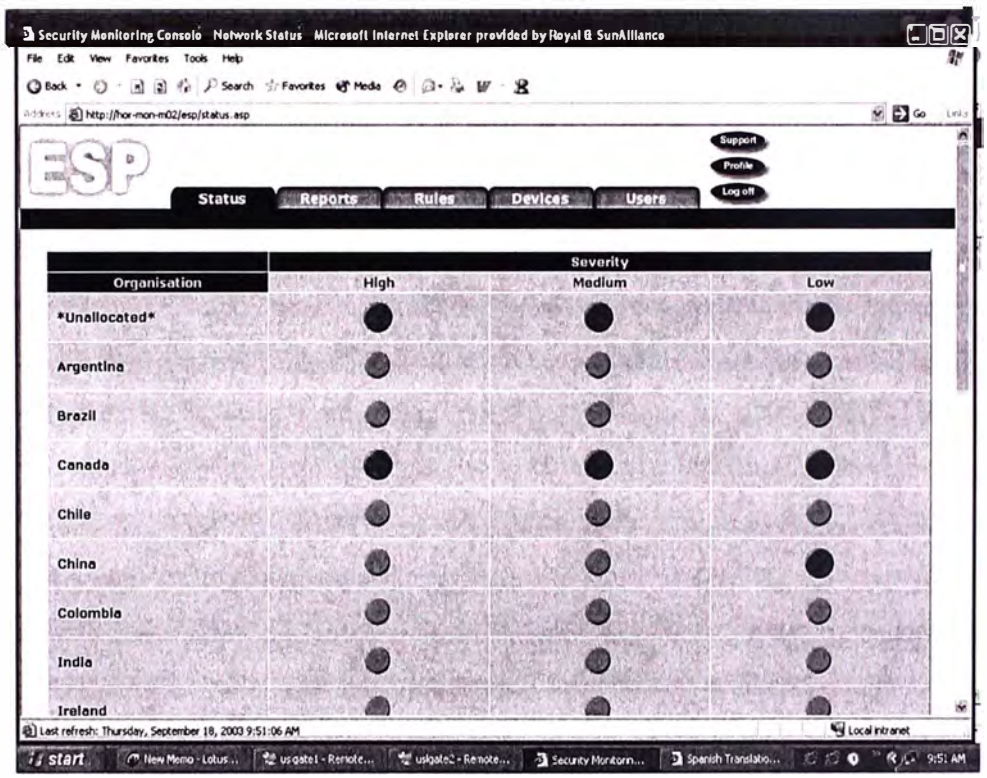

Figura 3.3: Semáforos de Alarmas de Monitoreo

3.6 Seguridad Normativa

Finalmente como señalamos en el capitulo de la aplicabilidad de la Norma, se describe las acciones de carácter administrativo que se llevaron a cabo en los ámbitos de manejo de incidentes, implementación del Plan de continuidad del Negocio, acciones para enfrentar las normas legales, difusión y administración de inventario.

Tabla 3.4: Aplicaciones Normativas

I. Manejo de Incidentes
Uno de los sub-proyectos de seguridad es el Manejo de Incidentes, cuyo objetivo se centra en la contención y eliminación de los incidentes de seguridad y en evitar la repetición de los mismos. Asimismo, la información recopilada puede ser utilizada como evidencia forense para cualquier acción legal que la empresa pueda decidir emprender. Para el manejo de incidentes se desarrollaron procedimientos de registro y seguimiento así como responsables en su seguimiento y reporte a Casa Matriz, los cuales se muestran en el diagrama adjunto.

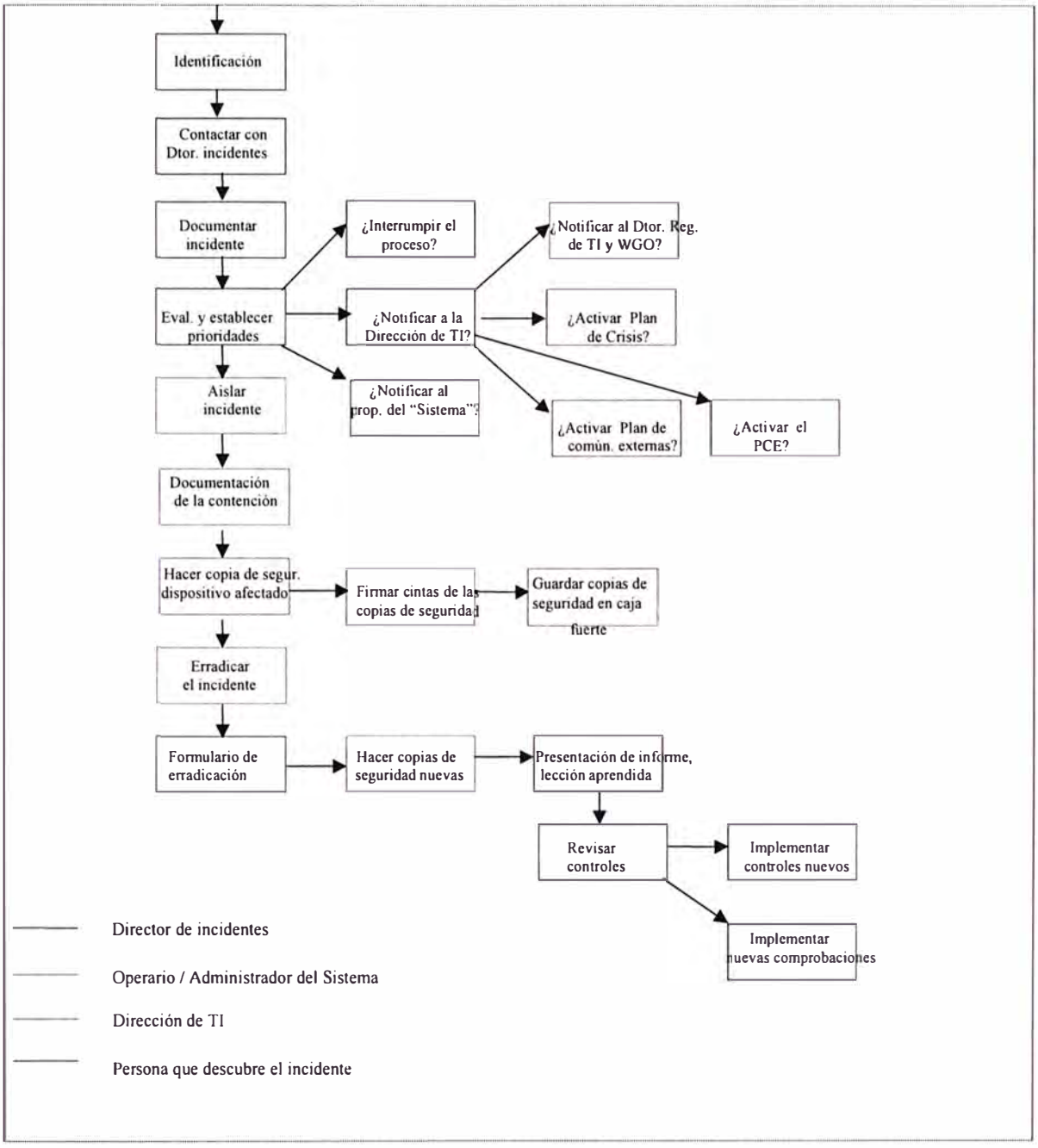

Fig. 3.1: Procedimientos de Seguridad

II. BCP (Plan de Continuidad del Negocio)

Para el desarrollo del BCP, el área de TI desarrolló su DRP (Disaster Recovery Plan) firmando un contrato con la empresa GMD para la implementación de su lugar alterno de procesamiento en el COT (Centro de Operaciones Tecnológicas) de dicha empresa, la cual se interconectó a través de un enlace dedicado proporcionado por Telefónica del Perú.

Como parte del plan de contingencia se realizaron pruebas y simulaciones de escenarios de desastre.

En el diagrama, se muestra a manera de resumen la cronología de gestión de desastres conforme el Plan de Contingencia del área de TI.

Diagrama 3.2: Gestión del Plan de Contingencia.

Secuencia	Conocimiento de emergencia	Declaración de Crisis IT	Gestión de Crisis IT	Gestión de restablecimiento IT	Gestión de Operación IT	Gestión de restitución IT	Gestión de puesta en marcha en local propio
Responsables	Cualquier empleado de la empresa	Gerente IT	Area de Producción	Area de Producción y Desarrollo IT	Area de Producción y Desarrollo IT	Gerente IT	Area de Producción
Duración	Inmediata	15 minutos	2 horas	14 horas	30 días	30 días	30 días

Los pasos seguidos en el desarrollo del proyecto fueron:

1. Comparar BCP contra la plantilla
2. Actualizar BCP IT Plan haciendo análisis de "gaps"
3. Planificar pruebas
4. Realizar las pruebas
5. Actualizar el plan BCP IT
6. Establecer planes para futuros pruebas y revisiones

III. Legal
1. Asegurar que todas las copias de contratos de TI está disponibles Se cruzó el inventario de contratos de TI existentes contra los documentos físicos, formalizando aquellos que estaban pendientes o inexistentes. Se definieron requerimientos mínimos de seguridad que deben incluir todos los contratos firmados por la empresa, los cuales fueron agregados a través de cláusulas de confidencialidad, acuerdos de nivel de servicio y penalidades.
2. Asegurar que todas las copias de contratos de terceros están disponibles
3. Establecer Prioridad de contratos
4. Ganar acuerdo con las contratantes para los cambios
5. Asegurar que consultores firmaron cláusulas de confidencialidad

VIII. Difusión
1. Presentaciones a los gerentes/personal.
2. Artículos en revistas/intranets de la compañía
3. Apoyo de iniciativas centrales
4. Implementación de e-learning

XIII. Administración de Inventarios
1. Inventario de Hardware
1.1. Se dispuso y aseguró el inventario de hardware actualizado Se desarrolló un sistema de control y gestión de inventario de hardware bajo Lotus Notes, el cual registra los equipos y su configuración de toda la empresa. Este sistema está enlazado al sistema de inventario de software.
1.2. Definición de política de adquisición de activos
1.3. Definición de política de control de activos nuevos y usados
1.4. Definición de políticas de ventas, baja y destrucción
2. Inventario de Software
2.1. Disponer y asegurar el inventario de software actualizado Se desarrolló un sistema de control y gestión de inventario de software bajo Lotus Notes, el cual permite identificar rápidamente el software instalado en cada equipo como el número total de licencias utilizadas en toda la organización.
2.2. Definición de política de adquisición de software y licencias Se definieron políticas de adquisición de software y gestión de licencias según los controles recomendados por la norma ISO 17799.
2.3. Definición de política de desincorporación de software

3.7 Políticas de Seguridad Implementadas

La empresa a través del comité de seguridad del grupo definió las políticas de seguridad para toda la infraestructura tecnológica según las recomendaciones de la norma ISO 17799, pero sin aspirar una certificación a corto plazo según la BS 7799.

Lo que se proyectó a corto plazo fue la certificación de su personal según la CISSP (Certified Information Systems Security Professional) que ofrece la $(ISC)^2$ (The internacional Information Systems Security Certification Consortium) con el propósito de asegurar la continuidad y calidad de este proyecto en el tiempo.

Tabla 3.5: Políticas de seguridad definidas

RSA-ISO-300-001-Política de Documentación del Programa de Seguridad de Información
RSA-ISO-311-001-Política de Seguridad de Información Total del Grupo
RSA-ISO-414-001-Política de Autorización de Facilidades del Procesamiento de Información
RSA-ISO-416-001-Cooperación entre Política de Organizaciones
RSA-ISO-430-001-Política para Fuentes Externas
RSA-ISO-511-001-Política de Manejo del Capital
RSA-ISO-521-001-Política de Clasificación de Información
RSA-ISO-600-001-Política de Filtración del Representante para Internet
RSA-ISO-600-002-Política de Filtración de E-mail
RSA-ISO-600-003-Política de Internet para Uso Aceptable
RSA-ISO-600-004-Política de E-mail para Uso Aceptable
RSA-ISO-600-006-Política Gerencial de Incidente de Seguridad
RSA-ISO-612-001Política de Protección de Personal
RSA-ISO-614-001-Política de Condiciones y Términos de Empleo
RSA-ISO-635-001-Política de Proceso Disciplinario
RSA-ISO-710-001-Política de Seguridad de Acceso Físico
RSA-ISO-720-001-Política para Equipo de Seguridad
RSA-ISO-723-001-Política de Seguridad Cableado
RSA-ISO-724-001-Política de Mantenimiento del Equipo
RSA-ISO-725-001-Política de Seguridad de Medios de Comunicación en Tránsito
RSA-ISO-726-001-Política para Desecho de Medios
RSA-ISO-730-001-Política de Manejo de Datos
RSA-ISO-800-002-Política de Redes Inalámbricas
RSA-ISO-800-003-Política de Solidez
RSA-ISO-800-004-Política de Corrección
RSA-ISO-800-005-Política Anti-Virus
RSA-ISO-800-007-Política de Seguridad de Firewall
RSA-ISO-800-008-Política de Seguridad para Conexión y Ruteo
RSA-ISO-800-009-Política de Sistemas de Detección de Intrusos
RSA-ISO-800-010-Política de Seguridad de Modem
RSA-ISO-800-012-Política de Seguridad para Inalámbrico
RSA-ISO-800-025-Política de Planeación de Capacidad Operacional
RSA-ISO-800-026-Política de Control de Cambio Operacional

RSA-ISO-800-027-Política de Limpieza Operacional
RSA-ISO-800-028-Política de Procedimientos Operacionales
RSA-ISO-800-029-Política de Segregación de Deberes Operacionales
RSA-ISO-800-030-Política de Aceptación del Sistema
RSA-ISO-800-041-Política de Aceptación del Sistema
RSA-ISO-851-001-Política de Tecnologías Emergentes
RSA-ISO-851-002-Política de Controles de Red
RSA-ISO-864-001-Política de Seguridad de Documentación del Sistema
RSA-ISO-871-001-Política de Acuerdos de Intercambio de Software e Información
RSA-ISO-875-001-Política de Seguridad de Sistemas de Oficina Electrónicos
RSA-ISO-876-001-Política de Sistemas Disponibles Públicamente
RSA-ISO-877-001-Política de Intercambio de otras formas de Información
RSA-ISO-910-001-Política de Control de Acceso – Acceso de Usuario
RSA-ISO-932-001-Política de Equipo de no vigilado por el Usuario
RSA-ISO-942-001-Política de Vía con Vigor
RSA-ISO-951-001-Política de Identificación de Terminal Automática
RSA-ISO-952-001-Política de Encendido de la Terminal
RSA-ISO-956-001-Alarma de Coacción para Salvaguardar Política del Usuario
RSA-ISO-962-001-Política de Aislamiento de Sistema Sensible
RSA-ISO-970-001-Política de Registro y Monitoreo
RSA-ISO-981-001-Política de Seguridad de Acceso Remoto
RSA-ISO-981-002-Política de Seguridad de Artefactos Manuales
RSA-ISO-1000-001-Política PKI (Infraestructura para Clave Pública)
RSA-ISO-1000-002-Política de Seguridad de Desarrollo de Sistemas
RSA-ISO-1031-001-Política de Criptografía
RSA-ISO-1041-001-Política de Sistema de Operación
RSA-ISO-1043-001-Política de Origen del Programa
RSA-ISO-1100-001-Política Gerencial para la Continuidad Comercial
RSA-ISO-1211-001-Identificación de Política de Legislación Aplicable
RSA-ISO-1212-001-Política de Derechos de Propiedad Intelectual
RSA-ISO-1213-001-Salvaguarda de la Política de Registros Organizacionales
RSA-ISO-1214-001-Protección y Privacidad de Datos de la Política de Información del Personal
RSA-ISO-1217-001-Política de Recolección de Evidencia
RSA-ISO-1221-001-Cumplimiento con la Política de Seguridad
RSA-ISO-1222-001-Política de Chequeo de Cumplimiento Técnico
RSA-ISO-1231-001-Política de Controles de Auditoria del Sistema

3.8 Beneficios cualitativos de la aplicación de la Norma.

La aplicación y desarrollo de las políticas de seguridad a través de la Norma tuvieron como consecuencia los siguientes beneficios dentro de las seguridades implementadas.

1. Anti-Virus

   Asegurar en toda la organización mantenga siempre la última versión de antivirus instalados en los servidores y estaciones de trabajo. Con esto se ahorró tiempo en el manejo de incidentes de reportes a mesa de ayuda. Todos los usuarios actualizaban la última versión de virus en sus PCs en forma centralizada y automatizada, con lo cual se dejó de perder información dentro de la organización debido a virus informático.

2. Email / Intranet

   Asegurar que las facilidades de Correo electrónico e Internet requeridas para soportar satisfactoriamente las operaciones de negocio no comprometan su seguridad y eficiencia. El acceso al correo electrónico sirvió para que el personal de la empresa trabaje en forma más eficiente con lo cual la productividad de la empresa se mejoró.

3. Control de Acceso

   Asegurar que todos los sistemas, redes, equipos e información estén protegidos por controles efectivos de autenticación y contraseñas. La seguridad de la información se protegió para accesos no autorizados. Se pudo monitorear los intentos de acceso no permitidos y los posibles daños a la empresa por robo de información se minimizaron.

4. Configuración de dispositivos

   Asegurar que todo hardware/software esté configurado con su nivel aprobado mas actualizado y de forma apropiada a fin de minimizar el riesgo de exposición de su seguridad. Generalmente los virus y los troyanos atacan vulnerabilidades de los dispositivos de red. Con esta implementación se trabajo en forma preventiva con lo cual se ahorro tiempo en su reparación y pérdida de información.

5. Acceso Internet

   Asegurar que todo acceso Internet a través de las facilidades de la organización es controlado y monitoreado. Un gran porcentaje de los problemas de las redes actuales es debido a la navegación irrestricta a Internet con las consecuencias que todos conocemos. El restringir y controlar el acceso sirvió para mejorar la productividad de

los empleados así como minimizar los ataques y vulnerabilidades de la red de la empresa.

6. Seguridad Física

Asegurar que toda infraestructura de TI es solamente accesible al personal aprobado y autorizado por la empresa. Aspecto importante sobre todo en la empresa en donde la información es bastante crítica debido a la competencia y los controles de las entidades fiscalizadoras como la SBS (Superintendencia de Banca y Seguros)

7. Sistemas Web

Asegurar que toda servicio de hosting cumpla con los principios y estándares de seguridad de la organización. El colocar los servicios Web en zonas seguras, DMZ, sirvió para minimizar los riesgos de contaminación de virus y ataques a través de Internet.

8. Cifrado / Gestión de archivos

Implementar las acciones mínimas que prevengan las amenazas de seguridad más comunes. El cifrado o herramientas/técnicas de gestión de archivos debe ser una solución aprobada internamente en la organización. El implementar el cifrado en las notebooks redujo el robo de información como consecuencia de la perdida de los equipos debido al constante viaje de los funcionarios dentro y fuera del país.

9. Monitoreo / Auditoria

Implementar mecanismos efectivos de monitoreo y auditoria. Sirvió para la gestión de infraestructura de la seguridad de la información de la empresa. Reportar los avances obtenidos con respecto a la seguridad, el reporte de ataques de intrusos a la red y sobre todo al análisis costo beneficio de la implementación de todas las herramientas de gestión de la red.

10. Establecimiento de un sistema de gestión de la seguridad de la información.

La empresa definió el alcance y los limites de la aplicación de la norma en términos de las características de la organización, se incluyó un marco conceptual estableciendo políticas y objetivos claros, se tuvieron requisitos legales e informáticos, se identificó una metodología para todas las subsidiarias, se controló los accesos y permisos, se identificó las vulnerabilidades, se evaluó el impacto en el negocio y se implementaron soluciones realistas acorde con el presupuesto.

3.9 Gastos de Seguridad y beneficios.

3.9.1 Beneficios.

Una vez implementadas las políticas y procedimientos de seguridad en el Hardware y Software se llevó a cabo el monitoreo y control de la posibles violaciones de seguridad. Habiendo realizado una serie de actividades e invertido tiempo y dinero se empezó a reportar en forma mensual las actividades de seguridad en base a las herramientas de seguridad.

La Tabla 3.6 muestra el reporte de incidentes donde se describe por cada área la métrica utilizada, la evidencia utilizada y los comentarios respectivos.

En resumen:

- Se bloquearon cerca de 3090 correos con virus.
- Se bloquearon cerca de 2561 sitios de la Web no autorizados.
- Se llevó a cabo la encriptación del 100% de las laptops.
- Se detectó 35 posibles ataques a la red, los cuales fueron bloqueados.
- Se detectó 5 contratos con clausulas relativas a la seguridad de información.
- Se tuvo la relación de los cien (100) principales usuarios de Internet.
- Se obtuvo la relación de los cien (100) sitios de la Web más visitados los cuales se filtraron.

Tabla 3.6: Reporte de Incidentes.

Area	Métrica	Evidencia	Comentarios
Operating System Hardening	**% of target devices hardened = 0**	**Security Expressions scans**	
AntiVirus	**Number of viruses blocked internally = 25 Number of machines lacking current AV**	**EPO* reports EPO* reports**	**El bloqueo de virus Internet en los servicios de mensajería Domino se**

	software = 0		realiza a través de Casa Matriz.
Filtering	Number of emails blocked internally = 3,090 Number of site visits blocked = 2,561	Watchdog* reports Surfcontrol* report	
Laptop Encryption	% of target devices encrypted = 100%	Number of encryption certificates in use = 4	
Firewall	Number of network scans blocked = 0	Firewall software report	
IDS	Number of attacks blocked = 35	IDS software report	Se envió un ZIP con el LOG del Snort
Server/desktop upgrades	% of target devices upgraded = 0	Security Expressions scans	Security Expressions
Access Control		Security Expressions scans	Security Expressions
Logging and Monitoring	Number of security-related events identified = 0	Logging and monitoring software reports = 0	En implementación. Planificada su culminación para Diciembre.
Incident Management	Number of incidents	Incident Management database report	

	reported/identifie d = 0		
BCP	**Number of tests performed =1**	**Up-to-date BCP document available**	
Physical Security	**Number of incidents = 0**	**Reports = 0**	
Legal	**% of contracts containing Information Security clauses = 5**	**Locally-customized contract clauses available**	
Awareness	**Material available**	**Locally-produced material available**	
Asset Management	**Inventories & licence documentation**	**Locally-produced inventories, license documentation**	
Other implementati on-related reports	**Top 100 Internet users** **Top 100 Internet sites visited**	**Surfcontrol* reporte** **Surfcontrol* reporte**	

3.9.2 Eficiencia y productividad de los usuarios

Los siguientes resúmenes muestran como a través del bloqueo a los usuarios a la navegación de Internet se redujo y de detectó los sitios Web que los usuarios ingresaban con mayor frecuencia para el consiguiente filtrado con autorización de sus jefaturas. De este modo el trabajo de la oficina se hizo más productivo toda vez que los usuarios navegaron en Internet solo a páginas Web autorizadas y que servían para el desarrollo de sus trabajo.

Se puede observar que hubieron 1,756 intentos de accesos a noticieros y/o periódicos a través de Internet, esto dato tiene su correspondencia en el consumo aproximado del 4%

del ancho de banda en la navegación, así como las 5,469 conexiones a noticieros y periódicos.

Resumen de bloqueos por categoría de intento de navegación en Internet.

Category No. of Blocked Connections

- News 1,756
- None 308
- Search Engines 231
- Web-based Email 43
- Sport 40
- Arts & Entertainment 38
- Shopping 33
- Travel 33
- Hacking 18
- Government & Politics 18
- Adult/Sexually Explicit 11
- Advertisements 6
- Reference 5
- Usenet News 4
- Real Estate 4
- Hate Speech 2
- Computing & Internet 2
- Motor Vehicles 2
- Hosting Sites 2
- Gambling 1
- Finance & Investment 1
- Job Search & Career Development 1
- Streaming Media 1
- Lifestyle & Cultures 1

Resumen de la Navegación a Internet: Ancho de banda consumido por categoría de sito Web

Data Received:

- Finance & Investment 70.3%
- Reference 8.3%
- News 4.2%
- None 4.1%
- Food & Drinks 3.2%
- Computing & Internet 3.0%
- Search Engines 1.3%
- Government & Politics 0.9%
- Health & Medicine 0.8%
- Travel 0.7%
- Others 3.1%

- Total: 100.0%

Data Sent

- Finance & Investment 54.4%
- Computing & Internet 23.9%
- Reference 6.2%
- News 4.0%
- None 3.9%
- Government & Politics 1.3%
- Search Engines 1.1%
- Photo Searches 0.8%
- Arts & Entertainment 0.6%
- Health & Medicine 0.5%
- Others 3.3%
- Total: 100.0%
- Data Received
- Total Bytes Received: 1,264.07 Mb
- Date Range: 01/12/2003 00:00 to 30/12/2003 23.59.59
- Total Bytes Sent: 67.03 Mb

Resumen de las 100 principales conexiones Internet por categoría de sitio Web

	Conections	BytesSent	Bytes Received
1 Finance & Investment	83,121	47.16 M	688.12 M
2 Reference	9,191	5.59 M	78.10 M
3 News	5,469	2.81 M	50.14 M
4 None	5,022	2.74 M	49.36 M
5 Food & Drinks	4,398	2.16 M	6.35 M
6 Computing & Internet	3,812	2.04 M	301.73 M
7 Search Engines	1,368	872.3 K	14.00 M
8 Government & Politics	1,317	619.7 K	16.59 M
9 Travel	1,029	448.8 K	5.17 M
10 Health & Medicine	954	525.3 K	6.37 M
11 Photo Searches	589	276.0 K	10.46 M

3.9.3 Gastos en Seguridad.

El presente proyecto tuvo un presupuesto estimado de inversión de 181,171 dólares americanos. La gerencia de sistemas tuvo que coordinar su ejecución a fin de controlar el gasto durante su ejecución. El presupuesto estaba compuesto de los rubros que se muestran en la tabla 3.7

Tabla 3.7: Presupuesto del Proyecto

I. PRE REQUISITOS PARA EL PROYECTO DE SEGURIDAD					
Inversión requerida	**Descripción**	**Cantidad**	**Costo unitario**	**Local $**	**Deducida $**
Reemplazo de PCs Pentium I y Pentium II	Renovación tecnológica de hardware para efecto de trabajar con Windows 2000/XP. Pre-requisito para el proyecto de Seguridad	128	1,080	138,240	
Ampliación de memoria para las Pentium III que quedan	Ampliación a 256 Mb RAM para que soporten Windows 2000 con un rendimiento aceptable.	20	55	1,100	
Reemplazo de Notebooks Pentium I	Renovación tecnológica de hardware para efecto de trabajar con Windows 2000/XP. Pre-requisito para el proyecto de Seguridad	1	2,000	2,000	
Upgrade Windows 9x a XP	Cumplimiento de utilización de Sistemas Operativos seguros. Pre-requisito para el proyecto de seguridad	32	188	6,016	
Upgrade Advantage CAL SQL Cliente 7 a SQL 2000 CAL	Licenciamiento de software. Pre-requisito para el proyecto de seguridad.	43	100	4,300	
Licenciamiento MS SQL - Central Telefónica	Licenciamiento de software.	1	706	706	
Upgrade de MS Backoffice a MS SQL 2000	Licenciamiento de software. Pre-requisito para el proyecto de seguridad.	1	455	455	
				152,817	

II. PROYECTO DE SEGURIDAD					
Inversión requerida	**Descripción**	**Cantidad**	**Costo unitario**	**Local $**	**Deducida $**
Security Expression	Actualización automática de versiones y parches de Sistemas Operativos				
Servidor		1	4,500	4,500	
Licencia por usuario		160	5		800
Safeboot	Software de encriptación. Requerido en el proyecto de seguridad solo para las notebooks				
Servidor					
Licencia por usuario		4	75		300
Enterprice Policy Orchestrator (EPO)	Software de distribución y actualización de antivirus				
Servidor					
Licencia por usuario		160	11		1,789
ISA Proxy	Reemplazo de nuestro Proxy bajo Linux por estándar del Grupo				
Servidor		1	4,500	4,500	
Software		1	1,000		1,000
Super Scout	Software de bloqueo de acceso a sites en Internet				
Servidor					
Software		160	12		1,920
Firewall Nokia/Checkpoint	Reemplazo de Firewall de acuerdo al estandar del grupo	1	13,545	13,545	
				22,545	**5,809**

CONCLUSIONES

1. La seguridad de la información y la gestión de la misma es fundamental en las actuales circunstancias, donde la información es de vital importancia para la empresa.
2. La empresa tuvo que identificar y gestionar muchas actividades para que funcione la norma de manera eficaz.
3. Lo importante fue comprender los requisitos de seguridad de la información de la empresa y la necesidad de establecer una política y objetivos claros para la seguridad de la información.
4. El implementar y operar controles para gestionar los riesgos de seguridad de la información es tan importante como la aplicación de la norma, por tal motivo el cuestionario sirve para este motivo.
5. Royal Sun Alliance Seguros Fénix al ser una empresa del sector financiero esta expuesta a ataques a través de la red por lo que dichos ataques pueden ocasionar graves daños financieros en la organización causando graves dificultades económicas, por lo que no implementar la norma es un gran riesgo.
6. De hecho los requisitos establecidos en la Norma son genéricos al pretender que sean capaces de aplicar a todas las organizaciones, por tal motivo la aplicación de la norma dentro de la empresa causo un gran esfuerzo de los funcionarios involucrados, por lo que el compromiso de su aplicación fue refrendado por la Gerencia General.
7. La implementación de la norma ISO sirvió para que la empresa alcance niveles de estándares de seguridad en el corto plazo.

8. La implementación de dicha norma conlleva un planeamiento y seguimiento exhaustivo para cumplir con los objetivos.
9. Es necesario la participación de la gerencia de la empresa a fin de comprometerse con el presupuesto de inversión requerido para aplicar la norma.
10. La utilización de una herramienta de fácil uso para el análisis de las brechas de seguridad es sumamente importante debido a que se establece en forma clara y concisa las debilidades de seguridad y sirve para planificar en forma inmediata la implementación de la norma en los campos comprometidos de seguridad.
11. El seguimiento de la norma ISO sirve para que la empresa se ordene en la implementación de la misma. Generalmente hay esfuerzos separados para mitigar los problemas de seguridad. El seguir los pasos definidos por la norma sirve para trabajar en forma ordenada y metodológica.
12. Las herramientas de hardware y software utilizadas para implementar las medidas de seguridad conllevaron a una especialización del personal de la empresa a fin cumplir con la implementación y gestión de las mismas.
13. Se minimizaron los ataques externos a la red de la empresa. Se eliminó la posibilidad de virus en las PCs de los usuarios, se monitoreó constantemente la actividad de la seguridad en la infraestructura de hardware y software de la empresa.
14. El filtrado y negación al acceso a Internet sirve para la mejora de la productividad del personal de la empresa. Se filtraron solo las páginas Web autorizadas para el trabajo con lo cual se hizo más eficiente el trabajo.
15. La puesta en marcha de las herramientas de bloqueo, antivirus, y demás sirvieron para la prevención de ataques con lo cual se minimizo la perdida de información.
16. La estandarización de los usuarios y passwords protegieron la información de cualquier robo o acto delictivo con la misma.

17. El asegurar la plataforma de la red informática con los últimos parches sirvieron para minimizar las vulnerabilidades de los mismos.

18. Finalmente se puede observar que la aplicación de la Norma de Seguridad de la información ISO 17799 requiere de un trabajo continuo. El aplicar toda la serie de recomendaciones señaladas en el presente trabajo no garantiza que en un futuro cercano la empresa pueda sufrir una violación de información. De hecho los ataques, virus, spams, gusanos, perdida de información, cambios de passwords, etc., seguirán existiendo en la red de la empresa, por tal motivo el gerente del área de tecnología de información de la empresa, como parte de sus funciones y responsabilidades, tuvo que incorporar el monitoreo y actualización permanente de la seguridad a través del comité respectivo de seguridad.

BIBLIOGRAFÍA

1. Presidencia del Consejo de Ministros "Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información – 1er. Edición NTP – ISO/IEC 17799:2004",
   Gobierno del Perú -ONGEI – Perú, 2004.
2. Richard Astill " Information Securtiy Self Assessment Questionnaire (SAQ) v1.0",
   Royal & Sun Alliance – London, 2003
3. Richard Astill & Group Operational Risk "Orverrall Group Information Securtiy Policity Statement",
   Royal & Sun Alliance – London, 2004