"DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA E IMPLEMENTACIÓN DE TRES DOMINIOS EN BASE A LA NORMA 27002 PARA EL ÁREA DE HARDWARE EN LA EMPRESA UNIPLEX SYSTEMS S.A. EN QUITO"

Richard Eduardo Posso Guerrero (richardposso@hotmail.com)
Pablo López Ing. (pablo.lopez@epn.edu.ec)

Ingeniería en Electrónica y Telecomunicaciones
Escuela Politécnica Nacional

Resumen

RESUMEN:

En el presente proyecto se desarrolla un Plan Piloto de Políticas de Seguridad Informática para ser implementado en el área de Networking de la empresa Uniplex Systems S.A. Se presenta un resumen de la historia de la ISO 27000 y se describe la norma de Seguridad de la Información ISO/IEC 27002. Se analizan tres dominios de la norma que tienen estrecha relación con la Seguridad Informática. Se analiza también la situación de las políticas de Seguridad Informática instauradas previo a la implementación del Plan Piloto. Se describe la metodología para desarrollar un Sistema de Seguridad Informática y se desarrolla el Plan Piloto de Políticas de Seguridad Informática. Se desarrollan las nuevas políticas en base al procedimiento visto y se procede a la implementación de las mismas. Se presentan las conclusiones y recomendaciones del presente proyecto. En los anexos se dispone de conceptos importantes de este proyecto; se detalla la documentación e instructivos que se desarrollaron para implementar la norma, se indica la implementación de las políticas de Seguridad Informática y se dispone de una guía para que los usuarios las apliquen sin dificultad.

Abstract

The present project is a Test Plan for Informatics Security Policies to be implemented in the Networking area at the Uniplex Systems S.A Company. This project provides a summary of ISO 27000 history and describes the standard for Information Security ISO/IEC 27002. It analyzes three standard domains which are closely related to Informatics Security. The state of information security policies in place, prior the Test Plan implementation is analyzed. Moreover describes the methodology to develop an Informatics Security System and the Test Plan for Informatics Security Policies. New policies are developed based on the procedure shown and proceed to implement them. Also, the conclusions and recommendations of this project are presented. In the annexes, are important concepts of this project, detailed documentation and instructions that were developed to implement the standard, indicating the implementation of information security policies and a guide for users to implement them smoothly.

1. MARCO TEÓRICO

1.1 INTRODUCCIÓN

En este mundo globalizado; las empresas, a más de estar en permanente evolución y desarrollo, requieren estar acorde con las regulaciones legales y técnicas del entorno, deben implementar normas que les permita cumplir estos preceptos, y desarrollar controles para evitar quedarse rezagadas de las demás.

Varias empresas piensan que disponen de una correcta Seguridad Informática y creen que sus "datos confidenciales" son inaccesibles a personal no autorizado; pero el hecho es que en la mayoría de casos, al fin de mes o de año, las empresas competidoras disponen en la Mesa de Reuniones los balances generales de estas "empresas con políticas de Seguridad Informática" equívocamente implementadas. Las fuentes de las empresas competidoras en muchos casos es gente inescrupulosa que pertenece a la misma empresa pero que se dedica al tráfico de información para sacar lucro.

Otro caso no tan alejado de la realidad son las empresas que tienen la información para desarrollar proyectos, pero que no saben donde la tienen, disponen de todos los documentos de investigaciones previas regada por todos lados, sin clasificar y desordenada, teniendo en algunos casos más de diez veces la copia de una canción favorita que un desarrollo investigativo.

Existen peores circunstancias en que la empresa nunca ha reflexionado acerca de la continuidad del negocio.

Como todos sabemos, mucha información es vulnerable; puede perderse debido a fallas en elementos físicos, afectarle un virus informático, desastres naturales, etc.

Es claro que la correcta aplicación de las Políticas de Seguridad de la Información mantiene la integridad, confidencialidad y disponibilidad de la misma; y por ello se aclara que este trabajo involucra un subconjunto de éstas, se habla de políticas de Seguridad Informática, que ayudan a establecer las Políticas de Seguridad de la Información.

- Publicación BS 8800 - ahora OHSAS 18001 (Requisitos de Sistema de Gestión de Seguridad y Salud)

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

Gráfico 1. Historia de la Norma ISO 27002

1.2 NORMAS ISO 27000[1]

Se presenta un resumen de las normas 27002.

Desde 1901, y como primera entidad de normalización a nivel mundial, el Instituto Británico de Estandarización (British Standards Institution BSI), fue responsable de la publicación de importantes normas como:

- Publicación BS 5750 - ahora ISO 9001 (Sistema de Gestión de Calidad)
- Publicación BS 7750 - ahora ISO 14001 (Especificaciones y elementos de cómo implementar un Sistema de Gestión Ambiental)

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, en la que no se establece un esquema de certificación. La segunda parte (BS 7799-2), publicada por primera vez en 1998, establece los requisitos de un sistema de Seguridad de la Información (SGSI) para ser certificable por una entidad independiente. Ver Gráfico 1.

[1] http://www.iso27000.es/doc_iso27000_all.htm

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.
En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

1.3 DESCRIPCIÓN DE LA NORMA 27002

Esta Norma contiene 39 objetivos de control y 133 controles que se encuentran agrupados en 11 dominios principales. A continuación se presenta un resumen de la Norma ISO/IEC 27002.

1. POLÍTICA DE SEGURIDAD.
1.1 Política de seguridad de la información.
1.1.1 Documento de política de seguridad de la información.
1.1.2 Revisión de la política de seguridad de la información.

2. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
2.1 Organización interna.
2.1.1 Compromiso de la Dirección con la seguridad de la información.
2.1.2 Coordinación de la seguridad de la información.
2.1.3 Asignación de responsabilidades para la segur. de la información.
2.1.4 Proceso de autorización de recursos para el tratamiento de la información.
2.1.5 Acuerdos de confidencialidad.
2.1.6 Contacto con las autoridades.
2.1.7 Contacto con grupos de interés especial.
2.1.8 Revisión independiente de la seguridad de la información.
2.2 Terceros.
2.2.1 Identificación de riesgos por el acceso de terceros.
2.2.2 Tratamiento de la seguridad en la relación con los clientes.
2.2.3 Requisitos de seguridad en contratos con terceros.

3. GESTIÓN DE ACTIVOS.
3.1 Responsabilidad sobre los activos.
3.1.1 Inventario de activos.
3.1.2 Propiedad de los activos.
3.1.3 Uso aceptable de los activos.
3.2 Clasificación de la información.
3.2.1 Directrices de clasificación.
3.2.2 Etiquetado y manipulado de la información.

4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
4.1 Antes de la contratación.
4.1.1 Funciones y responsabilidades.
4.1.2 Investigación de antecedentes.
4.1.3 Términos y condiciones de contratación.
4.2 Durante la contratación.
4.2.1 Responsabilidades de gestión.
4.2.2 Concienciación, educación y capacitación en segur. de la informac.
4.2.3 Proceso disciplinario.
4.3 Cese o cambio de puesto de trabajo.
4.3.1 Responsabilidad del cese o cambio.
4.3.2 Devolución de activos.
4.3.3 Retirada de los de derechos de acceso.

5. SEGURIDAD FÍSICA Y AMBIENTAL.
5.1 Áreas seguras.
5.1.1 Perímetro de seguridad física.
5.1.2 Controles físicos de entrada.
5.1.3 Seguridad de oficinas, despachos y recursos.
5.1.4 Protección contra las amenazas externas y ambientales.
5.1.5 El trabajo en áreas seguras.
5.1.6 Áreas de acceso público, carga y descarga.
5.2 Seguridad de los equipos.
5.2.1 Emplazamiento y protección de equipos.
5.2.2 Instalaciones de suministro.
5.2.3 Seguridad del cableado.
5.2.4 Mantenimiento de los equipos.
5.2.5 Seguridad de los equipos fuera de las instalaciones.
5.2.6 Reutilización o eliminación de equipos.
5.2.7 Retirada de materiales propiedad de la empresa.

6. GESTIÓN DE COMUNICACIONES Y OPERACIONES.
6.1 Responsabilidades y procedimientos de operación.
6.1.1 Documentación de procedimientos de operación.
6.1.2 Gestión de cambios.
6.1.3 Segregación de tareas.
6.1.4 Separación de los recursos de desarrollo, ensayo y producción.
6.2 Gestión de la provisión de servicios por terceros.
6.2.1 Prestación de servicios.
6.2.2 Supervisión y revisión de los servicios prestados por terceros.
6.2.3 Gestión de cambios en los servicios prestados por terceros.
6.3 Planificación y aceptación del sistema.
6.3.1 Gestión de capacidades.
6.3.2 Aceptación del sistema.
6.4 Protección contra código malicioso y móvil.
6.4.1 Controles contra el código malicioso.

6.4.2 Controles contra el código descargado en el cliente.
6.5 Copias de seguridad.
6.5.1 Copias de seguridad de la información.
6.6 Gestión de la seguridad de las redes.
6.6.1 Controles de red.
6.6.2 Seguridad de los servicios de red.
6.7 Manejo de los soportes.
6.7.1 Gestión de soportes extraíbles.
6.7.2 Eliminación de soportes.
6.7.3 Procedimientos de manejo de la información.
6.7.4 Seguridad de la documentación del sistema.
6.8 Intercambio de información.
6.8.1 Políticas y procedimientos de intercambio de información.
6.8.2 Acuerdos de intercambio.
6.8.3 Soportes físicos en tránsito.
6.8.4 Mensajería electrónica.
6.8.5 Sistemas de información de empresa.
6.9 Servicios de comercio electrónico.
6.9.1 Comercio electrónico.
6.9.2 Transacciones en línea.
6.9.3 Información a disposición pública.
6.10 Supervisión.
6.10.1 Registro de auditorías.
6.10.2 Supervisión del uso del sistema.
6.10.3 Protección de la información de registro.
6.10.4 Registros de administración y operación.
6.10.5 Registro de fallos.
6.10.6 Sincronización de relojes.

7. CONTROL DE ACCESOS.
7.1 Requisitos de negocio para el control de accesos.
7.1.1 Política de control de accesos.
7.2 Gestión de acceso de usuario.
7.2.1 Registro de usuario.
7.2.2 Gestión de privilegios.
7.2.3 Gestión de contraseñas de usuario.
7.2.4 Revisión de los derechos de acceso de los usuarios.
7.3 Responsabilidades del usuario.
7.3.1 Uso de contraseña.
7.3.2 Equipo informático de usuario desatendido.
7.3.3 Política de puesto de trabajo despejado y bloqueo de pantalla.
7.4 Control de acceso a la red.
7.4.1 Política de uso de los servicios de red.
7.4.2 Autenticación de usuario para conexiones externas.
7.4.3 Identificación de equipos en redes.
7.4.4 Diagnóstico remoto y protección de los puertos de configuración.
7.4.5 Segregación en redes.
7.4.6 Control de la conexión a red.
7.4.7 Control de encaminamiento de red.
7.5 Control de acceso al sistema operativo.
7.5.1 Procedimientos seguros de inicio de sesión.
7.5.2 Identificación y autenticación de usuario.
7.5.3 Sistema de gestión de contraseñas.
7.5.4 Uso de las utilidades del sistema.
7.5.5 Desconexión automática de sesiones.
7.5.6 Limitación del tiempo de conexión.
7.6 Control de acceso a la aplicación y a la información.
7.6.1 Restricción del acceso a la información.
7.6.2 Aislamiento de sistemas sensibles.
7.7 Ordenadores portátiles y teletrabajo.
7.7.1 Ordenadores portátiles y comunicaciones móviles.
7.7.2 Teletrabajo.

8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
8.1 Requisitos de seguridad de los sistemas de información.
8.1.1 Análisis y especificación de los requisitos de seguridad.
8.2 Procesamiento correcto en las aplicaciones.
8.2.1 Validación de los datos iniciales.
8.2.2 Control del procesamiento interno.
8.2.3 Autenticación e integridad de los mensajes.
8.2.4 Validación de los datos de salida.
8.3 Controles criptográficos.
8.3.1 Política de uso de los controles criptográficos.
8.3.2 Gestión de claves.
8.4 Seguridad de los archivos de sistema.
8.4.1 Control del software en explotación.
8.4.2 Protección de los datos de prueba del sistema.
8.4.3 Control de acceso al código fuente de los programas.
8.5 Seguridad en los procesos de desarrollo y soporte.
8.5.1 Procedimientos de control de cambios.
8.5.2 Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo.
8.5.3 Restricciones a los cambios en los paquetes de software.
8.5.4 Fugas de información.
8.5.5 Externalización del desarrollo de software.
8.6 Gestión de la vulnerabilidad técnica.
8.6.1 Control de las vulnerabilidades técnicas.

9. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN
9.1 Notificación de eventos y puntos débiles de la segur. de la información.
9.1.1 Notificación de los eventos de seguridad de la información.
9.1.2 Notificación de puntos débiles de la seguridad.
9.2 Gestión de incidentes de seguridad de la información y mejoras.
9.2.1 Responsabilidades y procedimientos.

9.2.2 Aprendizaje de los incidentes de seguridad de la información.
9.2.3 Recopilación de evidencias.

10. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
10.1 Aspectos de seguridad de la información en la gestión la de continuidad del negocio.
10.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
10.1.2 Continuidad del negocio y evaluación de riesgos.
10.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
10.1.4 Marco de referencia para la planificación de la cont. del negocio.
10.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

11. CUMPLIMIENTO.
11.1 Cumplimiento de los requisitos legales.
11.1.1 Identificación de la legislación aplicable.
11.1.2 Derechos de propiedad intelectual (DPI).
11.1.3 Protección de los registros de la organización.
11.1.4 Protección de datos y privacidad de la información personal.
11.1.5 Prevención del uso indebido de las instalaciones de procesamiento de la información.
11.1.6 Regulación de los controles criptográficos.
11.2 Cumplimiento de las políticas y normas de segur. y cumplimiento técnico.
11.2.1 Cumplimiento de las políticas y normas de seguridad.
11.2.2 Comprobación del cumplimiento técnico.
11.3 Consideraciones de las auditorías de los sistemas de información.
11.3.1 Controles de auditoría de los sistemas de información.
11.3.2 Protección de las herramientas de auditoría de los sist. de inform

2. ANÁLISIS DE LA NORMA ISO/IEC 27002

2.1 INTRODUCCIÓN

Como se ha visto, la norma ISO/IEC 27002 está constituida por once dominios:

a. Política de seguridad
b. Organización de la Seguridad de la Información
c. Gestión de activos
d. Seguridad de los Recursos Humanos
e. Seguridad física y del entorno
f. Gestión de operaciones y comunicaciones
g. Control de acceso
h. Adquisición, desarrollo y mantenimiento de sistemas de información
i. Gestión de los incidentes de Seguridad de la Información
j. Gestión de la continuidad del negocio
k. Cumplimientos

El presente trabajo es acerca de *políticas de Seguridad Informática*, por este motivo se centra el estudio en los tres dominios que involucran este tema:

a. Política de seguridad
b. Organización de la Seguridad de la Información
c. Gestión de activos

Se debe tener mucho cuidado de no mal interpretar el párrafo anterior ya que en ningún momento se dice que los tres dominios sean los más importantes o que los otros no lo sean, solamente se habla acerca del alcance que tiene un modelo se seguridad de información versus un modelo de Seguridad Informática.

2.2 PLAN DE CONTINUIDAD DEL NEGOCIO[2]

Las empresas no solamente son vulnerables a grandes desastres, sino también a pequeños cambios que pueden afectar la continuidad del negocio.

Existen factores como: Incremento en la dependencia tecnológica; las presiones de "velocidad del mercado" que han hecho a las empresas sumamente sensibles a catástrofes o eventos menores que generan perturbación en sus operaciones.

En la última década, los riesgos de desastres naturales, las fallas técnicas de carácter accidental, y las actividades maliciosas han incrementado las posibilidades de interrupciones en las empresas. A pesar de este hecho, muy pocas empresas invierten en planificación de actividades para minimizar posibles desastres.

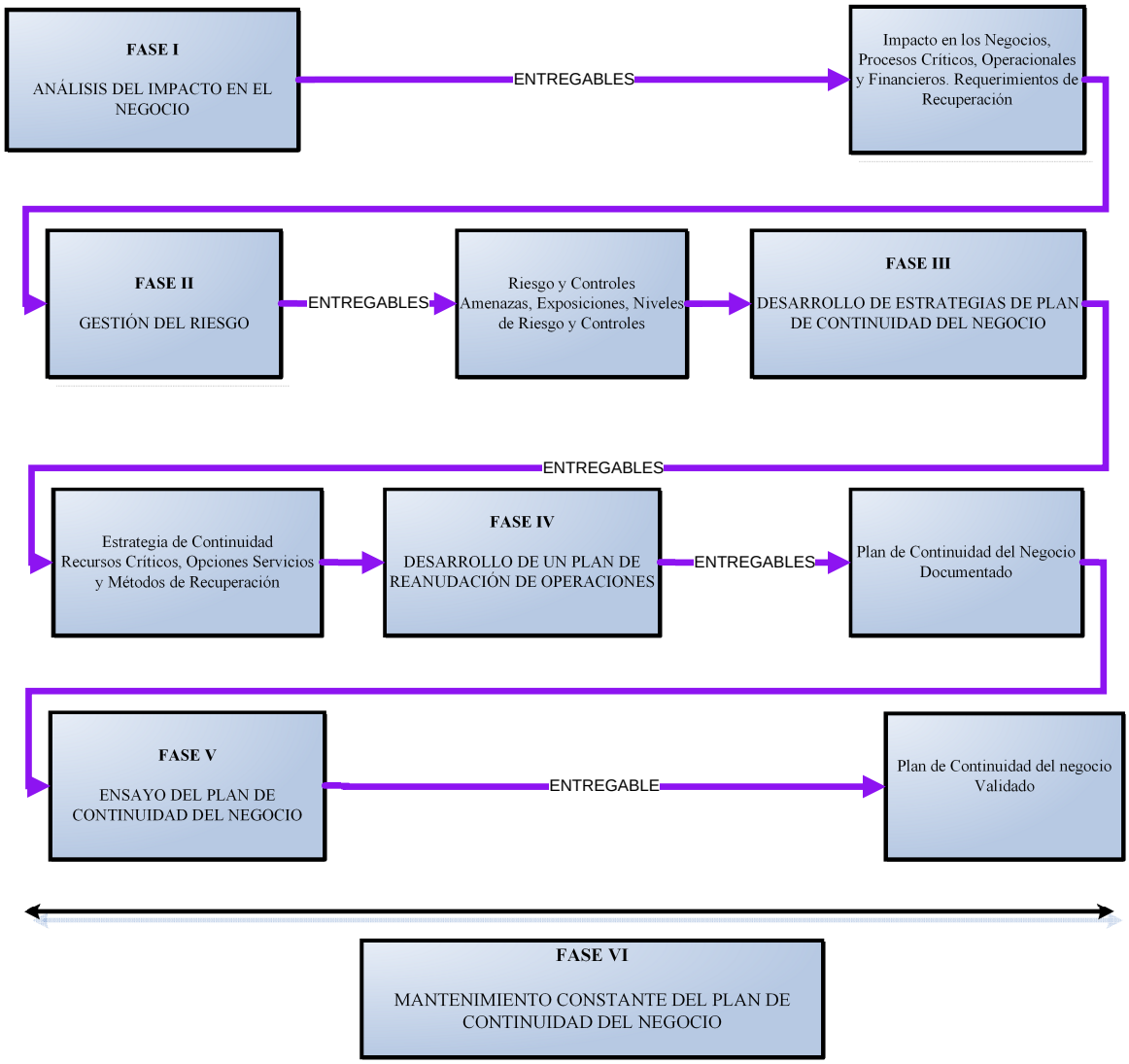

Gráfico 2. Proceso PCN y los entregables

[2] Plan de Continuidad del Negocio, Estándar Internacional BS 25999-2:2007, Alberto Alexander

Existen ciertos enfoques que son similares al Plan de Continuidad del Negocio y a la vez tienen sus diferencias que se enuncian a continuación:

Plan de Recuperación de Desastres (Disaster Recovery Planning DRP).- Se enfoca en la recuperación de los servicios de TI y los recursos de la empresa, dado un evento que ocasionara una interrupción mayor en su funcionamiento

Plan de Reanudación del Negocio (Business Resumption Planning BRP).- Se centraliza en la reanudación de los procesos de negocios afectados por una falla en las aplicaciones de TI. Se enfoca en la utilización de procedimientos relacionados con el área de trabajo.

Plan de Continuidad de las Operaciones (Continuity of Operations Planning COOP).- Busca la recuperación de las funciones estratégicas de una organización que se desempeñan en sus instalaciones corporativas.

Plan de Contingencia (Contingency Planning CP).- Se enfoca en la recuperación de los servicios y recursos de TI, después de un desastre de dimensiones mayores o de una interrupción menor. Especifica procedimientos y lineamientos para la recuperación, tanto en áreas de la empresa como en las alternas.

Plan Respuesta de Emergencia (Emergency Response Planning ERP).- Su objetivo es salvaguardar a los empleados, el público, el ambiente y los activos de la empresa. Últimamente se busca de inmediato llevar la situación de crisis a un estado de control.

Se puede decir que todos los enfoques tienen un alcance específico, ninguno cubre todas las áreas críticas, y por eso se requiere un enfoque que involucre a todos, este se llama Plan de Continuidad del Negocio (PCN).

Para establecer un PCN se debe seguir un ciclo de vida para el desarrollo y mantenimiento. En el gráfico 3 se ilustra el proceso con sus distintas fases y los entregables

2.3 ANÁLISIS DOMINIO POLÍTICAS DE SEGURIDAD

Este dominio comprende todas las políticas de Seguridad Informática que pueden aplicarse para salvaguardar información importante en una empresa. Se encuentra conformado por un objetivo de control y dos controles. Como se aprecia en el Gráfico 4.

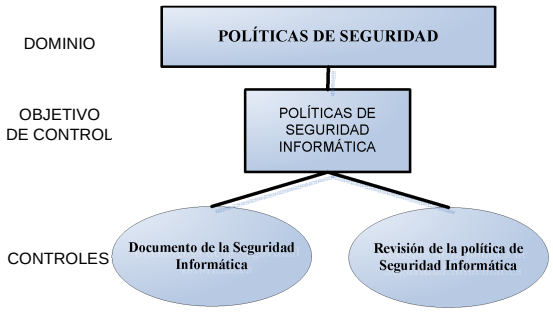

Gráfico 2. Dominio Políticas de Seguridad

2.4 ANÁLISIS DOMINIO ORGANIZACIÓN DE LA SEGURIDAD INFORMÁTICA

Con este control se pueden identificar los puntos clave para gestionar la información en la organización.

Este dominio posee dos objetivos de control el primero ADMINISTRAR LA ORGANIZACIÓN INTERNA con ocho controles y el segundo ADMINISTRAR PARTES EXTERNAS con tres controles. En el Gráfico 4 se aprecia la constitución de este Dominio.

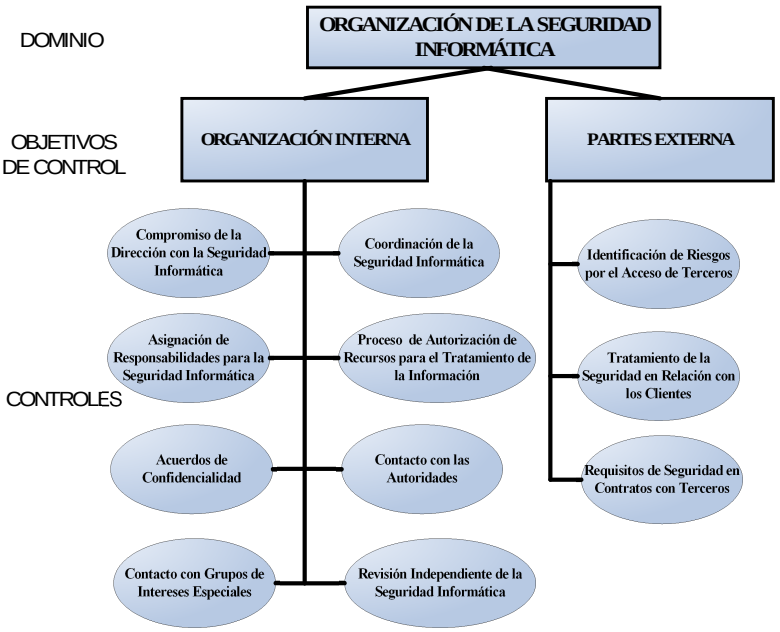

Gráfico 4. Dominio Organización de la Seguridad Informática

2.5 ANÁLISIS DOMINIO GESTIÓN DE ACTIVOS

El reconocimiento y gestión de los activos de información en la organización es importante para determinar los recursos que dispone la empresa y para darles la protección adecuada.

Este dominio posee dos objetivos de control; el primero DETERMINAR LA RESPONSABILIDAD POR LOS ACTIVOS con tres controles, el segundo CLASIFICAR LA INFORMACIÓN con dos controles, esto se aprecia en el Gráfico 5.

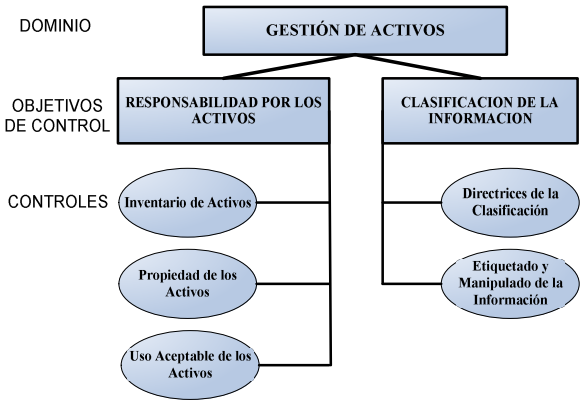

Gráfico 5. Dominio Gestión de Activos

3. ANÁLISIS DE POLÍTICAS PRECEDENTES DE SEGURIDAD Y ESTABLECIMIENTO DEL PLAN PILOTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

3.1 ANÁLISIS DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA PRECEDENTES EN EL ÁREA DE NETWORKING.

Para el *análisis de las políticas de Seguridad Informática* no existen definiciones oficiales, se han dado cursos y seminarios refiriéndose a ella, pero no se ha llegado a establecer un concepto.

Como primer concepto, se puede decir que: "el análisis de las políticas de Seguridad Informática comprende la revisión y evaluación independiente y objetiva, por parte de personas independientes y teóricamente competentes del entorno informático de una entidad, abarcando todo o algunas de sus áreas, los estándares y procedimientos en vigor, su idoneidad y el cumplimiento de éstos, de los objetivos fijados, los contratos y las normas legales aplicables, el grado de satisfacción de usuarios y directivos, los controles existentes y el análisis de riesgos".[3]

Se puede decir entonces que el análisis de las políticas de Seguridad Informática es aquella que tiene como objetivos evaluar los controles de la función informática, determinar la eficiencia de los sistemas, verificar el cumplimiento de las políticas y procedimientos de la empresa en este ámbito y revisar que los recursos materiales y humanos de esta área se utilicen eficientemente.
Este análisis surge debido a que la información es uno de los activos más importantes en las empresas, así como el uso de la tecnología y sistemas computarizados para el procesamiento de la información.

Mediante la Tabla 1 se puede decir que el proceso de Auditoría Informática es el proceso de recolección y evaluación de evidencia para determinar si un sistema:

Salvaguarda Activos	**Daños**
	Destrucción
	Uso no autorizado
	Robo
Mantiene la Integridad de los Datos	**Oportuna**
	Precisa
	Confiable
	Completa
Alcanza Metas Organizacionales	**Contribución de la función Informática**
Consume Recursos Eficientemente	**Utiliza recursos con mesura para procesar la información**

Tabla 1. Proceso de Auditoría Informática

3.2 GUÍA PARA EL ESTABLECIMIENTO DEL PLAN PILOTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

La implementación del Plan Piloto de Política de Seguridad Informática PPPSI requiere grandes recursos; por ello la empresa Uniplex Systems está consciente sobre sus razones para implantar el PPPSI.

La razón debe estar documentada y debe contener los costos en contraposición a los beneficios de gestionar la Seguridad Informática.

[3] Miguel Ángel Ramos González, Especialista en Auditoría Informática.

El PPPSI está conformado por:

- Introducción
  La implementación del Plan Piloto de Política de Seguridad Informática PPPSI requiere grandes recursos; por ello la empresa Uniplex Systems está consciente sobre sus razones para implantar el PPPSI. La razón debe estar documentada y debe contener los costos en contraposición a los beneficios de gestionar la Seguridad Informática

- Alcance del PPPSI
  La definición del alcance es una de las más importantes decisiones en todo el proceso de su establecimiento. El alcance del PPPSI va a depender totalmente de la empresa, puede contenerla totalmente o simplemente una parte, un simple proceso o un sistema de información.
  Una vez determinado el alcance se procede a identificar los distintos activos de información que se convierten en el eje principal del modelo.

- Ilustración para definir un alcance

Como ejemplo, se ha utilizado el Método de las Elipses (que es el más utilizado) y se han determinado brevemente los procesos del departamento de "Networking" de la empresa UNIPLEX Systems S.A.

El método (Gráfico 6) consiste en determinar en la elipse más interna los distintos procesos que conforman el proceso de "Networking", estos son:

- Registro de Llamada
- Verificación tipo de cliente
- Notificación a Ingeniero de Soporte
- Índice de satisfacción de cliente

Se identifican en la elipse intermedia las distintas interacciones que los procesos de la elipse más interna tienen con otros procesos de la organización.

En la elipse más externa, se identifican aquellas organizaciones extrínsecas a la empresa que tienen interacción con los procesos de la elipse concéntrica.
Las flechas indican la interacción entre ambas partes.

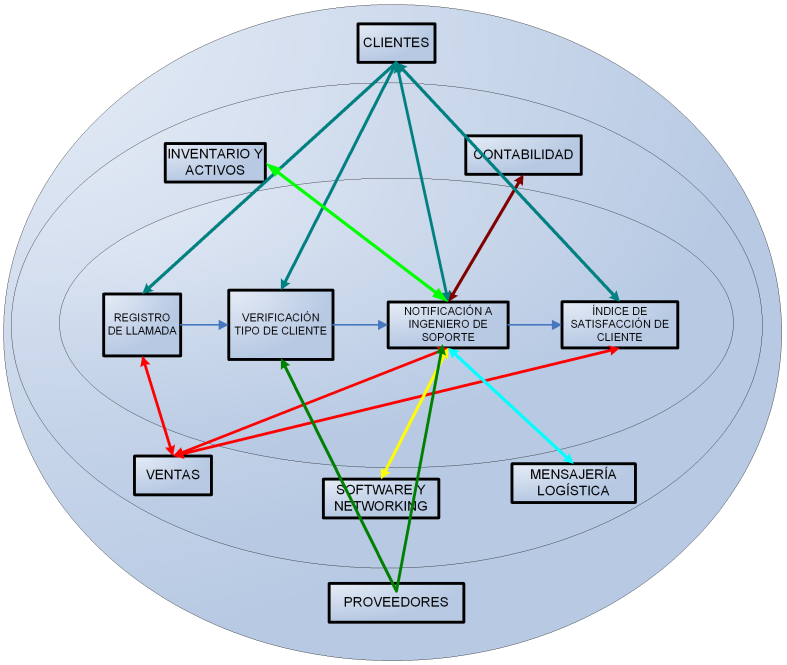

Gráfico 6. Método de las Elipses

para identificar interfaces, interdependencia con áreas y procesos, así como averiguar los contratos existentes y los grados de acuerdos necesarios. El método también se utiliza para obtener los activos de información, esto se consigue al analizar los procesos identificados y el flujo de información.

- Políticas del PPPSI

Una vez establecido el alcance, la empresa define claras políticas de seguridad para apoyar la implementación del PPPSI en la empresa.
La gerencia debe aprobar las políticas, y asegurarse de que todos los empleados las han recibido, entienden su efecto y las ejecutan en sus tareas cotidianas.

- Enfoque para la gestión del riesgo

El método de cálculo del riesgo lo puede decidir la organización, pero se debe asegurar que el enfoque sea el adecuado y apropiado para atender los requerimientos organizacionales legales o regulatorios.

El cálculo del riesgo debe ser detallado y complejo como sea necesario, a fin de poder atender todos los requerimientos de la organización y lo requerido por el alcance del PPPSI, pero nada más. El exceso de detalles puede determinar un exceso de trabajo, y un

enfoque muy genérico puede conducir a subestimar aspectos de riesgos importantes.

Debe existir un equilibrio entre las tres condiciones básicas para la protección de la información (Confidencialidad, Disponibilidad e Integridad)[4], por ejemplo si la información en un computador está protegida por demasiadas contraseñas difíciles de recordar, y si el responsable por esa información olvida las contraseñas, entonces se pierde la disponibilidad, por otro lado si no tiene ninguna contraseña o ninguna seguridad, entonces se pierde la confidencialidad porque cualquier persona puede acceder a su información.

- Proceso de cálculo del riesgo

El cálculo de los riesgos de Seguridad Informática para el área de Networking de la empresa Uniplex Systems S.A. incluye el análisis y la evaluación del riesgo.

El análisis del riesgo contempla:

- Identificación de activos de información.
- Identificación de requerimientos legales y comerciales que son relevantes para los activos identificados.
- Tasación de los activos identificados, considerando los requerimientos legales y comerciales, así como los impactos resultantes de una pérdida por confidencialidad, integridad y disponibilidad.
- Identificación de amenazas y vulnerabilidades para cada activo previamente identificado.
- Cálculo de la posibilidad de que las amenazas y vulnerabilidades ocurran.

La evaluación del riesgo contempla:

- Cálculo del riesgo
- Identificación del significado de los riesgos. Esto se hace definiendo criterios y evaluando los riesgos contra una escala predeterminada.

- Análisis de riesgo

Parte importante del PPPSI para determinar cuáles activos de información posee la empresa y cuáles son las amenazas y vulnerabilidades existentes. Se encuentra conformada por:

- Identificación de Activos
- Identificaciones de Requerimientos Legales y Comerciales Relevantes para los Activos Identificados
- Tasación de Activos
- Identificación de Amenazas y vulnerabilidades
- Cálculo de las Amenazas y Vulnerabilidades
- Análisis del riesgo y su Evaluación

- Evaluación del riesgo

Para realizar la evaluación del riesgo, se debe determinar cuáles son aquellas amenazas cuyos riesgos son los más relevantes.

Para determinar los más relevantes, se utiliza la escala de Likert y los siguientes criterios:

- Impacto económico del riesgo.
- Tiempo de recuperación de la empresa.
- Posibilidad real de ocurrencia del riesgo.
- Posibilidad de interrumpir las actividades de la empresa.

Se ilustra en la Tabla 2 la forma en que se debe evaluar el significado del riesgo.

Tabla 2. Evaluación del riesgo

RIESGO		CRITERIO PARA EVALUAR LA IMPORTANCIA DEL RIESGO				
Activos	Amenazas	Impacto Económico del Riesgo	Tiempo de Recuperación de la Empresa	Probabilidad de Ocurrencia del Riesgo	Probabilidad de Interrumpir Actividades de la empresa	TOTAL

- Riesgo Residual

[4] Ver Conceptos en Anexo A

El riesgo residual es el riesgo remanente que siempre está presente al implementar las decisiones del tratamiento del riesgo. Puede ser difícil de calcular pero al menos debe realizarse una evaluación para asegurar que logra la protección suficiente.

Si es inaceptable tener riesgo residual, deben tomarse decisiones para resolverlo. Se puede aplicar más controles, establecer arreglos con aseguradoras para lograr reducir el riesgo a niveles aceptables.

En algunas situaciones, el reducir el riesgo a niveles aceptables puede no ser posible o representar un costo exageradamente elevado. En este caso, se aplicaría la estrategia de aceptación del riesgo.

3.3 ESTABLECIMIENTO DEL PLAN PILOTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

Con el análisis de las políticas de Seguridad Informática precedentes en el área de Networking se pudo determinar cuáles políticas están siendo aplicadas y cuáles podrían hacer falta. A continuación se establece el Plan Piloto de Políticas de Seguridad Informática PPPSI.

Se desarrolla cada ítem indicado en el literal anterior.

4. ANÁLISIS DE LA NORMA ISO/IEC 27002

4.1 DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

El desarrollo de las políticas de Seguridad Informática realizada en el área de Networking de la empresa Uniplex Systems S.A. se deriva del análisis del tratamiento del riesgo (en donde se califican los activos de información y se determina si se acepta, reduce, transfiere o evita el riesgo) versus el enunciado de aplicabilidad de los controles correspondientes a los tres dominios de la norma:

- Política de Seguridad Informática
- Aspectos Organizativos de la Seguridad Informática
- Gestión de Activos

Se detalla el proceso para crear o mejorar una política de Seguridad Informática.

4.2 REFERENCIAS FORMULACIÓN DE GUÍAS PARA DOCUMENTAR Y EVALUAR LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA DEL PPPSI

Para la formulación de guías para documentar y evaluar las políticas se tiene como referencia la siguiente pirámide de documentos (Gráfico 7), la pirámide consta de cuatro niveles en donde el nivel uno será el primer instructivo que debe realizarse y el cuarto será el último.

Se explica en más detalle cada nivel y la documentación entregable para el PPPSI.

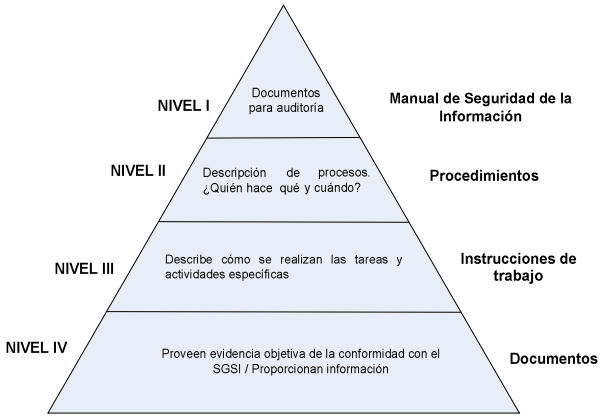

Gráfico 7. Pirámide de Documentos

4.3 MANUAL DE USUARIO PARA IMPLEMENTAR LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

En el anexo 4 se presenta una breve guía para los usuarios de Networking.

Esta guía brinda a los usuarios prácticos consejos para que protejan su información almacenada en medios informáticos y reduzcan los riesgos de perder la integridad, confidencialidad y disponibilidad de la misma.

4.4 COSTOS

Una vez concluida la implementación del Plan Piloto de Políticas de Seguridad Informática en el área de Networking de la empresa Uniplex Systems S.A. se presenta los costos referenciales.

Los costos se los ha dividido en dos grupos; costos de diseño y costos de implementación:

Los costos de diseño son (Tabla 3):

Costos de Diseño	Valor $
Norma ISO 27002	**33**
Costo Personal (cuatro meses)	**2000**
Cursos de Seguridad de la Información.	**300**
Otros	**200**
SUBTOTAL	**2533**

Tabla 3. Costos de Diseño

Los costos de implementación son (Tabla 4):

Costos de Implementación	$
*Costo de Software Whats Up	**0**
*Costo de Software Belarc	**0**
Disco Duro externo para respaldos.	**235**
Póliza de Seguro	**500**
Otros	**100**
SUBTOTAL	**835**[5]

Tabla 4. Costos de Implementación

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- En el área de Networking de la empresa Uniplex Systems S.A. se definieron los aspectos que involucran el Plan Piloto de Políticas de Seguridad Informática, la adopción de este Plan permitió establecer los aspectos que involucran una correcta Seguridad Informática. Se aplican programas de monitoreo, software para robustecer la infraestructura de la red.

- En el área de Networking de la empresa Uniplex S.A. se han especificado motivos principales por los cuales es necesario implementar políticas de Seguridad Informática, lo que fué objeto de análisis a través del desarrollo sistemático del Plan Piloto de Políticas de Seguridad Informática (PPPSI).

- En el área de Networking de la empresa Uniplex Systems S.A. se determinó el procedimiento que se consideró más conveniente para desarrollar políticas para la Seguridad Informática, corregir algunas y mejorar otras. No se desarrollan excesivas políticas de seguridad porque el plan piloto puede colapsar o ser rechazado por el exceso de normas aplicadas.

- En el área de Networking de la empresa Uniplex Systems S.A. se identificaron las falencias y fortalezas de las políticas de Seguridad Informática precedentes; con base a esto, se desarrollaron e implementaron mejores y nuevas Políticas de Seguridad Informática para el área.

- El propósito principal del Plan Piloto de Políticas de Seguridad Informática instaurado en el área de Networking de la empresa Uniplex Systems S.A. es disminuir el riesgo al cual están sujetos los activos de información en la empresa. El proceso para identificar los activos de información dentro del alcance del plan piloto es fundamental así como también lo es la evaluación de los riesgos de los activos.

- La GUÍA DE USUARIO instaurada en el área de Networking de la empresa Uniplex Systems S.A. es muy clara y específica, no da lugar a malos entendidos por parte de los usuarios del área. Además, se asignó responsabilidades y obligaciones de forma equitativa entre los miembros del área.

5.2 RECOMENDACIONES

- Se recomienda extender el modelo de políticas de Seguridad Informática desde el área de Networking a toda la empresa, por supuesto debe contar con el total apoyo de la gerencia y debe ser un objetivo planteado para la organización.

[5] La empresa Uniplex Systems S.A. al ser partner de algunos proveedores, puede utilizar software sin costo alguno.

- Se recomienda desarrollar y establecer un Sistema de Gestión de Seguridad de Información (SGSI) cuyo alcance es más extenso que el Plan Piloto de Políticas de Seguridad Informática (PPPSI) ya que involucra todos los once dominios de la norma, abarca todos los aspectos de seguridad de información que pueden ayudar a reducir aún más el riesgo con la información, con el fin de robustecer y hacer más confiable a la empresa.

- Se recomienda analizar las normas de la familia 27000 para mantener en mejoramiento continuo el Plan Piloto de Políticas de Seguridad Informática. En especial se recomienda revisar la Guía de Auditoría de un Sistema de Seguridad, porque este control debe ser implementado periódicamente.

- Debido a que la información es muy importante, se recomienda que las empresas capaciten personal referente a las normas de Seguridad de la Información, y no verlo como un gasto sino como una inversión ya que los beneficios obtenidos sobrepasan fácilmente a los costos de inversión.

BIBLIOGRAFÍA

- DESARROLLO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA E IMPLEMENTACIÓN DE TRES DOMINIOS EN BASE A LA NORMA 27002 PARA EL ÁREA DE HARDWARE EN LA EMPRESA UNIPLEX SYSTEMS S.A. EN QUITO.

- SEMINARIO ISO 27002 INTENSIVO. INFORMATION SECURITY INC. MEDIOS DIGITALES. 2007

- GUÍA PARA LA ELABORACIÓN DE POLÍTICAS DE SEGURIDAD. UNIVERSIDAD NACIONAL DE COLOMBIA. 2003.

- INFORMATION TECHNOLOGY – CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT. INTERNACIONAL STANDARD ISO/IEC 17790. FIRST EDITION, 2000.

- POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, DECISIÓN ADMINISTRATIVA. BUENOS AIRES, ARGENTINA 2004.

- POLÍTICA OFICIAL DE SEGURIDAD INFORMÁTICA DEL CENTRO DE INVESTIGACIÓN CIENTÍFICA Y DE EDUCACIÓN SUPERIOR DE ENSENADA. MÉXICO, MÉXICO 2001

- MODELO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA ORGANISMOS DE LA ADMINISTRACIÓN PÚBLICA. BUENOS AIRES, ARGENTINA 2001

- POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA UNA ENTIDAD FINANCIERA. CÓRDOVA EDITH. LIMA, PERÚ 2002.

- INTERNET: HTTP://WWW.ISO27000.ES

- INTERNET: HTTP://WWW.IPSWITCH.COM

- INTERNET: HTTP://NMAP.ORG

BIOGRAFÍA

Richard Eduardo Posso Guerrero

Nació en Quito, Ecuador, el 15 de julio de 1984. Obtuvo su bachillerato de Físico Matemático en el colegio Gonzaga.
Se graduó de Ingeniero en Electrónica y Telecomunicaciones, en Abril de 2009 en la Escuela Politécnica Nacional. Actualmente se encuentra laborando en la empresa Uniplex S.A. en el área de Networking.