PROYECTO FINAL

SEGURIDAD DE LA INFORMACION

CARLOS ARTURO BUITRAGO 122467

EDUARDO ROJAS ROMERO 122462

UNIVERSIDAD LIBRE CALI

FACULTA DE INGENIERÍA

INGENIERÍA EN SISTEMAS

SANTIAGO DE CALI

2012



PROYECTO FINAL

SEGURIDAD DE LA INFORMACION

CARLOS ARTURO BUITRAGO 122467

EDUARDO ROJAS ROMERO 122462

INTRODUCCIÓN A LA INGENIERÍA

GEREMÍAS GONZALEZ

INGENIERO

UNIVERSIDAD LIBRE CALI

FACULTA DE INGENIERÍA

INGENIERÍA EN SISTEMAS

SANTIAGO DE CALI

2012



### TABLA DE CONTENIDO

TEMA PÁGINA

1. INTRODUCCIÓN 1

2. PLANTEAMIENTO DEL PROBLEMA 2

2.1 SITUACION PROBLEMÁTICA 2

2.2 FORMULACION DEL PROBLEMA 2

3. MARCO TEORICO 3

3.1 ANALISIS Y GESTION DEL RIESGO 4

3.2 SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION 5

3.3 NORMA ISO/IEC 27002:2005 5

3.4 MAPA CONCEPTUAL 6

4. DIAGRAMA CAUSA-EFECTO 7

5. OBJETIVOS 8

5.1 OBJETIVO GENERAL 8

5.2 OBJETIVOS ESPECIFICOS 8

6. METAS 9

7. INDICADORES 10

8. CUADRO DE SOLUCIONES 11

8.1 ESTUDIO TECNICO – ECONOMICO 11

9. ACTIVIDADES 12

10. DIAGRAMA DE GANTT 13

11. VALORACION CUANTITATIVA Y CUALITATIVA 13

12. CONCLUSIONES 14

13. RECOMENDACIONES 15

14. REFERENCIAS URLGRAFICAS 16

### INTRODUCCION

Dentro del presente proyecto abarcaremos temas de seguridad informática, conocido como el conjunto de reglas, planes y acciones que permiten asegurar la información contenida en un sistema computacional, estableciendo algunas formas de control preventivo y correctivo que son necesarias a fin de lograr y tener seguridad de la información, cuando no se tiene implementado ningún sistema de seguridad informática en la estructura de una empresa.

1

### PLANTEAMIENTO DEL PROBLEMA

### 2.1 Situación problemática:

En la FCICN no hay políticas ni controles efectivos sobre la información de la organización, tampoco existe un plan de procedimientos internos para custodiar los datos, ni planes de acción para dar a entender la importancia del uso y salvaguarda de la información.

¿Cuál es la información más valiosa que manejamos?

* La información asociado a nuestros clientes.
* La información asociado a nuestras ventas.
* La información asociada a nuestro personal.
* La información asociada a nuestros servicios.
* La información asociada a nuestras operaciones.

¿Cuáles son los riesgos y amenazas que existen?

* La empresa necesita y debe contar con información de cada una de las áreas sobre la cual tomar decisiones a efectos de establecer controles necesarios y eficaces.
* Para esto es necesario proteger la información evitando fugas, ya que se ha presentado en algunas ocasiones el aparente “robo” y “borrado” de la información debido al retiro por parte de la organización de las personas encargadas de la misma.
* El uso de dispositivos extraíbles en los cuales pueden llevarse información valiosa.
* El acceso remoto mediante internet para realizar actividades por fuera del horario laboral.

¿Qué vulnerabilidades existen en la organización?

* Falta compromiso de la dirección.
* Personal no capacitado y concientizado.
* Inadecuada asignación de responsabilidades.
* Ausencia de políticas y procedimientos.
* Ausencia de controles (físicos / lógicos) (disuasivos / preventivos / de detección / correctivos)
* Ausencia de reportes de incidentes y vulnerabilidades.

### 2.2 Formulación del problema:

¿Cómo proteger la información en la FCICN?

No existen procesos ni procedimientos definidos para el manejo de la información en la FCICN.

2

### MARCO TEORICO

La seguridad informática nace a principios del siglo XIX conjuntamente con el avance tecnológico, en esta época solo se implementaba en organizaciones gubernamentales o para el ejercito, ya que los ataques en la guerras y para su comunicación era de suma importancia la información de las grandes naciones, es por ello que estallo todo lo referente a la computación.

Con el paso de los años fue evolucionando y su acceso ya no fue tan restringido, tanto la computación y la informática se empezaron a implementar en las grandes organizaciones, así mismo las actividades que se  realizaban en ellas ya no eran tan especificas, incluso se realizaban operaciones de planeación y de automatización de los datos.

La seguridad informática va adquiriendo una importancia creciente con el aumento del volumen de información importante que se halla en las computadoras distribuidas. En este tipo de sistemas resulta muy sencillo para un usuario experto acceder de forma no autorizada a datos de carácter confidencial.

Toda organización debe estar a la vanguardia de los procesos de cambio. Estas deben disponer de información continua y confiable en el tiempo, esto constituye una ventaja fundamental.

Como en todas las innovaciones se presentan los aspectos positivos y los aspectos negativos  ya que aunque la tecnología es buena porque reduce mucho esfuerzo, también produce muchas confusiones aun más cuando no se implementa correctamente, es por ello que nace la Seguridad Informática, puesto que por medio de las computadoras se maneja toda la información de las empresas.

Dentro del marco teórico se debe contemplar lo que es en si la seguridad de la información y sus características, llevar a cabo un análisis de gestión y riesgo, definir en sí que es un sistema de seguridad de la información detallando una normatividad a seguir y por último la metodología a utilizar.

La información es un activo que como otros activos importantes tiene valor y requiere en consecuencia una protección adecuada. Esta información puede estar impresa o escrita en papel (archivo físico), almacenada electrónicamente (medios extraíbles o fijos), trasmitida por correo o medios electrónicos (mail), mostrada en filmes (microfilmada) o hablada en conversación (grabaciones).

Debe protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparte o almacene.

3

La seguridad de la información se caracteriza por tres aspectos muy importantes:

* **Confidencialidad**, asegurando que sólo quienes estén autorizados pueden acceder a la información.
* **Integridad**, asegurando que la información y sus métodos de proceso son exactos y completos.
* **Disponibilidad**, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

****

### 3.1 ANALISIS Y GESTION DEL RIESGO

Es el uso sistemático de la información para identificar amenazas y coordinar las actividades para dirigir y controlar la organización con relación al riesgo. Se persigue identificar los sectores más vulnerables de la organización y permitir concentrar los esfuerzos de control en los lugares críticos.

La terminología a definir y utilizar para este análisis es la siguiente:

**Activo:** Cualquier cosa - tangible o no - que tenga valor para la organización.

**Vulnerabilidad:** Debilidad de un activo que puede ser explotada por una amenaza.

**Amenaza:** Causa potencial de un incidente no deseado, que podría dañar uno o más activos.

**Control ó Salvaguarda:** Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales.

**Riesgo:** Combinación de la probabilidad de materialización de una amenaza y el daño que produciría sobre un activo.

### 4

### 3.2 SGSI

En este orden de ideas podemos decir que un SGSI (Sistema de Gestión de Seguridad de la Información) consiste en la planificación, ejecución, verificación y mejora continua de un conjunto de controles que permitan reducir el riesgo de sufrir incidentes de seguridad.

### 3.3 Norma ISO/IEC 27001:2005

Es una metodología que se establece las especificaciones para un SGSI, con el fin de garantizar que los riesgos son conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, continua, repetible y eficiente.

Es un “Código de Buenas Prácticas” para la Seguridad de la Información, que establece cientos de controles y mecanismos de control, los cuales pueden ser implementados y posteriormente chequeados por la norma ISO/IEC 27001:2005

****

5

### 3.4 MAPA CONCEPTUAL

### C:\Users\user\Dropbox\Introduccion A Ingenieria\SGSI\SEGURIDAD INFORMATICA CMAP.jpg

### 6

### DIAGRAMA CAUSA EFECTO



En la imagen  encontramos el diagrama Causa Efecto sobre el problema de seguridad de la FCICN. En él podemos observar las causas que han ocasionado que exista un problema de seguridad de la información en cuanto a la información manejada, ya que no se han realizado los controles suficientes y tampoco se han aplicado políticas de seguridad informática.

Como causa raíz se detecto como la falta de un sistema de SGSI, ya que la empresa no cuenta con un sistema donde se pueda hacer un control y test constante sobre la información que se maneja a diario y hacer esta gestión manualmente sería muy desgastante y dispendioso para las personas que se asignaran para realizar esta labor.

7

### OBJETIVOS

### 5.1 OBJETIVO GENERAL

* Mejorar los procesos de uso y salvaguarda de la información de la FCICN con base a las necesidades y capacidades de la organización.

“El objetivo de este proyecto se debe llevar a cabo teniendo en cuenta la viabilidad técnica, operativa y económica en acuerdo a estándares y necesidades de la organización, proporcionando conocimientos técnicos, teóricos y prácticos requeridos, además de preparar todo el personal con capacitaciones teórico practicas para crear conciencia de lo importante del uso y buen manejo de la información con el fin de garantizar la confidencialidad, integridad y disponibilidad de la misma en la organización”.

### 5.2 OBJETIVOS ESPECIFICOS

1. Conocer la situación actual de la FCICN en relación al manejo de la Información, evaluando su nivel actual.
2. Determinar la capacidad técnica, operativa y económica para establecer procesos que mejores el manejo de la Información en la FCICN.
3. Generar informes sobre el tráfico de la información para detectar las fallas que se presentan en el proceso y corregir los errores que se presenten por mal manejo.
4. Implementar procedimientos de manejo de la Información basados en estándares de normas internacionales teniendo en cuenta las necesidades y capacidades de la FCICN.

### 8

### METAS

1. Hacer un inventario detallado de equipos de computo (servidores, estaciones, otros), clasificarlos según área, importancia y función, tiempo de adquirido y la vigencia del software/hardware.
2. Instalar y/o actualizar programas antivirus en cada equipo de cómputo verificando su correcto funcionamiento.
3. Instalar un servidor de dominio para el control de acceso a la red interna con autenticación de usuarios.
4. Generar informes sobre el tráfico de información para evaluar el nivel de buen uso de la misma en la organización.
5. Detectar y corregir las fallas en el manejo de la información dentro y fuera de la organización.
6. Implementar procesos de manejo de la Información basados en la Norma 27001.
7. Hacer capacitaciones sobre el manejo de la información con todo el personal para enseñar su buen uso y cuidado de ella. Se dividen en grupos administrativo, asistencial primario, asistencial secundario y operativo.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Meta** | **Objetivo Especifico** | **Proceso** | **Magnitud** | **UM** | **Descripción** | **Jul. /12** | **Ago. /12** | **Sep. /12** | **Oct. /12** |
| 1 | 1 | Inventariar | 175 | Equipo | Detalle de los equipos de computo existentes | 175 |  |  |  |
| 2 | 2 | Instalar y/o Actualizar | 175 | Equipo | Software antivirus y S.O. | 88 | 87 |  |  |
| 3 | 2 | Instalar | 1 | Servidor | Dominio control acceso a usuarios en la red. | 1 |  |  |  |
| 4 | 3 | Generar | 20 | Informe | Sobre tráfico de información y nivel de buen uso | 5 | 5 | 5 | 5 |
| 5 | 3 | Detectar y corregir | 120 | Días | Fallas de seguridad en manejo de la información | 30 | 30 | 30 | 30 |
| 4 | 4 | Capacitar | 238 | Persona | Enseñar uso, custodia de la información | 60 | 85 | 63 | 30 |
| 5 | 4 | Implementar | 4 | Acción | Norma internacional 27001 | 1 | 1 | 1 | 1 |

9

### INDICADORES

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nombre del Indicador** | **Formula del Indicador** | **Estado Inicial** | **Valor Esperado** | **Periodo** |
| % de acciones implementadas | (# de acciones implementadas/ total de acciones) \* 100 | 0% no se había hecho antes implementación de la norma ISO 27001 | 100% logrado de implementar las acciones de la norma | 4 meses |
| % de equipos actualizados | (# de equipos actualizados/ total de equipos) \* 100 | Se inicia con un 50% de los equipos actualizados | 100% de los equipos actualizados e instalados | 4 meses |
| % de fallas corregidas | (# fallas corregidas/ total fallas detectadas) \* 100 | 0% no se había hecho esta medición antes | 100% de las fallas importantes sean corregidas | 4 meses |
| % de personas capacitadas | (# personas que asisten a capacitación/ total de personas a capacitar) \*100 | 0% no se había realizado estas capacitaciones nunca antes | 100% de las personas de la organización estén capacitadas | 4 meses |
| Calificación promedio de la evaluación | Suma de calificación de las evaluaciones/ # personas evaluadas | 0 porque es la primera evaluación que se va a realizar | 4 puntos en una escala de 1 a 5 siendo 1 muy malo y 5 excelente | 4 meses |
| % detecciones documentadas | (# detecciones documentadas/ total detecciones) \* 100 | 0% no se había realizado reporte de detecciones ni su documentación | 100% de detecciones documentadas | 4 meses |

10

### CUADRO DE SOLUCIONES

### 8.1 ESTUDIO TECNICO - ECONOMICO

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Componente | Unidad Medida | Cantidad | Costo Unitario | Costo Total |
| Adecuación | Equipos a instalar licencias | 175 | $41.760 | $7’308.000 |
| Administración | Soporte Externo mensual | 12 | $400.000 | $4’800.000 |
| Capacitación | Personal de la organización y encargados de sistemas. | 238 | $0Está incluido en el soporte y licencias | $0 |
| Dotación | Mejora de equipos obsoletos | 22 | $1’400.000 | $30’800.000 |

### 11

### ACTIVIDADES

Para la ejecución del proyecto se presenta a continuación:

**Actividad 1**

Apropiar el conocimiento en sistemas de gestión de seguridad de la información y de los mecanismos existentes para la detección de intrusos.

**Actividad 2**

Simular tipos de ataques más frecuentes que pongan en riesgo la seguridad de un sistema o una red a fin de tener mejores fundamentos en la creación de políticas y procedimientos o en la mejora de ellos.

**Actividad 3**

Aplicar los controles de la norma ISO que permitan administrar un sistema de detección de fallas dentro de un sistema de gestión de seguridad de la Información.

**Actividad 4**

Evaluar las herramientas de software para sistemas gestión de seguridad Informática existentes en el mercado actualmente.

**Actividad 5**

Desarrollar módulos de software para la redacción, mejora y almacenamiento persistente de políticas de seguridad de la información.

**Actividad 6**

Elaborar la documentación que identifique los fundamentos básicos para el desarrollo de estrategias de seguridad de la información, basado en las normas

Internacionales y las necesidades de la organización.

12

### DIAGRAMA DE GANTT

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Actividad** | **Julio 2012** | **Agosto 2012** | **Septiemb 2012** | **Octubre 2012** |
| **semana** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | **4** |
| 1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

### VALORACION CUANTITATIVA Y CUALITATIVA

SEGÚN EL CUADRO DE SOLUCIONES

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CRITERIO SOLUCION** | **1 FISICO** | **2 TECNICO** | **3 COSTOS** | **4 TIEMPO** | **5 HUMANO** | **TOTAL** |
| **A** | 4 | 5 | 3 | 4 | 3 | 3.8 |
| 20% | 30% | 15% | 20% | 15% | 100% |
| **B** | 3 | 5 | 4 | 4 | 3 | 3.8 |
| 15% | 30% | 20% | 20% | 15% | 100% |
| **C** | 4 | 5 | 3 | 4 | 3 | 3.8 |
| 20% | 30% | 10% | 20% | 20% | 100% |
| **D** | 5 | 5 | 3 | 3 | 5 | 4.2 |
| 20% | 20% | 15% | 15% | 30% | 100% |

Valoración Cuantitativa (escala de calificación)

1. Deficiente
2. Bajo
3. Intermedio
4. Alto
5. Superior

13

### CONCLUSIONES

Actualmente en la sociedad de la información es necesario que todas las organizaciones sin tener en cuenta su tamaño implementen mecanismos que permitan mantenerla segura, donde se usen normas internacionales como un sistema principal basado en procesos que busca garantizar la seguridad de la información.

La metodología de un Sistema de Gestión de Seguridad de la Información SGSI permite descubrir los puntos vulnerables de una organización y provee herramientas valiosas para diseñar procesos y procedimientos de seguridad eficaces.

Es de vital importancia involucrar a todas y cada una de las personas que conforman el recurso humano de la organización en todos los procesos de la implementación del plan de Seguridad de la Información y que conozcan los beneficios del buen manejo y aplicación de ellos en sus labores.

Con una herramienta de análisis y gestión del riego AGR sólida y bien implementada se pueden producir resultados comparables y repetibles en el tiempo para evitar futuras fallas en el sistema de seguridad de la información que se haya adoptado por parte de la organización.

14

### RECOMENDACIONES

Se deben tomar acciones inmediatas para gestionar los riesgos que existen en el manejo de la información, además de disponer de planes de contingencia ante incidentes que se presenten fuera de lo previsto ya que todas las acciones deben ser proactivas y no reactivas.

Establecer formalmente un plan propuesto para comenzar a corregir las fallas en el manejo de la información y designar una persona que esté a la cabeza y encargada de la seguridad de la información del FCICN.

Implementar los planes y proyectos para el tratamiento de los riesgos detectados en el manejo de la información, para que una vez ganada la experiencia, no se deje decaer la aplicación en ninguna de las unidades de la organización.

Profundizar en el desarrollo de herramientas de análisis y gestión de riesgos AGR utilizando sistemas expertos, estudiando de políticas, metas, indicadores y técnicas para la determinación de la eficacia de los procesos y procedimientos adoptados para el manejo de la información.

Continuar con la realización de las auditorias constantes para hacer el seguimiento al manejo de la información, además de brindar al área de sistemas los recursos necesarios que permitan mantener en un alto nivel de seguridad en la organización en cuanto a informática se refiere.

Continuar con las capacitaciones y la concientización de todas las personas de la organización para que se sientan comprometidos y continúen involucrados con el desarrollo y aplicación de los procesos sugeridos en el plan de seguridad de la información.

### 15

### 14. REFERENCIAS

 [1] Network Working Group, “Site Security Handbook” , Request for Comments 2196,

Septiembre 1997.

[2] Instituto Argentino de Normalización, “Código de práctica para la administración de

la seguridad de la información”, IRAM-ISO IEC 17799, Buenos Aires, febrero 2002.

[3] Coordinación de Emergencia en Redes Teleinformáticas de la Administración

Pública Argentina, Manual de Seguridad en Redes.

[4] Jesús Herney Cifuentes, César Augusto Narváez, Manual de detección de

vulnerabilidades de sistemas operativos UNIX en redes TCP/IP, Universidad del

Valle 2004.

[5] Gustavo Adolfo Barreto, Estudio de seguridad en computadoras con sistemas

operativos UNIX conectados a una red TCP/IP, Universidad del Valle 2001.

[6] Liliana Rojas, Humberto Campiño, Seguridad en transacciones con base de datos

a través de una página web, Universidad del Valle 2002.

[7] Oscar Javier Dorado, Implementación de un algoritmo para mejorar la seguridad

de un sitio web utilizando una técnica de criptografía en una arquitectura de

interfaz CGI, Universidad del Valle 2001.

[8] Charles Davis, Eric Lakin, “Hasta las Pymes son Hacheadas”, Exposición en el

Congreso Internacional en Seguridad TI Informática H@cker Halted 2005.

[9] McAfee, “Estudio de criminología virtual McAfee”, Julio 2005, disponible en:

http://www.mcafeesecurity.com/us/local\_content/misc/mcafee\_na\_virtual\_criminol

ogy\_report.pdf

[10] GNU Free Documentation License, “UNIX“, disponible en :

http://es.wikipedia.org/wiki/Unix

[11] GNU Free Documentation License, " familia de protocolos de Internet",

http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml

[12] Monografías online, “CGI Master”, disponible en: http://www.ok.cl/cgi/chap0/.

16