UNIVERSIDAD Rafael Belloso Chacín

Revista Electrónica de Estudios Telemáticos

TÉLÉMATIQUE

AUDITORIA DE SEGURIDAD
CASO: PLATAFORMA TELEMÁTICA DE LA REDFEC – LUZ

David Rodolfo Bracho Rincón*
Universidad del Zulia - Venezuela
Correo electrónico: drbracho@luz.edu.ve

Neif Guzmán Silva Valero*
Universidad del Zulia - Venezuela
Correo electrónico: nsilva@luz.edu.ve

RESUMEN

La presente investigación evaluó la seguridad telemática que ofrece la red de voz, datos y video de la Facultad Experimental de Ciencias (FEC) de la Universidad del Zulia (LUZ). Se realizó una Auditoria de Seguridad al servicio Telemático, de Tipo Interna, sobre el área donde es administrado y distribuido el servicio principal de la RedFEC: el Edificio Grano de Oro. Se utilizó como punto de partida el Informe generado por la Unidad de Servicios Computacionales y Telemáticos de la FEC, que trata sobre la situación actual de la misma, comprendida para el período 2004 - 2006. La metodología utilizada fue la de Piattini y Del Peso, aplicando como instrumento de recolección, entrevistas estructuradas a los responsables de cada área física que tienen presencia en el Edificio Grano de Oro. Se aplicó el enfoque aportado por la norma ISO 17799 – 2005, abarcando los 10 dominios de control: Políticas de seguridad; Estructura organizativa; Clasificación y control de activos; Seguridad relacionada con el personal; Seguridad física y del entorno; Gestión de comunicaciones y operaciones; Control de accesos; Desarrollo y mantenimiento de sistemas; Gestión de continuidad de negocio; Conformidad. El instrumento de evaluación asoció los 10 dominios de control con las 8 zonas de servicios: Cumplimiento de normas y estándares; Sistemas operativos; Software; Comunicaciones y redes; Base de datos; Procesos; Aplicaciones; Física. Esta asociación fue una variante del modelo propuesto por Silva y Bracho, como metodología de selección de herramientas colaborativas. Los resultados obtenidos mostraron que la seguridad ofrecida sobre el cumplimiento de los distintos elementos a proteger de los servicios que son administrados desde y hacia el Edificio Grano de Oro fue del 75,14%. Finalmente se expuso un plan de acción que permite corregir y prevenir potenciales problemas en el corto, mediano y largo plazo.

Palabras clave: Auditoria; Seguridad; Telemática; RedFEC; ISO 17799-2005;

ABSTRACT

The present study evaluated the telematic safety that offers the voice, data and video network of the Experimental Faculty of Science (FEC) at the University of Zulia (LUZ). We performed an internal security auditory of the Telematic Service, on the area where it is managed and distributed the main service of RedFEC: Grano de Oro

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

Building. A report generated by the unit of Computer Services and Telematics of the FEC was used as starting point, which focuses on the current status of the network, including the period from 2004 to 2006. The PIATTINI and DEL PESO methodology was used, applying as recollection tool, structured interviews with the heads of each area that have physical presence in Grano de Oro Building. An approach provided by ISO 17799-2005 was applied, covering 10 domains of control: Security policies, organizational structure, classification and control of assets; Security-related personnel; Physical and environmental security, management and communications operations; Access Control; Development and maintenance of systems; Management Business continuity; Compliance. The assessment tool partnered the 10 domains of control with 8 service areas: Compliance with regulations and standards; OS, Software, Communications and networking; Database; Processes; Applications; Physics. This association was a variant of the model proposed by BRACHO and SILVA, as a methodology for selecting collaborative tools. The results showed that the security offered based on the compliance of the different elements to protect the services that are administered from and to the Grano de Oro Building was 75.14%. Finally, a plan of action was exposed that enables to correct and prevent potential problems in the short, medium and long term.

Key Words: Audit; Security; Telematics; RedFEC; ISO 17799-2005;

*Unidad de Redes e Ingeniería Telemática. Departamento de Computación. Facultad Experimental de Ciencias. Universidad del Zulia. Teléfono: (0261)-7597748. Fax: (0261) 7597735. Correo electrónico: drbracho@luz.edu.ve Maracaibo, Venezuela. 4001

Consejo Central de Pregrado. Vicerrectorado Académico. Universidad del Zulia. Teléfono: (0261)-7596824. Fax: (0261) 7596825. Correo electrónico: nsilva@luz.edu.ve. Maracaibo, Venezuela. 4001

INTRODUCCIÓN

La Universidad del Zulia, como institución de educación superior pública, inició un proceso de adecuación tecnológico, específicamente en cuanto al servicio telemático en el año 2001 con la consolidación de la RedLUZ, acercando a su comunidad a ésta por medio de la puesta en marcha de servicios telemáticos innovadores y de vanguardia dirigidos a atender la investigación, docencia, extensión y administración a un público tan diverso como lo son: estudiantes, personal docente y de investigación, administrativo, obrero y público en general.

La RedLUZ es la red de voz, datos y video que sirve a todo el campus universitario de LUZ, conformadas por núcleos que sirven a zonas específica, encontrándose la RedFEC como uno de esos núcleos y es a su vez quien provee de servicio de datos, voz y video a la comunidad que hace vida en la Facultad Experimental de Ciencias.

Según Acurero y Ferrer (2007) la RedFEC posee una topología tipo estrella extendida cuyo nodo principal esta ubicado en TV-Educativa, el cual suministra

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

señal a los siguientes segmentos: Módulo 1, Módulo III y Grano de Oro; que a su vez distribuyen a otros segmentos secundarios: Módulo II, Secretaría Docente, FORGAD, Bienes, Bloque A1 y Bloque A2.

Los objetivos fundamentales de la RedFEC son:

- Brindar soporte a nivel de cómputo científico intensivo, comunicación y procesamiento electrónico de textos e imágenes (estáticas y dinámicas), el tratamiento analítico, numérico y/o simbólico de funciones y ecuaciones matemáticas en general y el desarrollo de visualización gráfica de alta resolución.
- Incorporar nuevas tecnologías de "Software y Hardware" requeridas en Redes de Computación.
- Persigue la formación del personal técnico apropiado para la gerencia y administración de redes de computación con orientación científica.

Otros objetivos generales como son:

- Adecuar el buen funcionamiento de los mismos al cumplimiento de un marco legal que regula el ámbito de las Tecnologías de Información, como lo son: Ley Orgánica de Ciencia y Tecnología, Ley de Mensaje de Datos y Firmas Electrónicas, Decreto Uso de Software Libre en la Administración Pública, Decreto 825.
- Integrar la plataforma a proyectos nacionales de VoIP, Internet2, gobierno electrónico, entre otros.

Sin embargo, problemas propios y derivados inciden en la seguridad, eficiencia y cumplimiento de los objetivos anteriormente mencionados. Entre los problemas propios se cuenta con: áreas físicas no integradas a la RedLUZ, equipos obsoletos, aplicaciones heterogéneas incompatibles, servicios telemáticos que consumen demasiados recursos computacionales, migraciones y crecimiento no planificado, son factores que han contribuido la exposición de la misma y entre los problemas derivados se tiene: subordinación a una estructura superior administrativa (RedLUZ) que limita la capacidad de respuesta ante situaciones de mantenimiento planificados, no planificados y planes de contingencia.

Adicionalmente se cuenta con una serie de razones que fueron identificadas por Acurero y Ferrer (2007):

- Áreas sin servicios que requieren de la distribución de la RedLUZ.
- La administración de los equipos activos de la RedFEC es responsabilidad del personal de Telecomunicaciones adscrito a RedLUZ.
- Tener una visión distinta a las autorizadas por la Facultad Experimental de Ciencias y de la Universidad del Zulia.

Buandes (2002) por su parte, expone otra serie de razones que pueden catalogarse como de generales:

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

- Síntoma de inseguridad orientado hacia la evaluación del nivel de riesgos asumido.
- Síntoma de descoordinación y desorganización al no coincidir los objetivos telemáticos e informáticos de la RedLUZ con los de la RedFEC.
- Estándares de productividad desviados sensiblemente de los promedios conseguidos habitualmente.
- Síntoma de debilidad económico - financiero básicamente como consecuencia de la ausencia total de un plan estratégico informático que contribuya a la sustitución o adecuación oportuna de los equipos o software de la organización.

La realización de auditorias son muy comunes en organizaciones, empresas, instituciones que desean conocer el cumplimiento de los objetivos estratégicos y operacionales propuesto con la situación actual, así como medir si la función del servicio telemático fue, es y será seguro, incluso desde el punto de vista de rentabilidad.

La importancia que ha adquirido la RedFEC en los últimos años como consecuencia de la cantidad de servicios que por ella transitan y la dependencia de los usuarios de éstos, hace oportuno realizar una auditoria de seguridad telemática que comprendió no sólo la evaluación de los equipos de cómputo y transmisión, de un sistema o procedimiento específico, sino que evaluó los sistemas telemáticos en general desde sus entradas, procedimientos, controles, archivos, obtención de información y en especial de la seguridad que brinda, en el área de mayor relevancia, como lo es el Edificio Grano de Oro.

Para el caso de auditoría a realizar a la RedFEC, resultó conveniente aplicar la metodología de Piattini y Del Peso (2001), haciendo uso de la norma ISO 17799 – 2005 ya que ésta contempla de forma integral todos los elementos de la seguridad relevantes dentro de una organización, la cual a su vez depende significativamente del servicio telemáticos, utilizando como instrumento de evaluación una adaptación de contenido en la metodología de Bracho y Silva (2007) y como instrumento de recolección de datos la encuesta.

Finalmente, la estructuración de los aportes de este artículo está apoyada en una revisión documental que permitió utilizar una metodología que utiliza un modelo de métrica que consideró los factores particulares de la RedFEC. Este trabajo concluye con una visión general sobre la seguridad en la RedFEC y del plan de mejoras como instrumento de control gerencial y pretende convertirse en una guía de referencia para desarrollo de nuevas auditorias, sirve de divulgación y transferencia de conocimientos a través de la línea de investigación Gestión del Riesgo Telemático.

AUDITORIA TELEMÁTICA

Dentro del ciclo de vida de los sistemas y servicios telemáticos, sobresalen los procesos principales, los de la organización y los de soporte. Dentro de los procesos de soporte se encuentra la auditoría. A continuación se define y tipifica el tipo de

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

auditoria; la norma ISO 17799 – 2005, metodología, instrumento de evaluación y modelos de encuestas.

1.- Definición y Tipo de Auditoria

Según Buandes (2002) la auditoria temática es el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control, eficacia, seguridad y adecuación del servicio telemático en la empresa, por lo que comprende un examen metódico, puntual y discontinuo del servicio telemático, con vistas a mejorar en cuanto a: rentabilidad; seguridad y eficacia.

Martínez (2001) por su parte indica que la auditoria de seguridad telemática es de tipo interna, ya que tiene como función principal la evaluación y revisión de los sistemas y actividades que se dan en la organización desde el punto de vista de "Control Gerencial", verificando y comprobando que las directrices y políticas que emanan de la dirección se están aplicando y de forma correcta.

La auditoria de seguridad telemática aplicada a la RedFEC es de tipo interna, puesto que prevé revisar la función y el cumplimiento de las directrices que se emanan desde la RedLUZ hacia la RedFEC y viceversa.

Martínez (2001) expresa que la seguridad de los sistemas de Información, se define como la doctrina que trata de los riesgos informáticos – telemáticos, entonces, la auditoría es una de las figuras involucradas en este proceso de protección y preservación de la información y de sus medios de proceso y transmisión.

Continúa Martínez (2001) diciendo que los niveles de seguridad informática en una entidad es un objetivo a evaluar y está directamente relacionado con la calidad y eficacia de un conjunto de acciones y medidas destinadas a proteger y preservar la información de la entidad y sus medios de proceso.

Los elementos a considerar según MARTÍNEZ (2001) son:

- Amenaza: Una persona o cosa vista como posible fuente de peligro.
- Vulnerabilidad: La situación creada, por falta de uno o varios controles, con la que amenaza pudiera acaecer.
- Riesgo: La probabilidad de que una amenaza llegue a acaecer por una vulnerabilidad
- Exposición o impacto: La evaluación del efecto del riesgo.

Como elementos complementarios, PIATTINI y DEL PESO (2001) clasifica los riesgos según la afectación que generan sobre los datos, siendo los siguientes: errores de manipulación; fraudes intencionados; sabotajes; filtraciones; desastres naturales; accidentes generados por el entorno, y la forma de presentarse puede ser: evitados, transferidos, reducirlos o asumirlos.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

Por su parte, Echenique (2001) indica que se deben considerar la existencia de cinco (5) factores que han permitido el incremento en lo crímenes por computadoras:

- El aumento del número de personas que estudian computación o carreras afines.
- El aumento del número de empleados que tienen acceso a los equipos de computación.
- La facilidad del uso de los equipos de cómputo.
- El incremento en la concentración del número de aplicaciones y consecuentemente, de la información.
- El incremento de redes y de las facilidades para utilizar las computadoras en cualquier sitio y tiempo.

2.- Norma ISO 17799 - 2005

Según Alexander (2005) la norma ISO 17799 – 2005, está orientada a establecer un sistema gerencial que permita minimizar el riesgo y proteger la información en las empresas, de amenazas externas o internas.

Continua Alexander (2005) afirmando que la norma ISO 17799 – 2005, hace énfasis particular en la información, ya que, esta es vista como un activo, que como otros importantes activos del negocio, tiene valor para una empresa y consecuentemente requiere ser protegida adecuadamente. Igualmente, procura establecer mecanismos de seguridad de información, ya que se orienta a determinar qué requiere ser protegido y por qué, de qué debe ser protegido y cómo protegerlo.

Por otra parte Villalón (2004) completa la información anteriormente suministrada al indicar que la norma ISO 17799 – 2005, establece diez dominios de control que cubren por completo la gestión de la seguridad de la Información.

- **Política de seguridad:** Dirige y brinda soporte a la gestión de la seguridad de la información. Se mide a través de: documento de política y revisión y evaluación.

- **Aspectos organizativos para la seguridad:** Gestiona la seguridad de la información dentro de la organización; mantiene la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización que son accedidos por terceros; mantiene la seguridad de la información cuando la responsabilidad de su tratamiento se ha externalizado a otra organización. Se mide a través de: infraestructura de seguridad de información; seguridad en accesos de terceras partes y externalización.

- **Clasificación y control de activos:** Mantiene una protección adecuada sobre los activos de la organización; asegura un nivel de protección adecuado a los activos de información. Se mide a través de: responsabilidades sobre los activos y clasificación de la información.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

- **Seguridad ligada al personal:** Reduce los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios; asegura 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; minimiza los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos. Se mide a través de: seguridad en la definición de los puestos de trabajo; capacitación de los usuarios y respuesta ante incidentes de seguridad.

- **Seguridad física y del entorno:** Evita accesos no autorizados, daños e interferencias contra los locales y la información de la organización; evita pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización; Previene las exposiciones a riesgo o robos de información y de recursos de tratamiento de información. Se mide a través de: áreas seguras; seguridad de los equipos y controles generales.

- **Gestión de comunicaciones y operaciones:** Asegura la operación correcta y segura de los recursos de tratamiento de información; minimiza el riesgo de fallos en los sistemas; protege la integridad del software y de la información; mantiene la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación; asegura la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo; evita daños a los activos e interrupciones de actividades de la organización; previene la pérdida, modificación o mal uso de la información intercambiada entre organizaciones. Se mide a través de: procedimientos y responsabilidades; planificación del sistema; gestión de respaldos; protección de código malicioso; gestión de redes; uso y seguridad de soportes e Intercambios de información.

- **Control de accesos:** Controla los accesos a la información; evita accesos no autorizados a los sistemas de información; evita el acceso de usuarios no autorizados; Protege los servicios en red; evita accesos no autorizados a ordenadores; evita el acceso no autorizado a la información contenida en los Sistemas; detecta actividades no autorizadas; garantiza la seguridad de la información cuando se usan dispositivos de informática móvil y teletrabajo. Se mide a través de: requerimientos; gestión de acceso usuarios; responsabilidad usuarios; control de acceso a la red; control de acceso al sistema operativo; control acceso a aplicaciones; seguimiento de accesos y usos e Informática móvil y teletrabajo.

- **Desarrollo y mantenimiento de sistemas:** Asegura que la seguridad está incluida dentro de los sistemas de información; evita pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones; protege la confidencialidad, autenticidad e integridad de la información; asegura que los proyectos de Tecnología de la Información y las actividades complementarias son llevadas a cabo de una forma segura; mantiene la seguridad del software y la información de la aplicación del sistema. Se mide a través de: requerimientos de seguridad; seguridad en aplicaciones; controles criptográficos; seguridad de ficheros sistema; seguridad desarrollo y soporte.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

- **Gestión de continuidad del negocio:** Respuesta a la interrupción de actividades del negocio y protege los procesos críticos frente grandes fallos o desastres. Se mide a través de: proceso de la gestión de continuidad; análisis de impacto; plan de Contingencia (PNC); planificación PNC; pruebas y mantenimiento PNC

- **Conformidad con la legislación:** Evita el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad; garantiza la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma; maximiza la efectividad y minimizar la interferencia de o desde el proceso de auditoría de sistemas. Se mide a través de: cumplimiento de los requerimientos legales; revisiones de la política de seguridad y de conformidad técnica; consideraciones sobre la auditoría de sistemas.

De estos diez (10) dominios se derivan treinta y seis (36) objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y ciento veintisiete (127) controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo).

3.- Metodología

Se utilizó la metodología de Piattini y Del Peso (2001) como enfoque genérico, aplicando para ello la norma ISO 17799 – 2005 como parte de los elementos a ser evaluados. Al mismo tiempo, se usó una adaptación del modelo de instrumento de evaluación propuesto en la metodología de Bracho y Silva (2007) para la medición de los valores. Se aplicaron como técnicas de recolección de información: entrevistas estructuradas, revisión de documentos, entre otros.

El área objeto de estudio fue la seguridad y contándose únicamente con una (1) sola área física auditada, la cual fue el Edificio Grano de Oro.

3.1.- Metodología de PIATTINI

La metodología de Piattini y Del Peso (2001), consiste en identificar la existencia de unos controles establecidos o estandarizados, evaluando el riesgo potencial existente como consecuencia de la ausencia de controles o deficiencia de los sistemas. Estos riesgos deberán ser cuantificados y valorados, de forma tal que, permitan determinar el nivel de fiabilidad que ofrece el sistema sobre la exactitud, integridad y procesamiento de la información, para ello se aplica las técnicas de control que deben minimizar e riesgo, orientadas a las entradas, procesos y salida. Estás técnicas pueden ser: entrevistas, revisiones de documentos, evaluación de riesgo y controles, pruebas de cumplimientos, entre otras. Seguidamente se deben realizar pruebas, las cuales están orientadas a la obtención de evidencias, que deben validarse sobre la base de los siguientes propiedades: pertinencia, fehaciente, verificable e interrelacionadas con otros resultados. Finalmente se deben concluir los resultados sobre la base de los resultados obtenidos.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

Piattini y Del Peso (2001), propone que todo sistema puede ser evaluado en función de los siguientes componentes:

- Normas y estándares.
- Sistemas Operativos.
- Software.
- Comunicación y Redes.
- Base de Datos.
- Procesos.
- Aplicaciones.
- Física.

3.2.- Adaptación del Modelo de Instrumento de Evaluación de la Metodología de Bracho

La adaptación contempló establecer una matriz para la cual las categorías en el modelo original fueron adaptadas por los componentes que la metodología de PIATTINI indica, e identificadas ahora como segmentos, quedando conformada la matriz por ocho (8) segmentos. Los segmentos debieron ser ponderados en importancia utilizando un máximo de cien (100) para distribuir entre ellos. Cada segmento se dividió en subcategorías, tal cual como fue planteado en el modelo original, sin embargo, fueron adaptadas por los diez (10) dominios de control, identificados ahora como secciones. Las secciones fueron ponderadas sobre un máximo de veinte (20) puntos para distribuir entre ellas.

Cada sección posee varios ítems que fueron valorados en un rango de cero (0) puntos (ausencia total) a cinco (5) puntos (presencia absoluta). La suma total de los puntajes correspondientes a los ítems de cada sección (a) se divide entre el valor máximo posible a obtener en cada una de ella (b).

De esto se obtiene un valor proporcional entre 0 y 1 (c). Este resultado se multiplica por el valor ponderado asignado a la sección (d). Luego, se calcula la sumatoria de los valores (e) de cada sección y se divide entre el valor máximo ponderado para las secciones veinte (20), de lo cual se obtiene (f). Seguidamente se multiplica el valor (f) por el valor de ponderación de cada segmento, obteniendo así el valor (g).

Para obtener el valor final se debió calcular el promedio aritmético entre los valores (g) de cada segmento.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

Tabla N°1 Instrumento de Evaluación

Segmentos y Secciones	(a) Σ Ítems Subcategoría	(b)Máximo por Subcategoría	(c) = a/b Proporción	(d) Ponderación	(e) = (c)*(d)	(f) = Σ (e)/20	(g) = (f)*(d)/100
Normas y estándares • Política de seguridad de la información • Estructura organizativa • Clasificación y control de activos • Seguridad relacionada con el personal • Seguridad física y del entorno • Gestión de comunicaciones y operaciones • Control de accesos • Desarrollo y mantenimiento de sistemas • Gestión de continuidad de negocio • Conformidad **Sistemas Operativos** • Ídem anterior. **Software** • Ídem anterior. **Comunicación y Redes** • Ídem anterior. **Base de Datos** • Ídem anterior. **Procesos** • Ídem anterior. **Aplicaciones** • Ídem anterior. • **Física** • Ídem anterior.							

Fuente: Adaptación del Modelo de Instrumento de Evaluación de la Metodología de Bracho y Silva (2007).

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

3.2.1.- Modelo de Entrevista Estructurada

A continuación se muestra el modelo de entrevistas aplicado por igual a todos los segmentos, pero que evaluó únicamente las secciones 1 y 2.

Tabla Nº 2 Sección 1: Política de Seguridad de la Información – Subsección 1.1

Subsección 1.1: Documento de política.		
Preguntas	Respuesta	Puntos
¿Existen documentos de políticas de seguridad?		
¿Existe normativa relativa a la seguridad?		
¿Existen procedimientos relativos a la seguridad?		
TOTAL: Documento de política		Obt. /Máx.
		%

Fuente: Elaboración Propia (2007).

Tabla Nº 3 Sección 1: Política de Seguridad de la Información – Subsección 1.2

Subsección 1.2: Revisión y evaluación.		
Preguntas	Respuesta	Puntos
¿Existe un responsable de las políticas, normas y procedimientos?		
¿Existen mecanismos para la comunicación a los usuarios de las normas?		
¿Existen controles regulares para verificar la efectividad de las políticas?		
TOTAL: Revisión y evaluación.		Obt./Máx
		%

Fuente: Adaptación Palacios (2005).

Tabla Nº 4 Sección 2: Estructura Organizativa – Subsección 2.1

Subsección 2.1: Infraestructura de seguridad de información		
Preguntas	Respuesta	Puntos
¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad?		
¿Existe un responsable encargado de evaluar la adquisición y cambios?		
¿Existen programas de formación en seguridad?		
TOTAL: Revisión y evaluación.		Obt./Máx.
		%

Fuente: Adaptación Palacios (2005).

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

Tabla Nº 5 Sección 2: Estructura Organizativa – Subsección 2.2

Subsección 2.2: Seguridad en accesos de Terceras partes.		
Preguntas	Respuesta	Puntos
¿Existen condiciones contractuales de seguridad con terceros y outsourcing?		
¿Se revisa la organización de la seguridad periódicamente por una empresa externa?		
TOTAL: Revisión y evaluación.		Obt./Máx. %

Fuente: Adaptación Palacios (2005).

Tabla Nº 6 Sección 2: Estructura Organizativa – Subsección 2.3

Subsección 2.3: Externalización.		
Preguntas	Respuesta	Puntos
¿Existe contrato de mantenimiento y soporte con empresa externa para contingencias?		
¿Se revisa la organización de la seguridad periódicamente por una empresa externa?		
¿Estas empresas deben cumplir con las normas establecidas dentro de la universidad?		
TOTAL: Revisión y evaluación.		Obt./Máx. %

Fuente: Adaptación Palacios (2005).

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

Tabla Nº 7 Activo según Nivel de Importancia

Clave	Nombre del activo	Marca	Adm.	Usuario	Conf.			Int.			Disp.			Control de acceso			Crit. Valor
					A	M	B	A	M	B	A	M	B	A	M	B	

Fuente: Elaboración Propia (2007).

Tabla Nº 8 Identificación de Amenazas

	Existe	(Si existe), ¿Qué lugares son más vulnerables?	(Si existe), ¿Hay medidas de seguridad contra las amenazas?	(Si existe), ¿cuáles son?
Desastres naturales				
Estructurales				
Hardware				
Software				
Red LANy WAN				
Copias de seguridad				
Información				
Personal				
Riesgos contra el patrimonio				
Otros riesgos				

Fuente: Adaptación PALACIOS (2005).

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

Tabla Nº 9 Detalle de la Importancia de cada Activo

Activo		**ÁREA: SEGURIDAD**		
DESCRIPCIÓN AMENAZA	**¿ES UNA AMENAZA?**	**SEGMENTO DE SEGURIDAD:**		**¿FASE DE PREGUNTAS?**
Virus	SI [ ] NO[ ]	S. O.	[ ]	¿Utiliza el mismo antivirus para todos los módulos de la facultad? ¿Siempre se ha utilizado el mimo antivirus y porque? ¿Poseen un histórico de los virus que han causado mas impacto en los últimos meses?
		Software	[ ]	
		Comunicaciones	[ ]	
		Base de datos	[ ]	
		Procesos	[ ]	
		Aplicaciones	[ ]	
		Física	[ ]	
Acceso no autorizado a la información.	SI [ ] NO[ ]	S. O.	[ ]	¿Cada cuanto tiempo son actualizadas las claves de los sistemas informáticos? ¿Utilizan algún método de cifrado para otorgar las contraseñas a los diferentes niveles de usuarios? ¿se inician registro de sucesos una vez que el usuario inicia sesión? ¿Se tiene oculto, protegido o cifrado los datos de alta relevancia del sistema?
		Software	[ ]	
		Comunicaciones	[ ]	
		Base de datos	[ ]	
		Procesos	[ ]	
		Aplicaciones	[ ]	
		Física	[ ]	
Penetración del sistema por intrusos	SI [ ] NO[ ]	S. O.	[ ]	¿Se tienen antecedentes de intrusos que hayan entrado al sistema sin previa autorización? ¿Se han revisado la confiabilidad de los programas, sistemas operativos o bases de datos para afín prevenir puertas traseras?
		Software	[ ]	
		Comunicaciones	[ ]	
		Base de datos	[ ]	
		Procesos	[ ]	
		Aplicaciones	[ ]	
		Física	[ ]	
Abuso de la red	SI [ ] NO[ ]	S. O.	[ ]	¿Posee sistema de monitoreo para supervisar las

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

inalámbrica		Software	[ ]	operaciones de las redes y que registre las posibles fallas? ¿Ha evaluado los riesgos inherentes en lo que respecta a las intercepciones de comunicaciones inalámbricas y posee técnicas para proteger la integridad y confidencialidad de los datos y en que solución se basan?
		Comunicaciones	[ ]	
		Base de datos	[ ]	
		Procesos	[ ]	
		Aplicaciones	[ ]	
		Física	[ ]	
Robo de la propiedad de información	SI [ ] NO[ ]	S. O.	[ ]	¿Se ha tomado en cuenta los registros almacenados (E-mail, archivos de aplicaciones de ofimática, imágenes, etc.), los registros generados (Registro de auditorias, transacciones y eventos) y los que han sido almacenado y generados parcialmente (hojas de cálculos financieras, consulta de base de datos, vista parciales de datos, etc.) como parte de de evidencias digitales?
		Software	[ ]	
		Comunicaciones	[ ]	
		Base de datos	[ ]	
		Procesos	[ ]	
		Aplicaciones	[ ]	
		Física	[ ]	
Deterioro o daño de sitios Web.	SI [ ] NO[ ]	S. O.	[ ]	
		Software	[ ]	
		Comunicaciones	[ ]	
		Base de datos	[ ]	
		Procesos	[ ]	
		Aplicaciones	[ ]	
		Física	[ ]	
Sabotaje / Incendió o inundaciones inesperadas	SI [ ] NO[ ]	S. O.	[ ]	¿Ha configurado mensajes de advertencia sobre la mala conducta antes que el atacante pueda entrar al sistema del servidor? ¿Y reforzado la política corporativa para notificarle al administrador, cual es la política apropiada durante el proceso de acceso al sistema?¿Qué medidas de seguridad existen en caso de incendió o inundaciones?
		Software	[ ]	
		Comunicaciones	[ ]	
		Base de datos	[ ]	
		Procesos	[ ]	
		Aplicaciones	[ ]	

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

		Física	[ ]	
Respaldo de archivos y directorios	SI [ ] NO[ ]	S. O.	[ ]	¿Existe usuarios con privilegios para hacer copias de seguridad de datos de los equipos computacionales instalados, para posibles respaldos?
		Software	[ ]	
		Comunicaciones	[ ]	
		Base de datos	[ ]	
		Procesos	[ ]	
		Aplicaciones	[ ]	
		Física	[ ]	
Generación de auditorias de seguridad sin control	SI [ ] NO[ ]	S. O.	[ ]	¿Se controla la seguridad de auditoria contra usuarios que puedan llenar esta con eventos vanos e incluso sobrescribir los eventos, de modo que puedan quitar las pruebas de sus actividades no autorizadas?
		Software	[ ]	
		Comunicaciones	[ ]	
		Base de datos	[ ]	
		Procesos	[ ]	
		Aplicaciones	[ ]	
		Física	[ ]	
Inexistencia de políticas de restauración de archivo y directorios	SI [ ] NO[ ]	S. O.	[ ]	¿Existen medidas de seguridad para la restauración de archivos? a fin de evitar que un usuario del sistema sobrescriba los datos recientes y cause perdidas importantes, de forma que se pueda evitar la corrupción de datos y de versiones que incluyan claves maliciosas o peor aun la instalación de puertas traseras
		Software	[ ]	
		Comunicaciones	[ ]	
		Base de datos	[ ]	
		Procesos	[ ]	
		Aplicaciones	[ ]	
		Física	[ ]	

Fuente: Adaptación Palacios (2005).

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

Tabla Nº 10 Contramedida

Activo			
CONTRAMEDIDA	**SEGMENTO APLICABLE**	**PUNTAJE CONTRAMEDIDA (%)**	**ACATAMIENTO - CUMPLIMIENTO**
Políticas de seguridad	SI [ ] NO[ ]		
Pared de fuego externa	SI [ ] NO[ ]		
Antivirus	SI [ ] NO[ ]		
Manejador de contenido	SI [ ] NO[ ]		
Manejador de correcciones	SI [ ] NO[ ]		
Control de acceso a la Red	SI [ ] NO[ ]		
Manejador de SPAM	SI [ ] NO[ ]		
Anti – Spyware	SI [ ] NO[ ]		
Sistema de detección de intrusos	SI [ ] NO[ ]		
Sistema de prevención de intrusos	SI [ ] NO[ ]		
Software de manejo diario	SI [ ] NO[ ]		
Herramientas forenses	SI [ ] NO[ ]		
Cortafuegos de nivel de aplicaciones	SI [ ] NO[ ]		
Encriptación para los datos en tránsito	SI [ ] NO[ ]		
Encriptación para los datos de almacenamiento	SI [ ] NO[ ]		
Infraestructura de claves públicas	SI [ ] NO[ ]		
Antípicos y UPS	SI [ ] NO[ ]		

Fuente: Adaptación PALACIOS (2005)

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

4.- Resultado de la Evaluación del Edificio Grano de Oro

Tabla Nº 11 Ponderación de los Segmentos

Segmentos	Pesos Técnicos	Pesos Políticos	Pesos Finales
Seg. 1: Seguridad de Cumplimiento de Normas y Est.	25	15	**20**
Seg. 2: Seguridad de Sistema Operativo.	5	5	**5**
Seg. 3: Seguridad de Software.	5	5	**5**
Seg. 4: Seguridad de Comunicaciones y Redes.	15	25	**20**
Seg. 5: Seguridad de Base de Datos.	5	5	**5**
Seg. 6: Seguridad de Proceso.	5	5	**5**
Seg. 7: Seguridad de Aplicaciones.	15	15	**15**
Seg. 8: Seguridad Física.	25	25	**25**
TOTALES	**100**	**100**	**100**

Fuente: Metodología de Piattini y Del Peso (2001)

Tabla Nº 12 Ponderación de las secciones del segmento 1

Segmento 1: Seguridad de Cumplimiento de Normas y Estándares			
SECCIONES	**PESOS TÉCNICOS**	**PESOS POLÍTICOS**	**PESOS FINALES**
Sección 1: Política de seguridad de la información.	4	2	**3**
Sección 2: Estructura organizativa.	2	1	**1**
Sección 3: Clasificación y control de activos.	2	2	**2**
Sección 4: Seguridad relacionada con el personal.	1	2	**1**
Sección 5: Seguridad física y del entorno.	2	2	**2**
Sección6: Gestión de comunicaciones y operaciones.	3	3	**3**
Sección7: Control de accesos.	2	3	**3**
Sección8: Desarrollo y mantenimiento de sistemas.	0	0	**0**
Sección 9: Gestión de continuidad de negocio.	3	2	**3**
Sección 10: Conformidad.	1	3	**2**
TOTALES	**20**	**20**	**20**

Fuente: Metodología de Piattini y Del Peso (2001)

Tabla Nº 13 Ponderación de las secciones del segmento 2

Segmento 2: Seguridad de Sistema Operativo			
SECCIONES	**PESOS TÉCNICOS**	**PESOS POLÍTICOS**	**PESOS FINALES**
Sección 1: Política de seguridad de la información.	0	0	**0**
Sección 2: Estructura organizativa.	1	0	**1**
Sección 3: Clasificación y control de activos.	2	2	**2**
Sección 4: Seguridad relacionada con el personal.	0	0	**0**
Sección 5: Seguridad física y del entorno.	0	0	**0**
Sección 6: Gestión de comunicaciones y operaciones.	4	3	**4**
Sección 7: Control de accesos.	5	5	**5**
Sección 8: Desarrollo y mantenimiento de sistemas.	0	3	**2**
Sección 9: Gestión de continuidad de negocio.	4	3	**3**
Sección 10: Conformidad.	3	4	**3**
TOTALES	**20**	**20**	**20**

Fuente: Metodología de Piattini y Del Peso (2001)

Tabla Nº 14 Ponderación de las secciones del segmento 3

Segmento 3: Seguridad de Software.			
SECCIONES	**PESOS TÉCNICOS**	**PESOS POLÍTICOS**	**PESOS FINALES**
Sección 1: Política de seguridad de la información.	0	0	**0**
Sección 2: Estructura organizativa.	2	0	**1**
Sección 3: Clasificación y control de activos.	2	2	**2**
Sección 4: Seguridad relacionada con el personal.	1	0	**1**
Sección 5: Seguridad física y del entorno.	4	2	**3**
Sección 6: Gestión de comunicaciones y operaciones.	4	3	**4**
Sección 7: Control de accesos.	2	3	**2**
Sección 8: Desarrollo y mantenimiento de sistemas.	0	0	**0**
Sección 9: Gestión de continuidad de negocio.	3	5	**4**
Sección 10: Conformidad.	2	5	**3**
TOTALES	**20**	**20**	**20**

Fuente: Metodología de Piattini y Del Peso (2001)

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

Tabla Nº 15 Ponderación de las secciones del segmento 4

Segmento 4: Seguridad de Comunicaciones y Redes.			
SECCIONES	**PESOS TÉCNICOS**	**PESOS POLÍTICOS**	**PESOS FINALES**
Sección 1: Política de seguridad de la información.	1	1	**1**
Sección 2: Estructura organizativa.	1	1	**1**
Sección 3: Clasificación y control de activos.	2	1	**1**
Sección 4: Seguridad relacionada con el personal.	1	3	**2**
Sección 5: Seguridad física y del entorno.	4	3	**3**
Sección 6: Gestión de comunicaciones y operaciones.	5	4	**4**
Sección 7: Control de accesos.	2	3	**3**
Sección 8: Desarrollo y mantenimiento de sistemas.	1	0	**1**
Sección 9: Gestión de continuidad de negocio.	1	2	**2**
Sección 10: Conformidad.	2	2	**2**
TOTALES	**20**	**20**	**20**

Fuente: Metodología de Piattini y Del Peso (2001)

Tabla Nº 16 Ponderación de las secciones del segmento 5

Segmento 5: Seguridad de Base de Datos.			
SECCIONES	**PESOS TÉCNICOS**	**PESOS POLÍTICOS**	**PESOS FINALES**
Sección 1: Política de seguridad de la información.	1	0	**1**
Sección 2: Estructura organizativa.	1	0	**0**
Sección 3: Clasificación y control de activos.	4	3	**3**
Sección 4: Seguridad relacionada con el personal.	3	3	**3**
Sección 5: Seguridad física y del entorno.	4	5	**4**
Sección 6: Gestión de comunicaciones y operaciones.	2	0	**2**
Sección 7: Control de accesos.	2	2	**2**
Sección 8: Desarrollo y mantenimiento de sistemas.	0	0	**0**
Sección 9: Gestión de continuidad de negocio.	1	3	**2**
Sección 10: Conformidad.	2	4	**3**
TOTALES	**20**	**20**	**20**

Fuente: Metodología de Piattini y Del Peso (2001)

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

Tabla Nº 17 Ponderación de las secciones del segmento 6

Segmento 6: Seguridad de Procesos.			
SECCIONES	**PESOS TÉCNICOS**	**PESOS POLÍTICOS**	**PESOS FINALES**
Sección 1: Política de seguridad de la información.	1	0	**1**
Sección 2: Estructura organizativa.	1	0	**1**
Sección 3: Clasificación y control de activos.	3	2	**2**
Sección 4: Seguridad relacionada con el personal.	1	2	**1**
Sección 5: Seguridad física y del entorno.	2	1	**1**
Sección 6: Gestión de comunicaciones y operaciones.	2	2	**2**
Sección 7: Control de accesos.	5	6	**6**
Sección 8: Desarrollo y mantenimiento de sistemas.	1	2	**2**
Sección 9: Gestión de continuidad de negocio.	2	2	**2**
Sección 10: Conformidad.	2	3	**2**
TOTALES	**20**	**20**	**20**

Fuente: Metodología de Piattini y Del Peso (2001)

Tabla Nº 18 Ponderación de las secciones del segmento 7

Segmento 7: Seguridad de Aplicaciones.			
SECCIONES	**PESOS TÉCNICOS**	**PESOS POLÍTICOS**	**PESOS FINALES**
Sección 1: Política de seguridad de la información.	0	0	**0**
Sección 2: Estructura organizativa.	0	0	**0**
Sección 3: Clasificación y control de activos.	3	4	**4**
Sección 4: Seguridad relacionada con el personal.	2	0	**2**
Sección 5: Seguridad física y del entorno.	0	0	**0**
Sección 6: Gestión de comunicaciones y operaciones.	3	3	**3**
Sección 7: Control de accesos.	2	1	**1**
Sección 8: Desarrollo y mantenimiento de sistemas.	6	8	**6**
Sección 9: Gestión de continuidad de negocio.	2	2	**2**
Sección 10: Conformidad.	2	2	**2**
TOTALES	**20**	**20**	**20**

Fuente: Metodología de Piattini y Del Peso (2001)

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

Tabla Nº 19 Ponderación de las secciones del segmento 8

Segmento 8: Seguridad de Física.			
SECCIONES	**PESOS TÉCNICOS**	**PESOS POLÍTICOS**	**PESOS FINALES**
Sección 1: Política de seguridad de la información.	2	3	**2**
Sección 2: Estructura organizativa.	2	1	**2**
Sección 3: Clasificación y control de activos.	3	2	**2**
Sección 4: Seguridad relacionada con el personal.	3	3	**3**
Sección 5: Seguridad física y del entorno.	1	2	**1**
Sección 6: Gestión de comunicaciones y operaciones.	0	0	**0**
Sección 7: Control de accesos.	2	3	**3**
Sección 8: Desarrollo y mantenimiento de sistemas.	1	0	**1**
Sección 9: Gestión de continuidad de negocio.	3	3	**3**
Sección 10: Conformidad.	3	3	**3**
TOTALES	**20**	**20**	**20**

Fuente: Metodología de Piattini y Del Peso (2001)

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

Tabla Nº 20 Resultados de las secciones por segmento

Secciones	Seg.1	Seg.2	Seg. 3	Seg. 4	Seg. 5	Seg.6	Seg.7	Seg. 8
Política de Seguridad: Documento de política.	100%	100%	100%	100%	100%	100%	100%	100%
Revisión y evaluación.	93%	67%	100%	67%	67%	67%	67%	67%
Porcentaje de Cumplimiento	ΣPSi/i = 96,50%	ΣPSi/i = 83,50%	ΣPSi/i= 100,00%	ΣPSi/i = 83,50%	ΣPSi/= 83,50%	ΣPSi/i = 83,50%	ΣPSi/i = 83,50%	ΣPSi/i = 83,50%
Aspectos organizativos para la seguridad: Infraestructura de seguridad de información.	100%	67%	67%	67%	67%	67%	67%	60%
Seguridad en accesos de Terceras partes.	50%	0%	50%	0%	0%	0%	0%	50%
Externalización.	67%	0%	0%	0%	0%	0%	0%	0%
Porcentaje de Cumplimiento	**ΣAOSi/ i= 72,33%**	**ΣAOSi/ i= 22,33%**	**ΣAOSi/ i= 39,00%**	**ΣAOSi/ i= 22,33%**	**ΣAOSi/ i= 22,33%**	**ΣAOSi/ i=22,33 %**	**ΣAOSi/ i= 22,33%**	**ΣAOSi/ i=36,67 %**
Clasificación y control de activos: Responsabilidades sobre los activos.	80%	70%	100%	70%	70%	70%	50%	80%
Clasificación de la información.	100%	100%	100%	100%	100%	100%	67%	NA%
Porcentaje de Cumplimiento	**ΣCCAi/ i= 90,00%**	**ΣCCAi/ i= 85,00%**	**ΣCCAi/ i= 100,00 %**	**ΣCCAi/ i= 85,00%**	**ΣCCAi/ i=85,00 %**	**ΣCCAi/ i= 85,00%**	**ΣCCAi/ i=58,50 %**	**ΣCCAi/ i= 80,00%**
Seguridad ligada al personal: Seguridad en la definición de los puestos de trabajo.	100%	100%	100%	100%	100%	67%	67%	87%
Capacitación de los usuarios.	90%	60%	60%	100%	60%	75%	100%	87%
Respuesta ante incidentes de seguridad.	100%	80%	80%	100%	80%	80%	100%	100%
Porcentaje de Cumplimiento	**ΣSPi / i = 96,67%**	**ΣSPi / i = 80,00%**	**ΣSPi / i = 80,00%**	**ΣSPi / i = 100,00 %**	**ΣSPi/i= 80,00%**	**ΣSPi / i = 74,00%**	**ΣSPi / i =89,00 %**	**ΣSPi /i = 91,33%**
Seguridad física y del entorno:	90%	100%	100%	100%	100%	75%	75%	65%

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

Áreas seguras.								
Seguridad de los Equipos.	100%	50%	50%	50%	50%	50%	50%	100%
Controles generales.	100%	100%	100%	100%	100%	100%	50%	100%
Porcentaje de Cumplimiento	**ΣSFEi/i = 96,67%**	**ΣSFEi/i = 83,33%**	**ΣSFEi /i = 83,33%**	**ΣSFEi /i= 83,33%**	**ΣSFEi/i =83,33 %**	**ΣSFEi /i= 75,00%**	**ΣSFEi/i = 58,33%**	**ΣSFEi/i = 88,33%**
Gestión de comunicaciones y operaciones:								
Procedimientos y responsabilidades	80%	67%	67%	67%	67%	67%	67%	60%
Planificación del sistema.	100%	75%	75%	75%	75%	75%	75%	NA
Gestión de respaldos.	100%	100%	100%	100%	100%	100%	100%	NA
Protección código malicioso.	73%	33%	33%	33%	33%	67%	33%	100%
Gestión de redes.	100%	100%	100%	100%	100%	100%	100%	100%
Uso y seguridad de soportes.	70%	75%	75%	100%	75%	100%	50%	20%
Intercambios de información.	**ΣGCOi/ i= 89,00%**	**ΣGCOi/ i= 78,57%**	**ΣGCOi/ i= 78,57%**	**ΣGCOi/ i= 69,28%**	**ΣGCOi/ i=65,71 %**	**ΣGCOi/ i= 87,00%**	**ΣGCOi/ i= 5,00%**	**ΣGCOi/ i= 70,00%**
Porcentaje de Cumplimiento								
Control de accesos:								
Requerimientos.	100%	100%	100%	100%	100%	100%	100%	50%
Gestión de acceso usuarios.	100%	100%	100%	50%	100%	50%	100%	30%
Responsabilidad usuarios.	100%	100%	100%	100%	100%	100%	100%	0%
Control de acceso a la red.	76%	72%	72%	60%	72%	60%	80%	0%
Control de acceso al so.	100%	100%	100%	100%	100%	100%	100%	NA
Control acceso a aplicaciones.	100%	100%	100%	100%	100%	100%	100%	NA
Seguimiento de accesos y usos.	100%	50%	50%	50%	50%	50%	50%	NA
Informática móvil y teletrabajo.	100%	100%	100%	100%	100%	100%	100%	NA
Porcentaje de Cumplimiento	**ΣCAi /i = 97,00%**	**ΣCAi /i = 79,00%**	**ΣCAi /i = 79,00%**	**ΣCAi /i = 60,00%**	**ΣCAi/i = 90,25%**	**ΣCAi /i = 94,28%**	**ΣCAi /i = 1,25%**	**ΣCAi /i = 20,00%**
Desarrollo y mantenimiento de sistemas:								
Requerimientos de seguridad.	100%	100%	100%	100%	100%	100%	100%	100%
Seguridad en								

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

aplicaciones.	100%	100%	100%	100%	100%	100%	100%	100%
Controles criptográficos.	100%	100%	100%	100%	100%	100%	100%	100%
Seguridad de ficheros sistema.	100%	100%	100%	100%	100%	100%	100%	NA
Seguridad desarrollo y soporte.	100%	100%	100%	0%	100%	0%	100%	NA
Porcentaje de Cumplimiento	**ΣDMSi/ i= 100,00 %**	**ΣDMSi/ i= 100,00 %**	**ΣDMSi/ i= 100,00 %**	**ΣDMSi/ i= 80,00%**	**ΣDMSi/ i=100,0 %**	**ΣDMSi/ i= 80,00%**	**ΣDMSi/ i=100,0 %**	**ΣDMSi/ i= 100,00 %**
Gestión de continuidad del negocio: Proceso de la gestión de continuidad.	100%	60%	60%	100%	80%	100%	0%	80%
Análisis de impacto.	100%	100%	100%	100%	100%	100%	0%	80%
Plan de Contingencia (PNC).	80%	0%	100%	100%	100%	100%	0%	80%
Planificación PNC.	100%	100%	0%	100%	0%	0%	0%	80%
Pruebas y Mantenimiento PNC.	100%	100%	100%	100%	100%	100%	100%	80%
Porcentaje de Cumplimiento	**ΣGCNi/ i= 96,00%**	**ΣGCNi/ i= 72,00%**	**ΣGCNi/ i= 72,00%**	**ΣGCNi/ i= 100,00 %**	**ΣGCNi/ i=76,00 %**	**ΣGCNi/ i= 80,00%**	**ΣGCNi/ i=20,00 %**	**ΣGCNi/ i= 80,00%**
Conformidad con la legislación: Cumplimiento de los requerimientos legales.	100%	100%	100%	100%	100%	100%	100%	100%
Revisiones de la política de seguridad y de conformidad técnica.	60%	0%	0%	100%	0%	100%	0%	80%
Consideraciones sobre la auditoría de sistemas.	80%	0%	0%	0%	0%	0%	0%	NA
Porcentaje de Cumplimiento	**ΣCLi /= 80,00%**	**ΣCLi / i = 33,33%**	**ΣCLi / i = 33,33%**	**ΣCLi / i = 66,67%**	**ΣCLi / i =33,33 %**	**ΣCLi / i = 66,67%**	**ΣCLi / i =33,33 %**	**ΣCLi / i= 90,00%**
SubTotal	**ΣGOi/i = 91,41%**	**ΣGOi/i = 71,70%**	**ΣGOi/i = 75,02%**	**ΣGOi/i = 75,01%**	**ΣGOi /i= 71,94%**	**Σ GOi /i= 74,77%**	**Σ GOi/i= 63,12%**	**ΣGOi /i= 73,98%**

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

Luego de haber realizado el análisis detallado sobre los valores arrojado por cada segmento, los resultados fueron los siguientes, aplicando la adaptación del modelo de instrumento de evaluación de la metodología de Bracho y Silva (2007):

Segmento 1: Seguridad de Cumplimiento de Normas y Estándares. Ver Tabla N°12 y Tabla N° 20 columna 1.
Porcentaje de Cumplimiento = (((3)*(96,50%)) + ((1)*(72,33%)) + ((2)*(90,00%)) + ((1)*(96,67%)) + ((1)*(96,67%)) + ((2)*(89,00%)) + ((3)*(97,00%)) + ((0)*(100,00%)) + ((3)*(96,00%)) + ((2)*(80,00%))) / 20 = 1652,17 / 20 = 82,60%.
Segmento 2: Seguridad de Sistema Operativo. Ver Tabla N° 13 y Tabla N°20 columna 2.
Porcentaje de Cumplimiento = (((0)*(83,50%)) + ((1)*(22,33%)) + ((2)*(85,00%)) + ((0)*(80,00%)) + ((0)*(83,33%)) + ((4)*(78,57%)) + ((5)*(79,00%)) + ((2)*(100,00%)) + ((3)*(72,00%)) + ((3)*(33,33%))) / 20 = 1417,60 / 20 = 70,88%.
Segmento 3: Seguridad de Software. Ver Tabla N°14 y Tabla N°20 columna 3.
Porcentaje de Cumplimiento = (((0)*(100,00%)) + ((1)*(39,00%)) + ((2)*(100,00%)) + ((1)*(80,00%)) + ((3)*(83,33%)) + ((4)*(78,57%)) + ((2)*(79,00%)) + ((0)*(100,00%)) + ((4)*(72,00%)) + ((3)*(33,33%))) / 20 = 1429,26 / 20 = 71,46%.
Segmento 4: Seguridad de Comunicaciones y Redes. Ver Tabla N° 15 y Tabla N°20 columna 4.
Porcentaje de Cumplimiento = (((1)*(83,50%)) + ((1)*(22,33%)) + ((1)*(85,00%)) + ((2)*(100,00%)) + ((3)*(83,33%)) + ((4)*(69,28%)) + ((3)*(60,00%)) + ((1)*(80,00%)) + ((2)*(100,00%)) + ((2)*(66,67%))) / 20 = 1511,28 / 20 = 75,56%.
Segmento 5: Seguridad de Base de Datos. Ver Tabla N° 16 y Tabla N°20 columna 5.
Porcentaje de Cumplimiento = (((1)*(83,50%)) + ((0)*(22,33%)) + ((3)*(85,00%)) + ((3)*(80,00%)) + ((4)*(83,33%)) + ((2)*(65,71%)) + ((2)*(90,25%)) + ((0)*(100,00%)) + ((2)*(76,00%)) + ((3)*(33,33%))) / 20 = 1475,73 / 20 = 73,78%.
Segmento 6: Seguridad de Procesos. Ver Tabla N° 17 y Tabla N°20 columna 6.
Porcentaje de Cumplimiento = (((1)*(83,50%)) + ((1)*(22,33%)) + ((2)*(85,00%)) + ((1)*(74,00%)) + ((1)*(75,00%)) + ((2)*(87,00%)) + ((6)*(94,28%)) + ((2)*(80,00%)) + ((2)*(80,00%)) + ((2)*(66,67%))) / 20 = 1617,85 / 20 = 80,89%.
Segmento 7: Seguridad de Aplicaciones. Ver Tabla N ° 18 y Tabla N°20 columna 7.
Porcentaje de Cumplimiento = (((0)*(83,50%)) + ((0)*(22,33%)) + ((4)*(58,50%)) + ((2)*(89,00%)) + ((0)*(58,33%)) + ((3)*(75,00%)) + ((1)*(91,25%)) + ((6)*(100,00%)) + ((2)*(20,00%)) + ((2)*(33,33%))) / 20 = 1434,91 / 20 = 71,74%.
Segmento 8: Seguridad de Física. Ver Tabla Nº19 y Tabla Nº20 columna 8.
Porcentaje de Cumplimiento = (((2)*(83,50%)) + ((2)*(36,67%)) + ((2)*(80,00%)) + ((3)*(91,33%)) + ((1)*(88,33%)) + ((0)*(70,00%)) + ((3)*(20,00%)) + ((1)*(100,00%)) + ((3)*(80,00%)) + ((3)*(90,00%))) / 20 = 1432,04 / 20 = 71,60%.

Una vez obtenido el resultado de cada segmento es necesario mostrar el resultado del área en cuestión, ver Tabla Nº 9 y resultado anteriores arrojados por segmento.

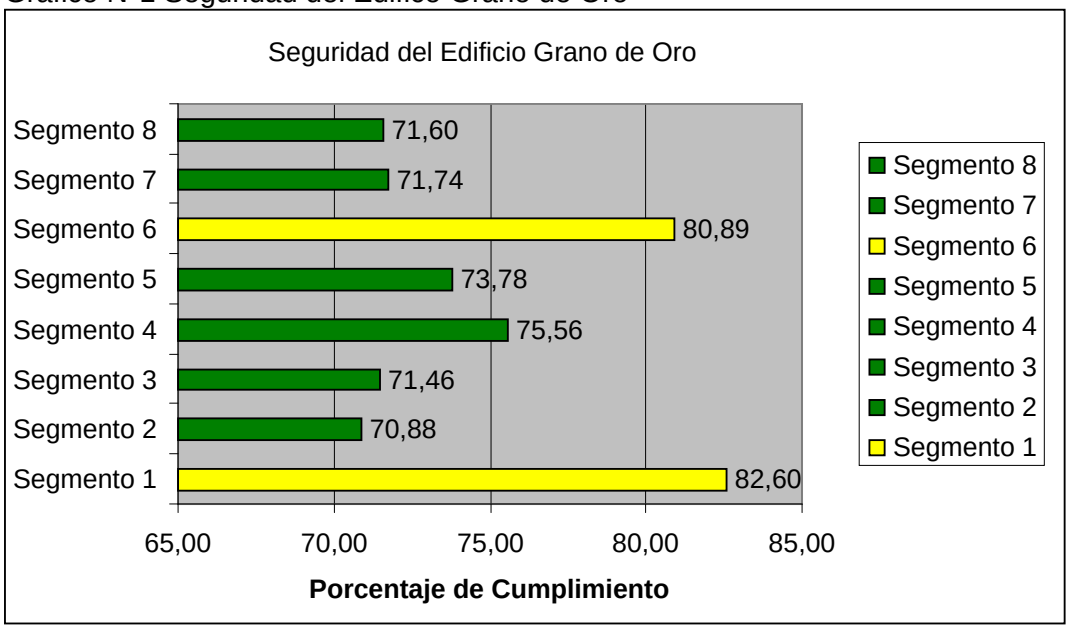
Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

Porcentaje de Cumplimiento = (((20)*(82,60%)) + ((5)*(70,88%)) + ((5)*(71,46%)) + ((20)*(75,56%)) + ((5)*(73,78%)) + ((5)*(80,89%)) + ((15)*(71,74%)) + ((25)*(71,60%))) / 100 = 7514,35 / 100 = 75,14%.

CONCLUSIONES

El Edificio Grano de Oro, correspondiente al área auditada de la RedFEC presenta a nivel general sólidos argumentos que permiten asegurar que existe un cumplimiento de las disposiciones a nivel administrativo y operativo en lo que compete a la seguridad del servicio telemático, superando los promedios establecidos, tal y como se muestra en el gráfico Nº 1.

Gráfico N°1 Seguridad del Edifico Grano de Oro



Fuente: Elaboración Propia (2008).

De igual forma, el Gráfico Nº 1 muestra que no existen segmentos de atención urgente pero ello no debe ser garantía absoluta que no se pueda vulnerar la seguridad del Edificio Grano de Oro, lo cual obliga a realizar mantenimientos periódicos que aseguran que las vulnerabilidades sean pocas y conocidas.

Plan de Acción: que comprende acciones a corto, mediano y largo plazo.

Acciones a Corto Plazo:

- Diseñar, ejecutar y revisar el Plan de Contingencia.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

- Mejorar los mecanismos de seguridad física de las instalaciones a través de protecciones físicas (ubicación del centro de proceso, servidores, terminales, portátiles; diseño, estructura, construcción y distribución de edificios; amenazas de fuego; controles de detección basados en horario; contenido de carteras, bolsos, cajas; protección de soportes magnéticos y ópticos) y protecciones lógicas (biometría; contraseñas; controles existentes para evitar y detectar caballos de Troya; no cesión, uso individual y responsable de cada usuario; sistemas de identificación únicos).

- Incorporar sistemas de controles de accesos a las áreas físicas y sistemas de vigilancia bajo circuito cerrado remoto.

- Solicitar y conocer los resultados de las auditorías que permitan evaluar la mejora en situaciones globales y específicas del servicio y seguridad de la RedFEC, además de la redacción de los procedimientos de control en el área de seguridad lógica; la aprobación de nuevos sistemas de gestión, la evaluación de los riesgos de los sistemas de información y las pruebas del plan de continuidad del negocio.

- Conocer los procesos y empresas que fungen como externas que están autorizadas para prestar servicios en la RedFEC, para que los costos propuesto para los servicios sea razonable, los mecanismos de seguridad está especificados en el contrato, los servicios contratados están basados en un análisis de las necesidades del negocio y el acceso de la auditoría a la RedFEC esté permitido conforme al contrato.

- Solicitar los permisos respectivos para adquirir una licencia académica con Microsoft y Symantec que garantice la actualización de los productos de software operativos, escritorio y antivirus presente en la ReFEC ó migrar de forma inmediata toda la plataforma operativa a software libre que no dejen abiertas vulnerabilidades como consecuencia de actualizaciones no realizadas para dar cumplimiento al decreto con rango de Ley del uso de Software Libre en Administración Pública Nº 3390.

- Utilizar el portal para difundir noticias sobre tips de seguridad que mantengan a los usuarios informados y alertas.

- Realizar evaluaciones al servicio realizado por RedLUZ, Departamento de Telecomunicaciones de LUZ, Centro de Computación y a las empresas externas.

- Revisar la bitácora (log) de todos los accesos a la información personal.

- Definir contraseñas iniciales y sucesivas, modo y vías de distribución; longitud mínima y composición de caracteres; vigencia; control para no asignar las “X” últimas; números de intentos; cifrado; cambio de las contraseñas iniciales.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

- Definir contraseñas separada para las transacciones sensitivas, utilizando claves de acceso de los usuarios robustas de 16 bits, con períodos de renovación de tres (3) meses como mínimo a seis (6) como máximo.

- Activar las reglas de acceso al personal autorizado.

- Programar acceso al sistema, sobre la base de horas hábiles, personal activo, entre otros.

- Registrar las actividades del usuario y de acceso a la comunicación de datos.

- Controlar todo lo posible sobre la seguridad de acceso, característica adscrita al atributo de funcionalidad de calidad del software.

- Participar con el Centro de Computación, Departamento de Telecomunicaciones de LUZ y RedLUZ la aprobación de la política de seguridad, pruebas del software y equipos de comunicaciones a nivel de seguridad de acceso del atributo de funcionalidad de calidad.

- Revisar los informes de disponibilidad del sistema, de coste-beneficio, de tiempo de respuesta, de utilización de bases de datos.

- Evaluar la validez de los casos en que se hayan efectuado cambios de contraseña, de la arquitectura de la aplicación cliente/servidor, de la arquitectura y el diseño de la red y de la protección de los cortafuegos y los servidores Proxy.

- Revisar el registro de las actividades del usuario, de acceso a la comunicación de datos.

- Verificar la autorización de usuario a nivel de campo, cambio de los archivos de datos.

- Denegar el acceso máximo no autorizado si se revelara una contraseña.

- Restrigir los derechos de acceso a usuario estarían restringidos por los parámetros adicionales de seguridad.

- Aumentar la carga de trabajo del administrador de seguridad.

- Utilizar sistemas de generación de electricidad que garantice la autosuficiencia de los equipos principales ante la interrupción temporal del servicio eléctrico externo.

- Llevar al día un inventario actualizado de los equipos telemáticos que están bajo administración de la RedFEC.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

- Realizar los respaldos de la data corporativa que es competencia de la RedFEC y tenerlos distribuidos en varias localidades.

- Escanear los archivos adjuntos de correo electrónico en el servidor de correo.

- Establecer mecanismos de monitoreo consolidados y centralizados de todas las áreas adscritas a la RedFEC de forma oportuna.

- Solicitar a RedLUZ y al Departamento de Telecomunicaciones administración conjunta del nodo principal de la RedLUZ.

- Contar con llaves que permitan acceder al sitio físico para monitorear el buen estado y protección de los equipos que allí reposan.

Acciones a Mediano Plazo:

- Revisar y actualizar las políticas de la RedFEC.

- Solicitar a la RedLUZ, Departamento de Telecomunicaciones de LUZ y Centro de Computación mayor participación en los procesos de administración y gestión del servicio telemático.

- Aplicar estándares para procesos específicos como los ISO 9126, ISO 9000 – 1, ISO 9000 – 2, ISO 9000 – 3, ISO 9000 – 4, ISO 8732, ISO 27001, ISO 14764, ISO 15504, ISO 15288, ISO 14598, IEEE 12207.

- Continuar con los procesos de formación del personal técnico de la RedFEC.

- Incoporar a los usuarios a los procesos de formación técnicos básicos telemáticos para disminuir el margen de error producto del desconocimiento o ingenuidad.

- Conocer oportunamente de parte del Centro de Computación de los procesos, procedimientos y mecanismos de seguridad incorporados en los distintos productos de software para contribuir con desarrollos locales en la RedFEC que sean homogéneos con los institucionales.

- Establecer modelos de calidad, métricas y ciclo de vida que permitan determinar los recursos computacionales exigidos para cada aplicación en desarrollo y uso, así como determinar oportunamente el momento de vida del software (introductorio, desarrollo, madurez y obsolescencia), de forma tal que sea posible conocer hasta donde soporta un producto informático nuevos servicios y cuando debe sacarse de uso.

- Desarrollar en conjunto con RedLUZ, Centro de Computación y Departamento de Telecomunicaciones de LUZ el Plan Maestro de Soporte a en cual se debe

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

especificar: los distintos tipos de mantenimiento a ejecutar, pretende ser una guía para la planificación, ejecución, control, revisión, evaluación y cierre del PMS, provee un marco formal para que planes genéricos y específicos de mantenimiento, puedan ser ejecutados, evaluados y adaptados, provee el entorno conceptual, terminología y procesos para la aplicación consistente de la tecnología (herramientas, técnicas y métodos) al Mantenimiento del Software (MS), define las actividades y tareas del MS, y provee requerimientos para la planificación del mantenimiento y es aplicable a situaciones de mantenimiento internas de una organización o a situaciones con dos organizaciones involucradas.

- Aprobar las actividades del DBA y segregación de funciones.

- Revisar los registros de acceso y actividades y del uso de las herramientas de bases de datos.

- Aplicar las siguientes leyes: Ley Orgánica de Ciencia y Tecnología, Ley de Mensaje de Datos y Firmas Electrónicas, Decreto Uso de Software Libre en la Administración Pública, Decreto 825, entre otros, así como, los proyectos nacionales de VoIP, Internet2, gobierno electrónico, entre otros.

- Conocer la percepción que los usuarios tienen de la RedFEC y del servicio telemático.

- Restaurar sistemas a partir de copias limpias.

- Deshabilitar las unidades de diskettes y puertos USB vía BIOS.

- Realizar escaneo en línea con definiciones actualizadas de virus.

Acciones a Largo Plazo:

- Las dispuestas como situación ideal según la norma ISO 17799 – 2005, que apliquen y que no hayan sido remendadas en acciones de corto y mediano plazo.

REFERENCIAS BIBLIOGRÁFICAS

ALEXANDER, Alberto (2005). Implantación del ISO 27001:2005. Sistemas de Gestión de Seguridad de Información. Obtenido el 07 de febrero de 2007 en http://www.centrum.pucp.edu.pe/excelencia/ensayos/ISO270012005_ysuImplantacion.pdf

ACURERO, Alfredo y FERRER Eugenio (2007). Informe Situación Actual RED-FEC 2004 al 2006. Universidad del Zulia – Facultad Experimental de Ciencias - REDFEC. 3, 9 – 10.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008

BRACHO, David y SILVA Neif (2007). Las herramientas colaborativas y publicación de contenidos en ambientes Web: Claves del éxito en la Herencia del Conocimiento trabajo presentado en la VI Conferencia Iberoamericana de Sistemas, Cibernética e Informática (CISCI), Julio, Orlando, Estados Unidos.

BUANDES, Gabriel (2002). Auditoría Informática. Ingeniería del Software III. Universidad de les Illes Balears. Obtenido el 3 de marzo de 2007 en http://dmi.uib.es/~bbuades/auditoria/index.htm

ECHENIQUE, José (2001). 2. Auditoría Informática. 194.

MARTÍNEZ, Antonio (2001). Introducción a la Auditoría de los S.I. Auditoría y Seguridad Informática. Universidad de Castilla - La Mancha. Obtenido el 09 de febrero de 2007 en http://alarcos.inf-cr.uclm.es/doc/Auditoria/auditoria.htm

PALACIOS, Rafael y SIERRA José y JARAUTA, Javier (2005). Seguridad Informática: Capítulo 2: Análisis de Riesgo. Obtenido el 10 de abril de 2007 en http://www.iit.upcomillas.es/palacios/seguridad/.

PIATTINI, Mario y DEL PESO, Emilio (2001). Seguridad de Sistemas de Información: Parte 2ª. Introducción. Obtenido el 23 de febrero de 2007 en http://alarcos.inf-cr.uclm.es/doc/Auditoria/index.htm

VILLALÓN, Antonio (2004). Código de Buenas Prácticas de Seguridad UNE-ISO/IEC 17799. El Sistema de Gestión de la Seguridad de la Información Obtenido el 19 de febrero de 2007 en http://www.criptored.upm.es/guiateoria/gt_m209d.htm

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 7 Edición No 1 – Año 2008