APLICACIÓN DE LOS ESTANDARES ISO 17799 Y 27001 PARA EL DIAGNÓSTICO DE LA SEGURIDAD FÍSICA Y LÓGICA EN LABORATORIOS DE INFORMÁTICA.

CLARA CARDOSO ARTEAGA
MANUEL GUILLERMO ZULUAGA CONTRERAS

UNIVERSIDAD MINUTO DE DIOS
Facultad de Ingeniería
Tecnología en Redes de computadores y seguridad informática
Bogotá D.C.
2007

APLICACIÓN DE LOS ESTANDARES ISO 17799 Y 27001 PARA EL DIAGNÓSTICO DE LA SEGURIDAD FÍSICA Y LÓGICA EN LABORATORIOS DE INFORMÁTICA.

Trabajo de grado para optar al título de Tecnólogo en Redes de Computadores y Seguridad Informática

CLARA CARDOSO ARTEAGA
MANUEL GUILLERMO ZULUAGA CONTRERAS

Director: Ing. Gustavo León.

UNIVERSIDAD MINUTO DE DIOS
Facultad de Ingenierías
Tecnología en Redes de computadores y seguridad informática
Bogotá D.C.
2007

Aplicación de los Estándares ISO 17799 y 27001 para el Diagnóstico de la Seguridad Física y Lógica en Laboratorios de Informática.

A nuestras familias por su apoyo incondicional, amigos por estar día a día con nosotros, a nuestros consagrados docentes, a todos aquellos que de una forma u otra hicieron parte de este proyecto, y mas importante aún, a Dios, a quien le debemos haber logrado culminar con Éxito este escalón tan importante en nuestras vidas.

Aplicación de los Estándares ISO 17799 y 27001 para el Diagnóstico de la Seguridad Física y Lógica en Laboratorios de Informática.

CONTENIDO

Pág.

Aplicación de los Estándares ISO 17799 y 27001 para el Diagnóstico de la Seguridad Física y Lógica en Laboratorios de Informática.

INTRODUCCION

Este trabajo se realizó luego de conocer la importancia que tiene el manejo de la información en la vida actual, esta información es fundamental tanto en organizaciones grandes como pequeñas ya que esta es considerada como un activo mas de las mismas; Conociendo este aspecto se comienza con a realizar este trabajo, el cual consta básicamente en el estudio de vulnerabilidades que puede tener un centro de computo (Laboratorio de Informática); Estos centros de computo son parte fundamental de toda organización, ya que desde allí es donde se ejecutan los procesos de sistematización de la información.

La finalidad del proyecto es generar un formato estándar que sirva para el diagnostico de las diferentes vulnerabilidades tanto físicas como lógicas de un centro de computo; Para ello se realizaron varios procesos de diagnostico los cuales arrojaron una serie de resultados que determinan el grado de vulnerabilidad en los laboratorios de informática donde se realizan dichas pruebas.

Aplicación de los Estándares ISO 17799 y 27001 para el Diagnóstico de la Seguridad Física y Lógica en Laboratorios de Informática.

1. ASPECTOS GENERALES

Para la elaboración de los formatos de evaluación, se tuvieron en cuenta una serie de procedimientos para aseguren la funcionabilidad de los mismos, ya que el no tenerlos en cuenta podría arrojar datos errados.

El objetivo es poder implementar los formatos con un diseño estandarizado que ayuden en el momento de realizar dichas evaluaciones, donde se detectaran las vulnerabilidades que se puedan presentar en los centros de cómputo.

La base utilizada inicialmente fueron los estándares ISO 17799 (ISO/IEC 27002 Code of practice for information security management - Actualmente ISO/IEC 17799:2005, publicado el 15 de junio del 2005 y 27001 (ISO/IEC 27001 ISMS - Requirements (revised BS 7799 Part 2:2005) – Publicado el 15 de octubre del 2005.

Para el diagnostico del estado lógico de los centros de computo se utilizo un software especializad para el análisis de vulnerabilidades como lo es Microsoft Baseline Security Analyzer 1.2.1, el cual arroja ciertos resultados dependiendo de las vulnerabilidades a que este expuesto cada host de los laboratorios de informática.

Al realizar el diagnostico físico se efectúo una revisión completa a los laboratorio de informática acerca del estado en que se encontraban las canaletas, tomas de datos, tomas de corriente eléctrica regulada y no regulada, interruptores, ubicación métrica de los puestos de trabajo entre otros.

Aplicación de los Estándares ISO 17799 y 27001 para el Diagnóstico de la Seguridad Física y Lógica en Laboratorios de Informática.

1.1 DESCRIPCION DEL PROYECTO

En los laboratorios de informática de la UNIMINUTO Sede principal Calle 80, se han detectado algunos riesgos de Seguridad informática, tanto física como lógicamente. Para la aplicación de políticas de seguridad y su respectivo control y evaluación se toma como directriz la Norma ISO 17799.

Al realizar la evaluación preliminar de los laboratorios de informática teniendo en cuenta la norma anteriormente mencionada se detectaron los siguientes problemas: se presenta levantamiento de canaletas en algunos sectores, los cables que se conectan a los puestos de trabajo se encuentran en desorden ocasionando daños en el cableado estructurado de la red, provocando ruidos en la transmisión de datos y generando con esto mal funcionamiento de la red. También se han detectando fallas de seguridad en la parte lógica de algunos equipos, dichas fallas van en contra del sistema de gestión de la seguridad de la información (confidencialidad, integridad y disponibilidad).

Por ello en este proyecto se dará a conocer el estado físico y lógico de los laboratorios de informática 209. 211 y 212 de la sede principal calle 80 UNIMINUTO (Bogotá).

Se realizo una evaluación lógica a cada salón de informática utilizando la herramienta Microsoft Baseline Security Analyzer 1.2.1 donde se analizo los Sistemas Operativos de cada maquina y se encontraron fallas y ataques en ellas, la evaluación física se ejecuto revisando el cableado y canaletas para constatar las condiciones en que se encuentran.

1.2 ANTECEDENTES

La población estudiantil de UNIMINUTO ha tenido un gran crecimiento, llegando a tener matriculados 12139 estudiantes en todas sus sedes, para el primer semestre del 2007

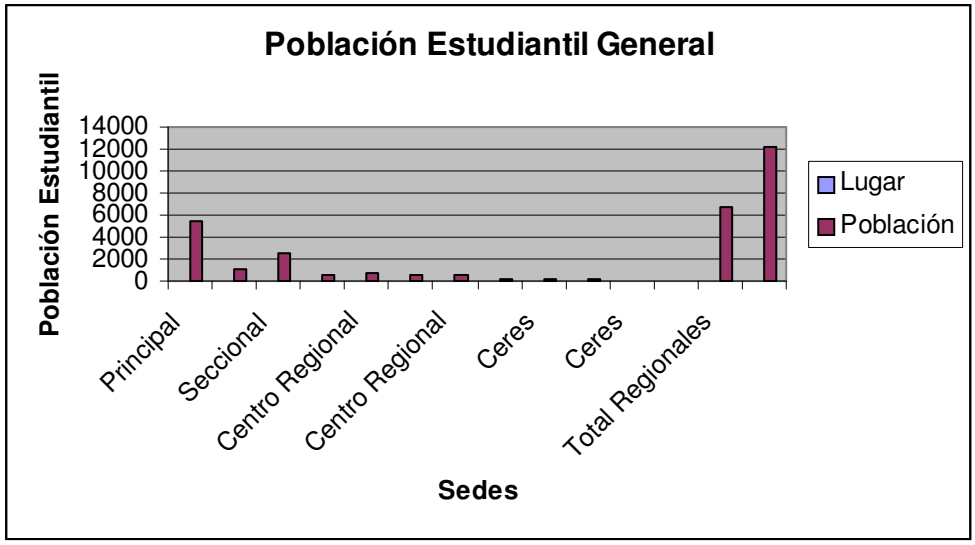
(ver Tabla 4). Esta situación demanda de un crecimiento en la plataforma tecnológica para garantizar una calidad de servicio óptima a estudiantes y profesores.

Para mostrar el crecimiento de alumnos que ha tenido la universidad en los últimos años, el cual es bien significativo, a continuación se presentan los datos recopilados de la cartelera del Centro de Regionales.

Población Estudiantil General

Sedes	Lugar	Población
Principal	Bogotá DC	5417
Seccional	Bello	1126
Seccional	Cali	2505
Seccional	Popayán	621
Centro Regional	Soacha	680
Centro Regional	Girardot	567
Centro Regional	Villavicencio	623
Ceres	Lérida	215
Ceres	B/manga	170
Ceres	Chinchina	157
Ceres	Mitú	58
Total Regionales		6722
Total Nacional		12139

Tabla 1. Distribución de la población estudiantil por sedes para el semestre I de 2007



Gráfica 1. Distribución de la población estudiantil por sedes. Fuente: Autor

Después de analizar el crecimiento estudiantil que ha obtenido la Universidad en los últimos años, se puede advertir la necesidad de hacer un estudio de los laboratorios de informática, puesto que al existir un incremento de alumnos, se hace mayor uso de las aulas y en ocasiones se presentan fallas de funcionamiento.

Los fallos que puede presentar un laboratorio de informática se pueden dividir en fallos físicos y lógicos, así:

Fallos físicos
Levantamiento de las canaletas.
Deficiencias en las tomas para las redes de datos.
Conectividad deficiente de los puntos de red.
Cable de red doblado y en ocasiones roto.
Conectores RJ45 desprendidos o en mal funcionamiento.

Fallos Lógicos
Vulnerabilidad en la seguridad de los ordenadores.
Ataques internos y/o externos.

Con el desarrollo del proyecto se pretende detectar las posibles fallas del sistema entre las cuales podrían estar las enumeradas con anterioridad o incluso otras no conocidas ("0 days,"), que puedan ir surgiendo y diseñar las soluciones necesarias que hagan menos vulnerables a los equipos.

El análisis de vulnerabilidad se ha convertido en un requisito indispensable dentro del proceso de gestión de riesgos y es clave dentro del sistema de gestión de la seguridad de la información.

Las variables del sistema de seguridad son:

Confidencialidad
Integridad
Disponibilidad .[1]

Adicionalmente a continuación se correlaciona un cuadro con datos básicos sobre las aulas o laboratorios de informática.

Aulas o Laboratorios de Informática Uniminuto Bogotá (Calle 80)

Aula	Laboratorio de Informática #	Número de Equipos	Estado
306	1	20	B
307	2	12	B
308	3	15	R
309	4	24	B
305	5	15	R
209	6	20	B
310	7	18	B
313	8	19	B
304	9	18	B
211	10	18	B
212	11	18	B

Tabla: 2 Número de Laboratorios de Informática y estado actual de las mismas.

(Conversiones: B = Bueno, R = Regular, M =Malo)

En este cuadro están registradas el número de aulas con que cuenta la sede principal de Uniminuto Bogotá (calle 80), además del número de equipos con que cuenta cada una y el estado actual, donde la variable B es Bueno y R Regular; Como se puede observar es un estudio realizado superficialmente el cual se pretende mejorar, a partir de la realización y ejecución de este proyecto. (Información suministrada por coordinación de aulas)

1.3 OBJETIVOS

1.3.1 Objetivo General

Realizar el diagnóstico de los laboratorios de informática 209, 211 y 212 de la sede principal calle 80 UNIMINUTO (Bogotá), basados en el estándar ISO 17799, para detectar las fallas y riesgos existentes, y plantear soluciones que conlleven a mejorar la práctica de la seguridad informática.

1.3.2 Objetivos Específicos.

- ✓ Recopilar y sintetizar en un documento los estándares ISO 17799 y 27001 para la evaluación de un laboratorio de informática.

- ✓ Diseñar los instrumentos de evaluación, que permitan estructurar, agilizar y documentar el proceso de diagnóstico de un laboratorio de informática.

- ✓ Aplicar los instrumentos de evaluación para el diagnostico de los laboratorios 209, 211 y 212, de la sede principal calle 80 (Bogotá).

- ✓ Realizar un reporte de la vulnerabilidad física y lógica a partir de los resultados obtenidos de la aplicación de los instrumentos de evaluación.

1.4 JUSTIFICACION

Este diagnostico ayudara a que la evaluación realizada a los laboratorios de informática en nuevas oportunidades sea más fácil y rápida de ejecutar.

Es importante realizar este proyecto por que ayudará a mejorar la calidad del servicio que actualmente se presta en las aulas de informática de UNIMINUTO sede principal calle 80 (Bogotá).

También se busca regular el sistema de gestión de seguridad de la información para evitar la pérdida de datos causados por infiltrados que buscan hacer daño a la institución.

En el aspecto económico reducirá los gastos innecesarios generados por daños físicos tales como: cables, tomas y conectores dañados y por daños lógicos los provocados por los ataques a los Sistemas Operativos dando como resulta el mal funcionamiento. Y en cuanto a la inversión es mínima ya que se busca aprovechar al máximo los recursos internos de la Universidad.

De esta misma manera se dará a conocer a continuación una lista completa de buenas prácticas en seguridad informática que se encuentran en la norma ISO/IEC 17799.

Objetivo: Proporcionar dirección y apoyo gerencial para brindar seguridad de la información.

El nivel gerencial debe establecer una dirección política clara y demostrar apoyo y compromiso con respecto a la seguridad de la información, mediante la formulación y mantenimiento de una política de seguridad de la información a través de toda la organización.

Política de seguridad de la información.

Los responsables del nivel gerencial deben aprobar y publicar un documento que contenga la política de seguridad y comunicarlo a todos los empleados, según

corresponda. Éste debe poner de manifiesto su compromiso y establecer el enfoque de la organización con respecto a la gestión de la seguridad de la información. Como mínimo, deben incluirse las siguientes pautas:

- Definición de la seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo que permite la distribución de la información.

- Una declaración del propósito de los responsables del nivel gerencial, apoyando los objetivos y principios de la seguridad de la información.

- Una breve explicación de las políticas, principios, normas y requisitos de cumplimiento en materia de seguridad, que son especialmente importantes para la organización, por ejemplo:

    - cumplimiento de requisitos legales y contractuales;
    - requisitos de instrucción en materia de seguridad;
    - prevención y detección de virus y demás software malicioso;
    - administración de la continuidad comercial;
    - consecuencias de las violaciones a la política de seguridad;

- Una definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información, incluyendo la comunicación de los incidentes relativos a la seguridad.

- Referencias a documentos que puedan respaldar la política, por ej. , políticas y procedimientos de seguridad más detallados para sistemas de información específicos o normas de seguridad que deben cumplir los usuarios.

Esta política debe ser comunicada a todos los usuarios de la organización de manera pertinente, accesible y comprensible.

Proceso de autorización para instalaciones de procesamiento de información

Debe establecerse un proceso de autorización gerencial para nuevas instalaciones de procesamiento de información. Debe considerarse lo siguiente.

Las nuevas instalaciones deben ser adecuadamente aprobadas por la gerencia usuaria, autorizando su propósito y uso. La aprobación también debe obtenerse del gerente responsable del mantenimiento del ambiente de seguridad del sistema de información local, a fin de garantizar que se cumplen todas las políticas y requerimientos de seguridad pertinentes.

Cuando corresponda, debe verificarse el hardware y software para garantizar que son compatibles con los componentes de otros sistemas.

> Nota: Puede ser necesaria la comprobación de categorías para ciertas conexiones.

Deben ser autorizados el uso de las instalaciones personales de procesamiento de información, para el procesamiento de información de la empresa, y los controles necesarios.

El uso de instalaciones personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades y en consecuencia debe ser evaluado y autorizado.

Estos controles son especialmente importantes en un ambiente de red.

Seguridad frente al acceso por parte de terceros

Objetivo: Mantener la seguridad de las instalaciones de procesamiento de información y de los recursos de información de la organización a los que acceden terceras partes.

El acceso a las instalaciones de procesamiento de información de la organización por parte de terceros debe ser controlado. Cuando existe una necesidad de la empresa para permitir dicho acceso, debe llevarse a cabo una evaluación de riesgos para determinar las incidencias en la seguridad y los requerimientos de control. Los controles deben ser acordados y definidos en un contrato con la tercera parte.

El acceso de terceros también puede involucrar otros participantes. Los contratos que confieren acceso a terceros deben incluir un permiso para la designación de otros participantes capacitados y las condiciones para su acceso.

Este estándar puede utilizarse como base para tales contratos y cuando se considere la tercerización del procesamiento de información.

Clasificación de la información

Objetivo: Garantizar que los recursos de información reciban un apropiado nivel de protección. La información debe ser clasificada para señalar la necesidad, las prioridades y el grado de protección. La información tiene diversos grados de sensibilidad y criticidad. Algunos ítems pueden requerir un nivel de protección adicional o un tratamiento especial. Se debe utilizar un sistema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de tratamiento especial.

2. MARCO TEORICO

En Colombia, a mediados de la década del 70, se inició "primitivamente" el procesamiento de información a través del computador, desplazando poco a poco, la máquina de escribir e incluso, el lápiz y el papel. Es así como cartas, oficios u otros documentos familiares o comerciales, que si no se hacía a mano, eran considerados como de "mala educación", a medida que avanzaban los sistemas computacionales fueron aceptados por la sociedad como documentos impresos en el nuevo medio de escritura e información.

Los avances computacionales no sólo han reemplazado esta clase de escritura, sino que ha ido reemplazando muchas costumbres de la sociedad, como, por ejemplo, la presentación de tareas en los colegios, de tesis en las universidades, la forma de comunicación (desplazando al teléfono) a través del correo electrónico, del chat o videochat, etc.

Así mismo, se puede participar, en tiempo real, de video-conferencias de temas de interés particular o general desde cualquier parte del mundo; algo que era imposible de imaginar antes de los años setentas.

Pero esto no es todo. Las grandes investigaciones, los grandes científicos, consultan el Internet, a través de la página Web, para actualizarse o consultar y profundizar en aquellos temas de su interés. E incluso, las tareas de los colegiales pueden resolverla con este mismo medio.

Este sistema informático, actualmente aprovechado por todas las personas de diferentes edades, es utilizado para asuntos personales, familiares, comerciales, profesionales, académicos, políticos y de solución de conflictos. El desconocerlo, no

sólo es estar desactualizado sino ignorar herramientas que pueden fácilmente solucionar problemas y facilitar accesos comunicacionales.

Desde su nacimiento, la Universidad Minuto de Dios tiene una filosofía humanitaria, muy acertada con la comunidad del barrio de su mismo nombre y con la sociedad colombiana en general, y es que no puede haber joven, mujer u hombre, que habiendo terminado sus estudios de bachillerato básico secundario, no ingresen a continuar sus estudios en un plantel de nivel superior, de acuerdo a sus preferencias, cualidades y conocimientos personales, para profundizar, especializarse y lograr ejercer profesionalmente en aquello que, además de gustarle, ayuda al desarrollo de su familia, la comunidad y la sociedad.

La Universidad MD, que fue planeada, muy bien proyectada hacia el futuro, ha venido mostrando los resultados de sus siembras. Los frutos reconocidos y apoyados por la sociedad, no sólo bogotana sino colombiana e incluso internacionalmente, muestran que el querer de sus creadores ha sido realidad, gracias a la calidad de los egresados que han ejercido con gran profesionalismo los conocimientos adquiridos en el desarrollo de sus estudios, el aporte de los profesores y la calidad de sus directivos y académicos.

Sin embargo, los avances de la tecnología informática son acelerados y la Universidad Minuto de Dios no puede dejarse rezagar. Debe estar a la par, hombro a hombro con la tecnología, con el crecimiento de la demanda universitaria, con las necesidades de comunicación interna, para ser vanguardia del profesionalismo de sus estudiantes y egresados.

2.1 Por qué es necesaria la seguridad de la información

La información y los procesos, sistemas y redes que le brindan apoyo constituyen importantes recursos de la empresa.

Las organizaciones y sus redes y sistemas de información, se enfrentan en forma creciente con amenazas relativas a la seguridad, de diversos orígenes, incluyendo el fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio o inundación.

La dependencia de las organizaciones respecto de los sistemas y servicios de información denota que ellas son más vulnerables a las amenazas concernientes a seguridad. La interconexión de las redes públicas y privadas y el uso compartido de los recursos de información incrementa la dificultad de lograr el control de los accesos.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados. La administración de la seguridad de la información, exige, como mínimo, la participación de todos los empleados de la organización.

2.2 Evaluación de los riesgos en materia de seguridad

Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. Puede resultar necesario que el proceso de evaluación de riesgos y selección de controles deba llevarse acabo en varias ocasiones, a fin de cubrir diferentes partes de la organización o sistemas de información individuales.

2.3 Selección de controles

Una vez identificados los requerimientos de seguridad, deben seleccionarse e implementarse controles para garantizar que los riesgos sean reducidos a un nivel aceptable. No obstante, es necesario reconocer que algunos controles no son

aplicables a todos los sistemas o ambientes de información, y podrían no resultar viables en todas las organizaciones.

Algunos controles de este documento pueden considerarse como principios rectores para la administración de la seguridad de la información, aplicables a la mayoría de las organizaciones.

2.4 Punto de partida para la seguridad de la información

Algunos controles pueden considerarse como principios rectores que proporcionan un buen punto de partida para la implementación de la seguridad de la información.

Los controles que se consideran esenciales para una organización, desde el punto de vista legal comprenden:

Protección de datos y confidencialidad de la información personal
Protección de registros y documentos de la organización derechos de propiedad intelectual.

Los controles considerados como práctica recomendada de uso frecuente en la implementación de la seguridad de la información comprenden:

Documentación de la política de seguridad de la información.
Asignación de responsabilidades en materia de seguridad de la información
Instrucción y entrenamiento en materia de seguridad de la información.
Comunicación de incidentes relativos a la seguridad.
Administración de la continuidad de la empresa.

2.5 Origen y posicionamiento estándar.

ISO (Organización Internacional de Estándares) e IEC (Comisión Internacional de Electrotécnia) conforman un especializado sistema especializado para los estándares mundiales. Organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos por la organización respectiva para tratar con los campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en relación con ISO e IEC, también forman parte del trabajo.

En el campo de tecnología de información, ISO e IEC han establecido unir un comité técnico, ISO/IEC JTC 1 (Join Technical Committee Nº1). Los borradores de estas Normas Internacionales adoptadas por la unión de este comité técnico son enviados a los organismos de las diferentes naciones para su votación. La publicación, ya como una Norma Internacional, requiere la aprobación de por lo menos el 75% de los organismos nacionales que emiten su voto.

El Estándar Internacional ISO/IEC 17799 fue preparado inicialmente por el Instituto de Normas británico (como BS 7799) y fue adoptado, bajo la supervisión del grupo de trabajo "Tecnologías de la Información", del Comité Técnico de esta unión entre ISO/IEC JTC 1, en paralelo con su aprobación por los organismos nacionales de ISO e IEC.

El estándar ISO/IEC 27001 es el nuevo estándar oficial, su título completo en realidad es: BS 7799- 2:2005 (ISO/IEC 27001:2005). También fue preparado por este JTC 1 y en el subcomité SC 27, IT "Security Techniques". La versión que se considerará en este texto es la primera edición, de fecha 15 de octubre de 2005, si bien en febrero de 2006 acaba de salir la versión cuatro del mismo.

1870 organizaciones en 57 países han reconocido la importancia y los beneficios de esta nueva norma. A fines de marzo de 2006, son seis las empresas españolas que poseen esta certificación declarada.

El conjunto de estándares que aportan información de la familia ISO-2700x que se puede tener en cuenta son:

ISO/IEC 27000 Fundamentals and vocabulary
ISO/IEC 27001 ISMS - Requirements (revised BS 7799 Part 2:2005) – Publicado el 15 de octubre del 2005
ISO/IEC 27002 Code of practice for information security management - Actualmente ISO/IEC 17799:2005, publicado el 15 de junio del 2005
ISO/IEC 27003 ISMS implementation guidance (bajo desarrollo)
ISO/IEC 27004 Information security management measurement (bajo desarrollo)
ISO/IEC 27005 Information security risk management (basado e incorporado a ISO/IEC 13335 MICTS Part 2) (bajo desarrollo).

3. RESUMEN ESTANDARES ISO

La información es un recurso que, como el resto de los importantes activos comerciales, tiene valor para una organización y por consiguiente debe ser debidamente protegida.

La información puede existir en muchas formas.
La seguridad de la información se logra implementando un conjunto adecuado de controles, que abarca política, práctica, procedimientos, estructuras organizacionales y funciones del software.

Se deben establecer estos controles para garantizar que se logren los objetivos específicos de seguridad de la organización.
En el estudio realizado a los laboratorios de informática de la universidad Minuto de Dios se encontró que dichos laboratorios tienen las siguientes necesidades las cuales están dentro en los estándares anteriormente mencionados.

- Política de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de activos
- Seguridad ligada al personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Gestión de incidentes de seguridad de la información
- Gestión de continuidad de negocio
- Conformidad

Por que motivo se encontró que no se aplican los ítems anteriormente mencionados. Por que dentro de los laboratorios se hallaron las siguientes falencias.

- Cableado desordenado en un alto porcentaje.
- Los muebles de cómputo del laboratorio informática se encuentran en regular estado
- Los puntos de red no se encuentran bien marcados.
- Los equipos que se encuentran cerca de la ventana, están expuestos al sol.
- Los equipos que se encuentran cerca de la ventana están expuestos a posibles ataques.
- No cuenta con piso elevado o cámara plena.
- No existe un sistema de vigilancia las 24 horas a los centros de cómputo.
- No existen alarmas para detección de fuego automática ni manual.
- No existen políticas para realizar simulacros en caso de tener que desalojar las instalaciones en caso de emergencia.
- No se cuenta con máscaras contra gases o sistemas portátiles de oxígeno.
- Actualizaciones de seguridad críticas están faltantes y las actualizaciones de seguridad no podían ser confirmadas.
- Varios productos están usando un paquete de servicio que no es la más reciente versión o tienen otras advertencias.
- Algunas cuentas de usuario (2 de 5) tienen contraseñas en blanco.
- Autologin es arreglado sobre esta computadora.
- No se lleva un control sobre el número de violaciones en sucesión que la computadora ha tenido.

3.1 ESTÁNDAR INTERNACIONAL ISO/IEC 17799

ISO/IEC 17799 es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por International Organization for Standardization y por la comisión International Electrotechnical Commission en el año 2000 y con el título de *Information technology - Security techniques - Code of practice for information security management*. Tras un periodo de revisión y actualización de los contenidos del estándar se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005. El estándar ISO/IEC 17799 tiene su origen en la norma británica British Standard BS 7799-1 que fue publicada por primera vez en 1995.
En España existe la publicación nacional UNE-ISO/IEC 17799 que fue elaborada por el comité técnico AEN/CTN 71 y titulada *Código de buenas prácticas para la Gestión de la Seguridad de la Información* que es una copia idéntica y traducida del Inglés de la Norma Internacional ISO/IEC 17799:2000. La edición en español equivalente a la revisión ISO/IEC 17799:2005 se estima que esté disponible en la segunda mitad del año 2006.

ISO/IEC 17799 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la Información se define en el estándar como *la preservación de la 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) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)*.

La versión de 2005 del estándar incluye las siguientes once secciones principales:
Política de seguridad
* Aspectos organizativos para la seguridad

* Clasificación y control de activos
* Seguridad ligada al personal
* Seguridad física y del entorno
* Gestión de comunicaciones y operaciones
* Control de accesos
* Desarrollo y mantenimiento de sistemas
* Gestión de incidentes de seguridad de la información
* Gestión de continuidad de negocio
* Conformidad

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 133 entre todas las secciones aunque cada organización debe considerar previamente cuantos serán realmente los aplicables y según sus propias necesidades.

Con la aprobación de la norma ISO/IEC 27001 en Octubre de 2005 y la reserva de la numeración 27000 para la seguridad de la información, se espera que ISO/IEC 17799:2005 pase a ser renombrado como ISO/IEC 27002 en la revisión y actualización de sus contenidos en el 2007. [1]

La norma ISO/IEC 17799 es una guía de buenas prácticas y no especifica los requisitos necesarios que puedan permitir el establecimiento de un sistema de certificación adecuado para este documento.

La norma ISO/IEC 27001 (*Information technology - Security techniques - Information security management systems - Requirements*) sí es certificable y especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información según el famoso “Círculo de Deming”: PDCA

- acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 y tiene su origen en la norma británica British Standard BS 7799-2 publicada por primera vez en 1998 y que se elaboró con el propósito de poder certificar los Sistemas de Gestión de la Seguridad de la Información implantados en las organizaciones y por medio de un proceso formal de auditoría realizado por un tercero. [1]

3.1.1 Alcance

Esta parte del estándar brinda recomendaciones para la gestión de la seguridad de la información que han de ser aplicadas por los responsables de iniciar, implementar o mantener la seguridad en sus organizaciones. [2]

3.1.2 Términos y definiciones.

A los efectos de este documento se aplican las siguientes definiciones:

a) Seguridad de la información

La preservación de la confidencialidad, integridad y disponibilidad de la información.

b) Evaluación de riesgos

La evaluación de las amenazas, impactos y vulnerabilidades relativos a la información y a las instalaciones de procesamiento de la misma, y a la probabilidad de que ocurran

c) Administración de riesgos

El proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los sistemas de información.

3.1.3 POLÍTICA DE SEGURIDAD

3.1.3.1 Política de seguridad de la información

Objetivo: Proporcionar dirección y apoyo gerencial para brindar seguridad de la información.

El nivel gerencial debe establecer una dirección política clara y demostrar apoyo y compromiso con respecto a la seguridad de la información, mediante la formulación y mantenimiento de una política de seguridad de la información a través de toda la organización.

Políticas y procedimientos de seguridad más detallados para sistemas de información específicos o normas de seguridad que deben cumplir los usuarios.

Esta política debe ser comunicada a todos los usuarios de la organización de manera pertinente, accesible y comprensible. Incidentes de seguridad significativos, nuevas vulnerabilidades o cambios en la infraestructura técnica o de la organización.

3.1.4 ORGANIZACIÓN DE LA SEGURIDAD

3.1.4.1 Infraestructura de seguridad de la información

Objetivo: Administrar la seguridad de la información dentro de la organización. Debe establecerse un marco gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

Deben establecerse adecuados foros de gestión liderados por niveles gerenciales, a fin de aprobar la política de seguridad de la información, asignar funciones de seguridad y

coordinar la implementación de la seguridad en toda la organización. Se debe alentar la aplicación de un enfoque multidisciplinario de la seguridad de la información, por ej.,

3.1.4.2 Foro gerencial sobre seguridad de la información

La seguridad de la información es una responsabilidad de la empresa compartida por todos los miembros del equipo gerencial.

- Generalmente, un foro de esta índole comprende las siguientes acciones:

- Revisar y aprobar la política y las responsabilidades generales en materia de seguridad de la información;

- Monitorear cambios significativos en la exposición de los recursos de información frente a las amenazas más importantes;

- Revisar y monitorear los incidentes relativos a la seguridad;

- Aprobar las principales iniciativas para incrementar la seguridad de la información.

Un gerente debe ser responsable de todas las actividades relacionadas con la seguridad.

3.1.4.3 Coordinación de la seguridad de la información

En una gran organización, podría ser necesaria la creación de un foro ínter funcional que comprenda representantes gerenciales de sectores relevantes de la organización para coordinar la implementación de controles de seguridad de la información.

Normalmente, dicho foro:

Acuerda funciones y responsabilidades específicas relativas a seguridad de la información para toda la organización;
acuerda metodologías y procesos específicos relativos a seguridad de la información, por ej.

Evaluación de riesgos, sistema de clasificación de seguridad;
acuerda y brinda apoyo a las iniciativas de seguridad de la información de toda la organización, por ej.

Programa de concientización en materia de seguridad;
Garantiza que la seguridad sea parte del proceso de planificación de la información;
Evalúa la pertinencia y coordina la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios;
Revisa incidentes relativos a la seguridad de la información;
Promueve la difusión del apoyo de la empresa a la seguridad de la información dentro de la organización.

3.1.4.4 Asignación de responsabilidades en materia de seguridad de la información.

Deben definirse claramente las responsabilidades para la protección de cada uno de los recursos y por la implementación de procesos específicos de seguridad.

La política de seguridad de la información (ver punto 3) debe suministrar una orientación general acerca de la asignación de funciones de seguridad y responsabilidades dentro la organización.

En muchas organizaciones, se asigna a un gerente de seguridad de la información la responsabilidad general por el desarrollo e implementación de la seguridad y por el soporte a la identificación de controles.

Los propietarios de los recursos de información pueden delegar sus responsabilidades de seguridad a cada uno de los gerentes o proveedores de servicios.

** Deben identificarse y definirse claramente los diversos recursos y procesos de seguridad relacionados con cada uno de los sistemas.* [2]

3.1.4.5 Proceso de autorización para instalaciones de procesamiento de información.

Debe establecerse un proceso de autorización gerencial para nuevas instalaciones de procesamiento de información.

** Las nuevas instalaciones deben ser adecuadamente aprobadas por la gerencia usuaria, autorizando su propósito y uso. La aprobación también debe obtenerse del gerente responsable del mantenimiento del ambiente de seguridad del sistema de información local, a fin de garantizar que se cumplen todas las políticas y requerimientos de seguridad pertinentes.*

Cuando corresponda, debe verificarse el hardware y software para garantizar que son compatibles con los componentes de otros sistemas.

Deben ser autorizados el uso de las instalaciones personales de procesamiento de información, para el procesamiento de información de la empresa, y los controles necesarios.

El uso de instalaciones personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades y en consecuencia debe ser evaluado y autorizado.

Estos controles son especialmente importantes en un ambiente de red. [2]

3.1.4.6 Asesoramiento especializado en materia de seguridad de la información

Es probable que muchas organizaciones requieran asesoramiento especializado en materia de seguridad. Idealmente, éste debe ser provisto por un asesor interno experimentado en seguridad de la información.

Los asesores en seguridad de la información o puntos de contacto equivalentes serán los encargados de brindar asesoramiento acerca de todos los aspectos de la seguridad de la información, utilizando sus propias recomendaciones o las externas. La calidad de su evaluación de las amenazas a la seguridad y de su asesoramiento en materia de controles determinará la eficacia de la seguridad de la información de la organización.
Si bien la mayoría de las investigaciones de seguridad internas se llevan a cabo bajo el control de la gerencia, el asesor de seguridad de la información puede ser posteriormente convocado para asesorar, liderar o dirigir la investigación.

Se deben limitar los intercambios de información de seguridad, para garantizar que no se divulgue información confidencial, perteneciente a organización, entre personas no autorizadas.

3.1.5 SEGURIDAD FRENTE AL ACCESO POR PARTE DE TERCEROS

Objetivo: Mantener la seguridad de las instalaciones de procesamiento de información y de los recursos de información de la organización a los que acceden terceras partes.

El acceso a las instalaciones de procesamiento de información de la organización por parte de terceros debe ser controlado.

Cuando existe una necesidad de la empresa para permitir dicho acceso, debe llevarse a cabo una evaluación de riesgos para determinar las incidencias en la seguridad y los requerimientos de control. Los controles deben ser acordados y definidos en un contrato con la tercera parte. [2]

3.1.5.1 Tipos de acceso

El tipo de acceso otorgado a terceras partes es de especial importancia. Por ejemplo, los riesgos de acceso a través de una conexión de red son diferentes de los riesgos relativos al acceso físico.

Los tipos de acceso que deben tenerse en cuenta son: Acceso físico, por Ej. A oficinas, salas de cómputos, armarios.

b) acceso lógico, por Ej. A las bases de datos y sistemas de información de la organización.

3.1.5.2 Requerimientos de seguridad en contratos con terceros

Las disposiciones que contemplan el acceso de terceros a las instalaciones de procesamiento de información de la organización deben estar basadas en un contrato formal que contenga todos los requerimientos de seguridad, o haga referencia a los mismos, a fin de asegurar el cumplimiento de las políticas y estándares (normas) de

seguridad de la organización. Se deben considerar las siguientes cláusulas para su inclusión en el contrato.

La política general de seguridad de la información; la protección de activos, con inclusión de procedimientos de protección de los activos de la organización, incluyendo información y software; Procedimientos para determinar si se han comprometido los activos.

3.1.6 TERCERIZACIÓN

Objetivo: Mantener la seguridad de la información cuando la responsabilidad por el procesamiento de la misma fue delegada a otra organización.

Los acuerdos de tercerización deben contemplar los riesgos, los controles de seguridad y los procedimientos para sistemas de información, redes y/o ambientes de PC (desk top environments) en el contrato entre las partes.

3.1.6.1 Requerimientos de seguridad en contratos de tercerización

Los requerimientos de seguridad de una organización que terceriza la administración y el control de todos sus sistemas de información, redes y/o ambientes de PC, o de parte de los mismos, deben ser contemplados en un contrato celebrado entre las partes.

Entre otros ítems, el contrato debe contemplar:

cómo se cumplirán los requisitos legales, por ej., la legislación sobre protección de datos;

qué disposiciones se implementarán para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, estarán al corriente de sus responsabilidades en materia de seguridad;

cómo se mantendrá y comprobará la integridad y confidencialidad de los .activos de negocio de la organización ;

qué controles físicos y lógicos se utilizarán para restringir y delimitar el acceso de los usuarios autorizados a la información sensible de la organización;

Cómo se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres;
Qué niveles de seguridad física se asignarán al equipamiento tercerizado;
El derecho a la auditoría.

Asimismo, se deben tener en cuenta las cláusulas enumeradas en el punto 4.2.2 como parte de este contrato. El mismo debe permitir la ampliación de los requerimientos y procedimientos de seguridad en un plan de administración de la seguridad a ser acordado entre las partes.

Si bien los contratos de tercerización pueden plantear algunas cuestiones complejas en materia de seguridad, los controles incluidos en este código de práctica pueden servir como punto de partida para acordar la estructura y el contenido del plan de gestión de la seguridad.

3.1.7 CLASIFICACIÓN Y CONTROL DE ACTIVOS

3.1.7.1 Responsabilidad por rendición de cuentas de los activos

a) Objetivo: Mantener una adecuada protección de los activos de la organización. La responsabilidad por la implementación de los controles puede ser delegada. Ejemplos de activos asociados a sistemas de información son los siguientes:

b) Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia para la reposición de información perdida ("fallback"), información archivada.

c) Recursos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios.

d) Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos), medios magnéticos (cintas y discos), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado), mobiliario, lugares de emplazamiento.

e) servicios: servicios informáticos y de comunicaciones, utilitarios generales, por ej., calefacción, iluminación, energía eléctrica, aire acondicionado.

3.1.7.2 Clasificación de la información

Objetivo: Garantizar que los recursos de información reciban un apropiado nivel de protección.

La información debe ser clasificada para señalar la necesidad, la prioridades y el grado de protección.

La información tiene diversos grados de sensibilidad y criticidad.

Acceso no autorizado o daño ala información. La información y las salidas de los sistemas que administran datos clasificados deben ser rotuladas según su valor y grado de sensibilidad para la organización.

Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, verbigracia, cuando la información se ha hecho pública.

Un documento, registro de datos, archivo de datos o disquete, y por la revisión periódica de dicha clasificación, debe ser asignada al creador o propietario designado de la información. Estos procedimientos deben incluir los recursos de información en formatos físicos y electrónicos. Todos los empleados y usuarios externos de las

instalaciones de procesamiento de información deben firmar un acuerdo de confidencialidad (no revelación).

3.1.8 INCLUSIÓN DE LA SEGURIDAD EN LAS RESPONSABILIDADES DE LOS PUESTOS DE TRABAJO.

Las funciones y responsabilidades en materia de seguridad, según consta en la política de seguridad de la información de la organización (ver 3.1), deben ser documentadas según corresponda. Información financiera o altamente confidencial, la organización también debe llevar a cabo una verificación de crédito.

3.1.8.1 Capacitación del usuario

Objetivo: Garantizar que los usuarios están al corriente de las amenazas e incumbencias en materia de seguridad de la información, y están capacitados para respaldar la política de seguridad de la organización en el transcurso de sus tareas normales.

Los usuarios deben ser capacitados en relación con los procedimientos de seguridad y el correcto uso de las instalaciones de procesamiento de información, a fin de minimizar eventuales riesgos de seguridad.

3.1.8.2 Formación y capacitación en materia de seguridad de la información

Todos los empleados de la organización y, cuando sea pertinente, los usuarios externos, deben recibir una adecuada capacitación y actualizaciones periódicas en materia de políticas y procedimientos de la organización. Esto comprende los requerimientos de seguridad, las responsabilidades legales y controles del negocio, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información, por ej. el procedimiento de entrada al sistema ("log-on") y el uso de paquetes de software, antes de que se les otorgue acceso a la información o a los servicios.

3.1.8.3 Comunicación de debilidades en materia de seguridad

Los usuarios de servicios de información deben advertir, registrar y comunicar las debilidades o amenazas supuestas u observadas en materia de seguridad, con relación a los sistemas o servicios.

Si se ha de examinar el equipo, éste debe ser desconectado de las redes de la organización antes de ser activado nuevamente. c) El asunto debe ser comunicado inmediatamente al gerente de seguridad de la información.

La recuperación debe ser realizada por personal adecuadamente capacitado y experimentado.

3.1.8.4 Proceso disciplinario

Debe existir un proceso disciplinario formal para los empleados que violen las políticas y procedimientos de seguridad de la organización.

3.1.9 SEGURIDAD FÍSICA Y AMBIENTAL

3.1.9.1 Áreas seguras

Objetivo: Impedir accesos no autorizados, daños e interferencia a las sedes e información de la empresa.

Las instalaciones de procesamiento de información crítica o sensible de la empresa deben estar ubicadas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con vallas de seguridad y controles de acceso apropiados. Deben estar físicamente protegidas contra accesos no autorizados, daños e intrusiones.

3.1.9.2 Perímetro de seguridad física

La protección física puede llevarse a cabo mediante la creación de diversas barreras físicas alrededor de las sedes de la organización y de las instalaciones de procesamiento de información.

Las organizaciones deben utilizar perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información.

a) El perímetro de seguridad debe estar claramente definido.

b) El perímetro de un edificio o área que contenga instalaciones de procesamiento de información debe ser físicamente sólido (por ej. no deben existir claros [o aberturas] en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser de construcción sólida y todas las puertas que comunican con el exterior deben ser adecuadamente protegidas contra accesos no autorizados, por ej., mediante mecanismos de control, vallas, alarmas, cerraduras, etc.

c) Debe existir un área de recepción atendida por personal u otros medios de control de acceso físico al área o edificio. El acceso a las distintas áreas y edificios debe estar restringido exclusivamente al personal autorizado.

d) Las barreras físicas deben, si es necesario, extenderse desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo, la ocasionada por incendio e inundación.

e) Todas las puertas de incendio de un perímetro de seguridad deben tener alarma y cerrarse automáticamente.

3.1.9.3 Controles de acceso físico

Las áreas protegidas deben ser resguardadas por adecuados controles de acceso que permitan garantizar que sólo se permite el acceso de personal autorizado.

a) El acceso a la información sensible, y a las instalaciones de procesamiento de información, debe ser controlado y limitado exclusivamente a las personas autorizadas.

b) El personal del servicio de soporte externo debe tener acceso limitado a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso debe ser otorgado solamente cuando sea necesario y debe ser autorizado y monitoreado. Los requerimientos de seguridad de dichas áreas deben ser determinados mediante una evaluación de riesgos.

3.1.9.4 Seguridad del cableado

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información debe ser protegido contra interceptación o daño.

3.1.9.5 Seguridad del equipamiento fuera del ámbito de la organización

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la organización, debe ser autorizado por el nivel gerencial, sin importar quien es el propietario del mismo. Los controles de trabajo en domicilio deben ser determinados a partir de un análisis de riesgo y se aplicarán controles adecuados según corresponda, por ej. Gabinetes de archivo con cerradura, política de escritorios limpios y control de acceso a computadoras.

3.1.9.6 Controles generales

Objetivo: Impedir la exposición al riesgo o robo de la información o de las instalaciones de procesamiento de la misma.

Las instalaciones de procesamiento de la información y la información deben ser protegidas contra la divulgación, modificación o robo por parte de personas no autorizadas, debiéndose implementar controles para minimizar pérdidas o daños.

3.1.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES

3.1.10.1 Procedimientos y responsabilidades operativas

Se deben documentar y mantener los procedimientos operativos identificados por su política de seguridad. Los procedimientos operativos deben ser tratados como documentos formales y los cambios deben ser autorizados por el nivel gerencial.

También debe prepararse documentación sobre procedimientos referidos a actividades de mantenimiento del sistema, relacionadas con las instalaciones de procesamiento de información y comunicaciones, tales como los procedimientos de inicio y cierre, resguardo, mantenimiento de equipos, salas de cómputos y administración y seguridad del manejo de correo.

3.1.10.2 Documentación de los procedimientos operativos

Se deben documentar y mantener los procedimientos operativos identificados por su política de seguridad. Los procedimientos operativos deben ser tratados como documentos formales y los cambios deben ser autorizados por el nivel gerencial.
También debe prepararse documentación sobre procedimientos referidos a actividades de mantenimiento del sistema, relacionadas con las instalaciones de procesamiento de información y comunicaciones, tales como los procedimientos de inicio y cierre, resguardo, mantenimiento de equipos, salas de cómputos y administración y seguridad del manejo de correo.

3.1.10.3 Control de cambios en las operaciones

Se deben controlar los cambios en los sistemas e instalaciones de procesamiento de información. El control inadecuado de estos cambios es una causa común de las fallas de seguridad y de sistemas.

Se deben implementar responsabilidades y procedimientos gerenciales formales para garantizar un control satisfactorio de todos los cambios en el equipamiento, el software o los procedimientos. Los programas operativos deben estar sujetos a un control estricto de los cambios. Siempre que sea factible, los procedimientos de control de cambios en las operaciones y aplicaciones deben estar integrados

3.1.10.4 Procedimientos de manejo de incidentes

Se deben establecer responsabilidades y procedimientos de manejo de incidentes para garantizar una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad

Se deben considerar los siguientes controles.

Si el personal de desarrollo y prueba tiene acceso al sistema que esta operativo y a su información, éste puede ser capaz de introducir líneas de códigos no autorizados o no probados, o alterar los datos de las operaciones.
Las actividades de desarrollo y pruebas pueden producir cambios no planificados en el software y la información si los sistemas comparten el mismo ambiente informático. Se deben tener en cuenta los siguientes controles.
Estos controles deben garantizar que dichas contraseñas se modifiquen una vez utilizadas.

3.1.10.5 Planificación y aprobación de sistemas

Objetivo: Minimizar el riesgo de fallas en los sistemas. Estas proyecciones deben tomar en cuenta los nuevos requerimientos de negocios y sistemas y las tendencias actuales y proyectadas en el procesamiento de la información de la organización.
Éstos deben identificar las tendencias de uso, particularmente en relación con las aplicaciones comerciales o las herramientas de sistemas de información de gestión.

Los gerentes deben utilizar esta información para identificar y evitar potenciales cuellos de botella que podrían plantear una amenaza a la seguridad del sistema o a los servicios del usuario, y planificar una adecuada acción correctiva..

3.1.10.6 Aprobación del sistema

Se deben establecer criterios de aprobación para nuevos sistemas de información, actualizaciones ("upgrades") y nuevas versiones, y se deben llevar a cabo adecuadas pruebas de los sistemas antes de su aprobación.

3.1.10.7 Protección contra software malicioso.

Se deben implementar controles de detección y prevención para la protección contra software malicioso, y procedimientos adecuados de concientización de usuarios. La protección contra software malicioso debe basarse en la concientización en materia de seguridad y en controles adecuados de acceso al sistema y administración de cambios.

Se deben tener en cuenta los siguientes controles:

a) una política formal que requiera el uso de software con licencia y prohíba el uso de software no autorizado (ver 12.1.2.2);
b) una política formal con el fin de proteger contra los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier

otro medio, señalando qué medidas de protección deberían tomarse (ver también 10.5, especialmente 10.5.4 y 1 0.5.5);

c) instalación y actualización periódica de software de detección y reparación anti-virus, para examinar computadoras y medios informáticos, ya sea como medida precautoria o rutinaria,

d) realización de revisiones periódicas del contenido de software y datos de los sistemas que sustentan procesos críticos de al empresa. La presencia de archivos no aprobados o modificaciones no autorizadas debe ser investigada formalmente;

e) verificación de la presencia de virus en archivos de medios electrónicos de origen incierto o no autorizado, o en archivos recibidos a través de redes no confiables, antes de su uso;

f) verificación de la presencia de software malicioso en archivos adjuntos a mensajes de correo electrónico y archivos descargados por Internet ("downloads") antes de su uso. Esta verificación puede llevarse a cabo en diferentes lugares, por ej. en servidores de correo electrónico, computadoras de escritorio o al ingresar en la red de la organización;

g) procedimientos y responsabilidades gerenciales para administrar la protección contra virus en los sistemas, el entrenamiento con respecto a su uso, la comunicación y la recuperación frente a ataques (ver 6.3 y 8.1.3)

h) adecuados planes de continuidad de los negocios para la recuperación respecto de ataques de virus, incluyendo todos los datos necesarios, el resguardo del software y las disposiciones para la recuperación (ver el punto 11)

i) procedimientos para verificar toda la información relativa a software malicioso, y garantizar que los boletines de alerta sean exactos e informativos. Los gerentes deben garantizar que se utilizan fuentes calificadas, por ej. publicaciones acreditadas, sitios de Internet o proveedores de software anti-virus confiables, para diferenciar entre virus falaces y reales. Se debe concientizar al personal acerca del problema de los virus falsos (hoax) y de qué hacer al recibirlos.

Estos controles son especialmente importantes para servidores de archivos de red que brindan soporte a un gran número de estaciones de trabajo.

3.1.11 MANTENIMIENTO

Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento y comunicación de información.

3.1.11.1 Resguardo de la información

Se deben realizar periódicamente copias de resguardo de la información y el software esenciales para la empresa. Las disposiciones para el resguardo de cada uno de los sistemas deben ser probadas periódicamente para garantizar que cumplen con los requerimientos de los planes de continuidad de los negocios (ver punto 11). Se deben tener en cuenta los siguientes controles.

3.1.11.2 Administración de la red

Objetivo: Garantizar la seguridad de la información en las redes y la protección de la infraestructura de apoyo. También pueden requerirse controles adicionales para los datos sensibles que circulen por redes públicas.

3.1.11.3 Controles de redes

Se requiere un conjunto de controles para lograr y mantener la seguridad de las redes informáticas. Los administradores de redes deben implementar controles para garantizar la seguridad de los datos en la misma, y la protección de los servicios conectados contra el acceso no autorizado, En particular, se deben considerar los siguientes ítems.

Todos los procedimientos y niveles de autorización deben ser claramente documentados.

Deben considerarse los siguientes controles.

3.1.11.4 Procedimientos de manejo de la información

Se deben establecer procedimientos para el manejo y almacenamiento de la información para protegerla contra su uso inadecuado o divulgación no autorizada.

3.1.11.5 Seguridad de la documentación del sistema

La documentación del sistema puede contener cierta cantidad de información sensible, por ej. Descripción de procesos de aplicaciones, procedimientos, estructuras de datos, procesos de autorización. Se deben considerar los siguientes controles para proteger la documentación del sistema de accesos no autorizados.

a) La documentación del sistema debe ser almacenada en forma segura;
El listado de acceso a la documentación del sistema debe restringirse al mínimo y debe ser autorizado por el propietario de la aplicación;
La documentación del sistema almacenada en una red pública, o suministrada a través de una red pública, debe ser protegida de manera adecuada

3.1.11.6 Seguridad de los sistemas electrónicos de oficina

Se deben preparar e implementar políticas y lineamientos para controlar las actividades de la empresa y riesgos de seguridad relacionados con los sistemas electrónicos de oficina. el uso de boletines electrónicos corporativos (ver 9.1)

c) exclusión de categorías de información sensible de la empresa, si el sistema no brinda un adecuado nivel de protección (ver 5.2)

d) limitación del acceso a la información de agenda de personas determinadas, por ej. Empleados de la organización o contratistas en directorios a beneficio de otros usuarios

i) retención y resguardo de la información almacenada en el sistema (ver 12.1.3 y 8.4.1)

j) requerimientos y disposiciones relativos a sistemas de soporte UPC de reposición de información perdida (ver 1 1.1).
Es posible que la información de un sistema de acceso público, por ej.
El software, los datos y demás información que requiera un alto nivel de integridad, y que esté disponible en un sistema de acceso público, deben ser protegidos, mediante mecanismos adecuados, por ej. Firmas digitales

3.1.12 CONTROL DE ACCESOS

3.1.12.1 Registración de usuarios.

Debe existir un procedimiento formal de registración y desregistración de usuarios para otorgar acceso a todos los sistemas y servicios de información multi-usuario. El acceso a servicios de información multi-usuario debe ser controlado a través de un proceso formal de registración de usuarios, el cual debe incluir los siguientes puntos:

Utilizar IDs de usuario únicos de manera que se pueda vincular y hacer responsables a los usuarios por sus acciones. El uso de IDs grupales solo debe ser permitido cuando son convenientes para el trabajo a desarrollar; verificar que el usuario tiene autorización del propietario del sistema para el uso del sistema o servicio de información.

Los sistemas multi-usuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.

3.1.12.2 Administración de contraseñas de usuario.

Las contraseñas constituyen un medio común de validación de la identidad de un usuario para acceder a un sistema o servicio de información. Los usuarios deben acusar recibo de la recepción de la clave (password);

Las contraseñas nunca deben ser almacenadas en sistemas informativos sin protección

3.1.12.3 Uso de contraseñas.

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

3.1.12.4 Control de acceso a la red

Áreas públicas o externas que están fuera de la administración y el control de seguridad de la organización.

Se debe formular una política concerniente al uso de redes y servicios de red. Esta debe comprender:

Las redes y servicios de red a los cuales se permiten el acceso; procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales tienen permitido el acceso; controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

Esta política debe ser coherente con la política de control de accesos de la organización Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones de negocios, o para el uso no autorizado de servicios de información. Redes privadas virtuales para grupos de usuarios dentro de la organización.

Los requerimientos relativos a enrutamientos forzados deben basarse en la política de control de accesos de la organización.

3.1.12.5 Autenticación de usuarios para conexiones externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información de la empresa, por ej., accesos mediante discado. Por consiguiente, el acceso de usuarios remotos debe estar sujeto a la autenticación.

Los procedimientos y controles de rellamada deben ser probados exhaustivamente respecto de esta posibilidad.

Por consiguiente, las conexiones a sistemas informativos remotos deben ser autenticadas. Esto es particularmente importante si la conexión utiliza una red que esta fuera de control de la gestión de seguridad de la organización.

Muchas computadoras y sistemas de comunicación son instalados con una herramienta de diagnostico remoto por discado, para uso de los ingenieros de mantenimiento. Por consiguiente, deben ser protegidos por un mecanismo de seguridad apropiado, por ej. una cerradura de seguridad y un procedimiento que garantice que solo son accesibles mediante un acuerdo entre el gerente de servicios informativos y el personal de soporte de hardware y software que requiere acceso.
Dichas extensiones pueden incrementar el riesgo de acceso no autorizado a sistemas de información ya existentes que utilizan la red, algunos de los cuales podrían requerir de protección contra otros usuarios de red, debido a su sensibilidad o criticidad. En tales circunstancias, se debe considerar la introducción de controles dentro de la red, a fin de segregar grupos de servicios de información, usuarios y sistemas de información.
dominios de red internos y externos de una organización, cada uno protegido por un perímetro de seguridad definido. Dicho perímetro puede ser implementado mediante la instalación de una compuerta (“gateway”) segura entre las dos redes que han de ser interconectadas, para controlar el acceso y flujo de información entre los dos dominios. Este “gateway” debe ser configurado para filtrar el tráfico entre los dominios (ver 9.4.7 y 9.4.8) y para bloquear el acceso no autorizado de acuerdo con la política de control de accesos de la organización.

3.1.12.6 Control de conexión a la red

Los requerimientos de la política de control de accesos para redes compartidas, especialmente aquellas que se extiendan más allá de los limites de la organización, pueden requerir la incorporación de controles para limitar la capacidad de conexión de los usuarios.

3.1.12.7 Restricción del acceso a la información.

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, deben tener acceso a la información y a las funciones de los sistemas de aplicación de conformidad con una política de control de acceso definida, sobre la base de los requerimientos de cada aplicación comercial, y conforme a la política de la organización para el acceso a la información, se debe considerar la aplicación de los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

Provisión de menús para controlar el acceso a las funciones de los sistemas de aplicación; restricción del conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizadas a acceder, con la adecuada edición de documentación de usuario; control de los derechos de acceso de los usuarios.

3.1.13 DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

3.1.13.1 Requerimientos de seguridad de los sistemas.

Objetivo: Asegurar que la seguridad es incorporada a los sistemas de información.

El diseño e implementación de los procesos comerciales que apoyen la aplicación o servicio pueden ser cruciales para la seguridad. Los requerimientos de seguridad deben ser identificados y aprobados antes del desarrollo de los sistemas de información.

3.1.13.2 Análisis y especificaciones de los requerimientos de seguridad.

Las comunicaciones de requerimientos comerciales para nuevos sistemas o mejoras a los sistemas existentes deben especificar las necesidades de controles. Tales especificaciones deben considerar los controles automáticos a incorporar al sistema y la necesidad de controles manuales de apoyo.

Los requerimientos de seguridad y los controles deben reflejar el valor comercial de los recursos de información involucrados y el potencial daño al negocio que pudiere resultar por una falla o falta de seguridad. El marco para analizar los requerimientos de seguridad e identificar los controles que los satisfagan son la evaluación y la administración de riesgo.

3.1.13.3 Validación de datos de entrada

Los datos de entrada en sistemas de aplicación deben ser validados para asegurar que son correctos y apropiados.

3.1.13.4 Validaciones de los datos de salida

La salida de datos de un sistema de aplicación debe ser validada para garantizar que el procesamiento de la información almacenada sea correcto y adecuado a las circunstancias.

3.1.14 REVISIONES DE LA POLÍTICA DE SEGURIDAD Y LA COMPATIBILIDAD TÉCNICA.

Objetivo: Garantizar la compatibilidad de los sistemas con las políticas y estándares (normas) de seguridad de la organización.

La seguridad de los sistemas de información debe revisarse periódicamente. Dichas revisiones deben llevarse a cabo con referencia a las políticas de seguridad pertinentes y las plataformas técnicas y sistemas de información deben ser auditados para verificar su compatibilidad con los estándares (normas) de implementación de seguridad.

3.1.14.1 Cumplimiento de la política de seguridad

La gerencia debe garantizar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad. Entre las áreas a revisar deben incluirse las siguientes:

Sistemas de información; proveedores de sistemas; propietarios de información y de recursos de información; usuarios; gerentes.

Los propietarios de los sistemas de información deben apoyar la revisión periódica de la conformidad de sus sistemas con las políticas, estándares y otros requisitos de seguridad aplicables. El tópico referido al monitoreo operacional del uso del sistema es tratado en el punto.

3.1.14.2 Controles de auditoria de sistemas

Los requerimientos y actividades de auditoria que involucran verificaciones de los sistemas operacionales deben ser cuidadosamente planificados y acordados a fin de minimizar el riesgo de discontinuidad de los procesos de negocio.

3.2 RESUMEN ISO 27001

Se debe dejar claro que el tema de certificación en aspectos de seguridad, tal vez aún no ha sido considerado con la seriedad que merece en el ámbito empresarial, pero no cabe duda que lo será en el muy corto plazo. Justamente, la sensación que deja el análisis de esta norma, es que se está gestando con toda rigurosidad este hecho, y que como cualquier otra certificación ISO, este estándar internacional ha sido desarrollado (por primera vez con relación a la seguridad, a juicio de este autor) con toda la fuerza y detalle que hacía falta para empezar a presionar al ámbito empresarial sobre su aplicación. Es decir, se puede prever, que la certificación ISO-27001, será casi una obligación de cualquier empresa que desee competir en el mercado en el corto plazo, lo

cual es lógico, pues si se desea interrelacionar sistemas de clientes, control de stock, facturación, pedidos, productos, etc. entre diferentes organizaciones, se deben exigir mutuamente niveles concretos y adecuados de seguridad informática, sino se abren brechas de seguridad entre sí, este estándar apunta a poder exigir dichos niveles; y ya no puede caber duda que las empresas, para competir con sus productos (sean de la índole que fueren) en este mercado cibernético actual, tienen cada vez más necesidad de interrelacionar sus infraestructuras de información. ISO-27001 en este sentido es una muy buena y sólida opción. .

Actualmente el ISO-27001:2005 es el único estándar aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad

A los efectos de la certificación, la transición entre ambas normas queda propuesta (o establecida) por el TPS-55 de UKAS (United Kingdom Acreditation Service): ”Transition Statement Regarding Arrangements for the Implementation of ISO 27001:2005”. Establece que las empresas (en realidad los auditores, lo cual afecta directamente a las empresas) durante los primeros seis meses (desde que se firmó el acuerdo “MoU: Memorandum of Understanding” entre UKAS y el Departamento de Comercio e Industria de Reino Unido), pueden elegir acerca de qué estándar aplicar, a partir del 23 de julio del 2006, la única certificación que se deberá aplicar será la ISO/IEC 27001:2005. Ante cualquier no conformidad con la aplicación de la misma motivada claramente por su transición, se establece un plazo de un año para solucionarla, es decir, hasta el 23 de julio de 2007. [5] .

3.2.1 Presentación de este texto. .

El presente documento es un muy breve resumen de los aspectos más importantes a tener en cuenta para la aplicación del Estándar Internacional ISO-27001:2005. Se debe

dejar claro que este es la versión actual del ISO-17799:2002, y dentro del primero se detallan claramente todos los aspectos de compatibilidad entre ellos. El verdadero enfoque que se debe encarar para tratar de alcanzar la compatibilidad con este estándar es aplicar la Norma ISO-27001 con todo detalle y a través del seguimiento de todos los aspectos que propone, se estará cumplimentando también con la anterior (lo cual no elude el hecho que se deba conocer también esta predecesora).

3.2.2 Consideraciones clave del estándar.

La propuesta de esta norma, no está orientada a despliegues tecnológicos o de infraestructura, sino a aspectos netamente organizativos, es decir, la frase que podría definir su propósito es "Organizar la seguridad de la información", por ello propone toda una secuencia de acciones tendientes al "establecimiento, implemanetación, operación, monitorización, revisión, mantenimiento y mejora del ISMS (Information Security Management System)" (como podrán apreciar que se recalcará repetidas veces a lo largo del mismo). El ISMS, es el punto fuerte de este estándar.

Los detalles que conforman el cuerpo de esta norma, se podrían agrupar en tres grandes líneas:

ISMS.
Valoración de riegos (Risk Assesment)
Controles

3.2.3 Implantación del SGSI

Evidentemente, el paso previo a intentar la certificación es la implantación en la organización del sistema de gestión de seguridad de la información según ISO 27001.

Este sistema deberá tener un historial de funcionamiento demostrable de al menos tres meses antes de solicitar el proceso formal de auditoria para su primera certificación.

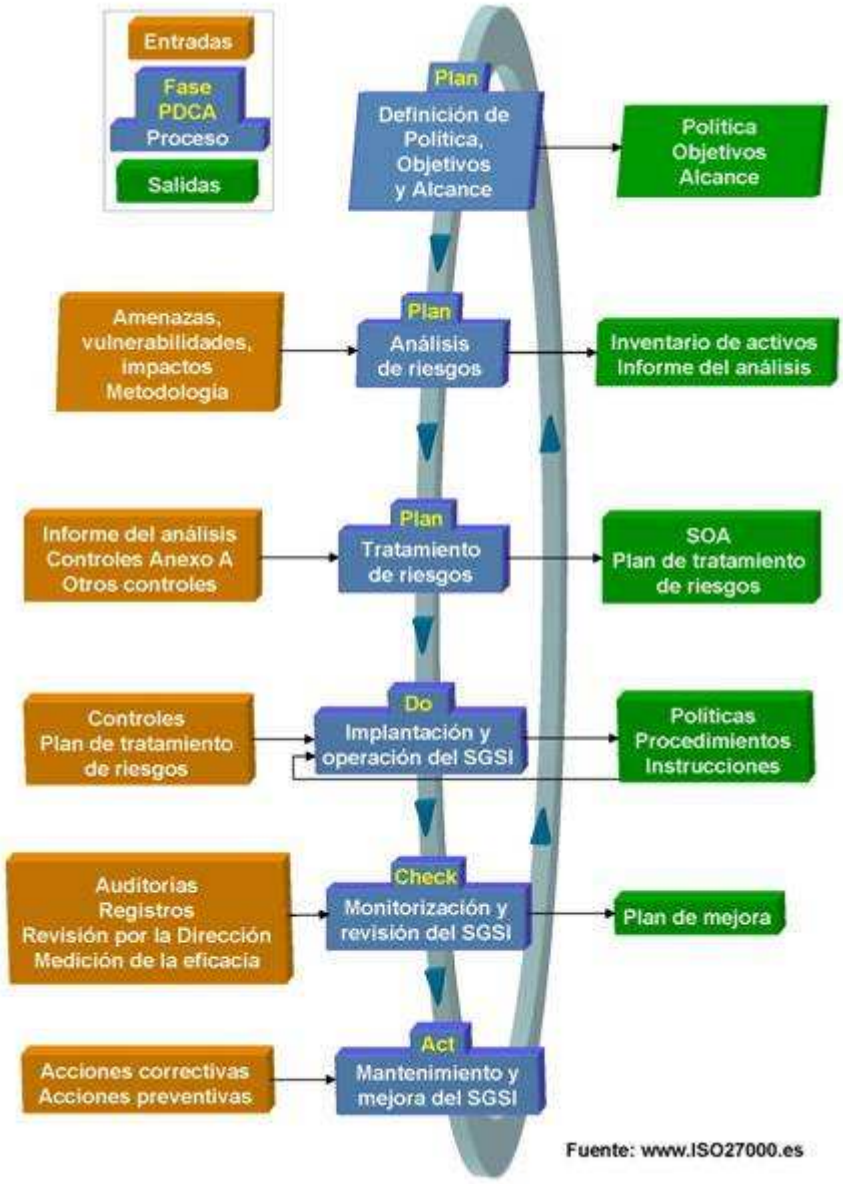
ISO 27001 exige que el SGSI contemple los siguientes puntos:

- Implicación de la Dirección.
- Alcance del SGSI y política de seguridad.
- Inventario de todos los activos de información.
- Metodología de evaluación del riesgo.
- Identificación de amenazas, vulnerabilidades e impactos.
- Análisis y evaluación de riesgos.
- Selección de controles para el tratamiento de riesgos.
- Aprobación por parte de la dirección del riesgo residual.
- Declaración de aplicabilidad.
- Plan de tratamiento de riesgos.
- Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo.
- Definición de un método de medida de la eficacia de los controles y puesta en marcha del mismo.
- Formación y concienciación en lo relativo a seguridad de la información a todo el personal.
- Monitorización constante y registro de todas las incidencias.
- Realización de auditorias internas.
- Evaluación de riesgos periódica, revisión del nivel de riesgo residual, del propio SGSI y de su alcance.
- Mejora continua del SGSI.

La documentación del SGSI deberá incluir:

- Política y objetivos de seguridad.
- Alcance del SGSI.
- Procedimientos y controles que apoyan el SGSI.
- Descripción de la metodología de evaluación del riesgo.

- Informe resultante de la evaluación del riesgo.
- Plan de tratamiento de riesgos.
- Procedimientos de planificación, manejo y control de los procesos de seguridad de la información y de medición de la eficacia de los controles.
- Registros.
- Declaración de aplicabilidad (SOA -Statement of Applicability-).
- Procedimiento de gestión de toda la documentación del SGSI.



Grafica Implantación del SGSI

3.2.4 Auditoria y certificación

Una vez implantado el SGSI en la organización, y con un historial demostrable de al menos 3 meses, se puede pasar a la fase de auditoria y certificación, que se desarrolla de la siguiente forma[5]:

- Solicitud de la auditoria por parte del interesado a la entidad de certificación y toma de datos por parte de la misma.

- Respuesta en forma de oferta por parte de la entidad certificadora.

- Compromiso.

- Designación de auditores, determinación de fechas y establecimiento conjunto del plan de auditoria.

- Pre-auditoria: opcionalmente, puede realizarse una auditoria previa que aporte información sobre la situación actual y oriente mejor sobre las posibilidades de superar la auditoria real.

- Fase 1 de la auditoria: no necesariamente tiene que ser in situ, puesto que se trata del análisis de la documentación por parte del Auditor Jefe y la preparación del informe de la documentación básica del SGSI del cliente, destacando los posibles incumplimientos de la norma que se verificarán en la Fase 2. Este informe se envía junto al plan de auditoria al cliente. El periodo máximo entre la Fase 1 y Fase 2 es de 6 meses.

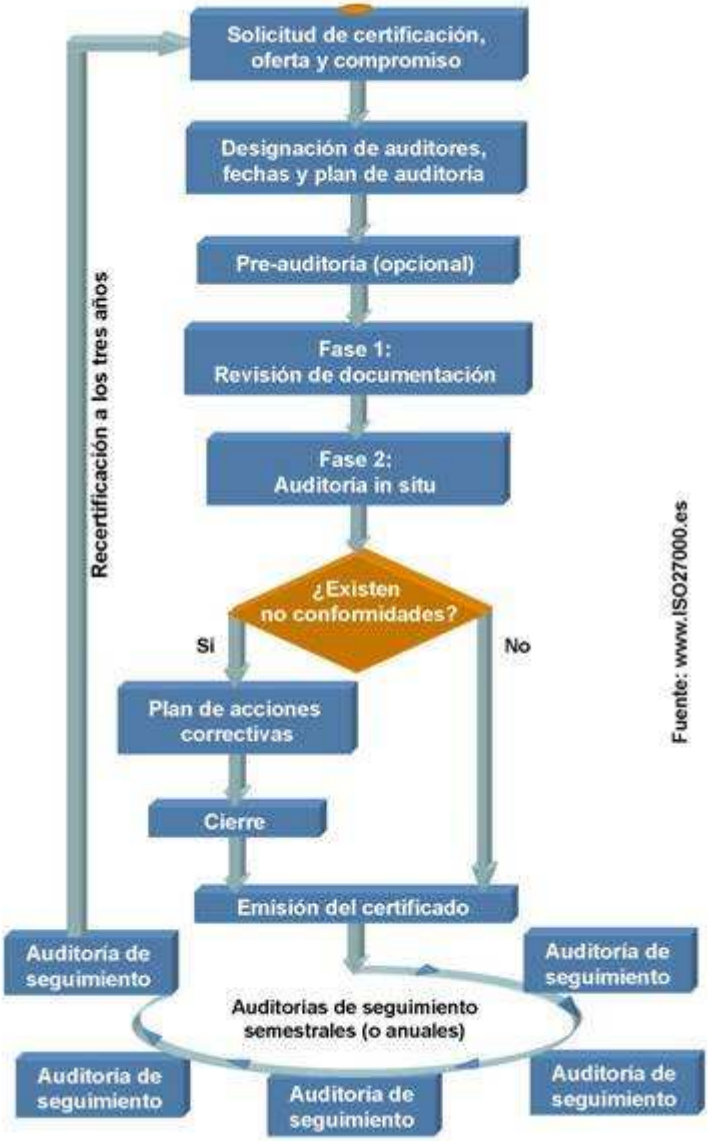
- Fase 2 de la auditoria: es la fase de detalle de la auditoria, en la que se revisan in situ las políticas, la implantación de los controles de seguridad y la eficacia del sistema

en su conjunto. Se inicia con una reunión de apertura donde se revisa el objeto, alcance, el proceso, el personal, instalaciones y recursos necesarios, así como posibles cambios de última hora. Se realiza una revisión de las exclusiones según la Declaración de Aplicabilidad (documento SOA), de los hallazgos de la Fase 1, de la implantación de políticas, procedimientos y controles y de todos aquellos puntos que el auditor considere de interés. Finaliza con una reunión de cierre en la que se presenta el informe de auditoria.

- Certificación: en el caso de que se descubran durante la auditoria no conformidades graves, la organización deberá implantar acciones correctivas; una vez verificada dicha implantación o, directamente, en el caso de no haberse presentado no conformidades, el auditor podrá emitir un informe favorable y el SGSI de organización será certificado según ISO 27001.

- Auditoria de seguimiento: semestral o, al menos, anualmente, debe realizarse una auditoria de mantenimiento; esta auditoria se centra, generalmente, en partes del sistema, dada su menor duración, y tiene como objetivo comprobar el uso del SGSI y fomentar y verificar la mejora continua. [5]

- Auditoria de re-certificación: cada tres años, es necesario superar una auditoria de certificación formal completa como la descrita.



Grafica Auditoria y Certificación

Las organizaciones certificadas a nivel mundial en ISO 27001 (o, anteriormente, en BS 7799-2) por entidades acreditadas figuran listadas en [5]http://www.iso27001certificates.com. Para aquellas organizaciones que lo han autorizado, también está publicado el alcance de certificación.

Naturalmente, la organización que implanta un SGSI no tiene la obligación de certificarlo. Sin embargo, sí es recomendable ponerse como objetivo la certificación, porque supone la oportunidad de recibir la confirmación por parte de un experto ajeno a la empresa de que se está gestionando correctamente la seguridad de la información, añade un factor de tensión y de concentración en una meta a todos los miembros del proyecto y de la organización en general y envía una señal al mercado de que la empresa en cuestión es confiable y es gestionada transparentemente. [5]

3.2.5 El auditor.

[5]El auditor es la persona que comprueba que el SGSI de una información se ha diseñado, implementado, verificado y mejorado conforme a lo detallado en la norma. En general, se distinguen tres clases de auditores:

- De primera parte: auditor interno que audita la información en nombre de sí misma, normalmente, como mantenimiento del sistema de gestión y como preparación a la auditoria de información;
- De segunda parte: auditor de cliente, es decir, que audita una información en nombre de un cliente de la misma; por ejemplo, una empresa que audita a su proveedor de outsourcing;
- De tercera parte: auditor independiente, que audita una información como tercera parte información; normalmente, porque la información tiene la intención de lograr la información y contrata para ello los servicios de una entidad de información.

El auditor, sobre todo si actúa como de tercera parte, ha de disponer también de una información personal. Esto quiere decir que, información un tercero, certifica que posee las competencias información y personales necesarias para desempeñar la labor de auditoria de la materia para la que está certificado.

En este punto, hay pequeñas diferencias entre las información certificadoras, que pueden formular requisitos distintos para homologar a sus auditores. Pero, en general, la información de auditores se ciñe a la norma ISO 19011 de información para la

auditoria de sistemas de gestión, que dedica su punto 7 a la competencia y evaluación de los auditores. Al auditor se le exigen una serie de atributos personales, conocimientos y informaciones, información formal, experiencia laboral y información como auditor. [5]

4. APLICACIÓN FORMATOS DE EVALUACION.

A continuación se dan a conocer los formatos en donde se encuentran los datos arrojados, después de haber realizado la evaluación tanto física como lógica de los laboratorios de informática de la universidad Minuto de Dios sede Calle 80 (laboratorio 209, 211, 212).

Evaluación física. (Ver anexo 1, 2)

Evaluación lógica. (Ver anexo 3)

5. TRABAJO DE CAMPO

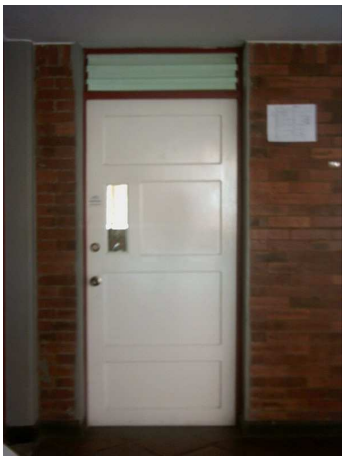
En este informe se hace un resumen de la forma como se realizo la evaluación tanto física como lógica de los laboratorios de informática 209 – 211 – 212.

5.1 Evaluación física.

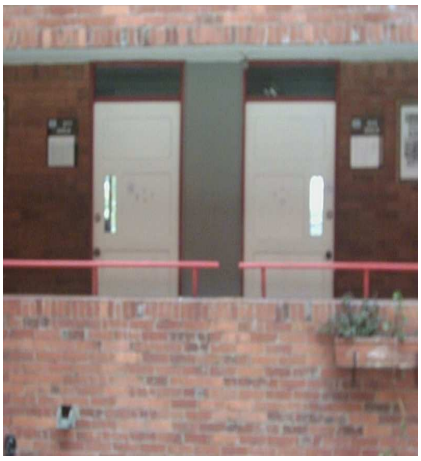
5.1.1 Laboratorio 209.

Se presentaron algunas dificultades, aún teniendo permiso del director del programa; mas, sin embargo, se sortearon los inconvenientes y se llegó a feliz termino con el trabajo de recolección de información, vital para el proyecto que presentamos.

De tal recolección de información, se desprende el siguiente análisis de la evaluación física en los laboratorios ya nombrados:



Entrada Laboratorio 209.



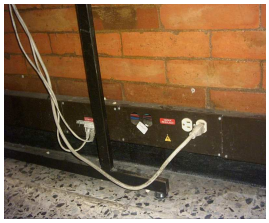
Entrada Laboratorios 211 – 212.

Con los permisos concedidos por GTL (Gestión de Tecnologías y Laboratorios) de Uniminuto, se dispone a realizar la respectiva evaluación, la cual nos lleva a sacar las conclusiones que están contempladas en los anexos (Conclusiones Evaluación Física).

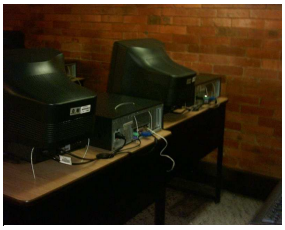
Interior Laboratorio 209 I

Interior Laboratorio 209 II

En medio de la evaluación física se encuentra una serie de fallos que se pondrán a disposición del lector de este documento para que también pueda sacar sus propias conclusiones (Laboratorio 209).

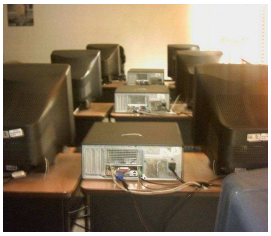


Deficiencia en canaleta



Host 94 y 95 no escaneo

Cable Host 98 desconectado



Espacio entre host es reducido

Cableado desordenado en un alto porcentaje

Toma corriente no regulada en regular estado

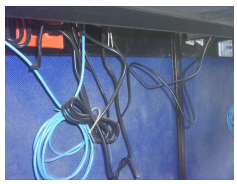
Interruptor en mal estado

Puntos de red marcación defectuosa

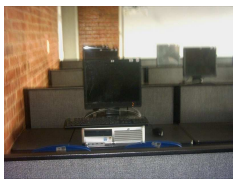
Equipos cerca a ventanas

5.1.2 Laboratorio 211

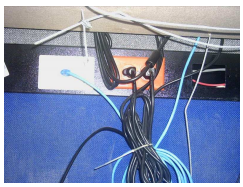
Las observaciones del laboratorio 209, también aplican para los laboratorios 211 y 212, adicionalmente, a continuación se referencian las fallas presentadas en estos laboratorios.



Cableado desordenado



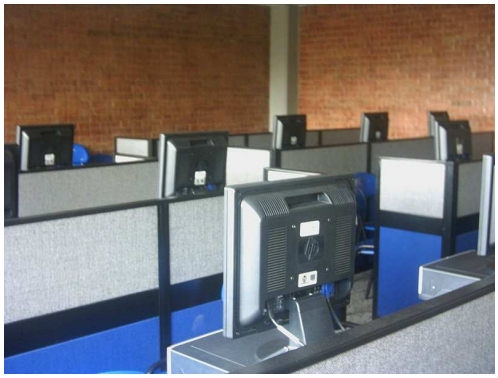
Bandejas del teclado estropeadas.



Puntos de red no están bien marcados

Equipos cerca de ventanas

5.1.3 Fallas generalizadas en todos los laboratorios.



Laboratorio 211

Los siguientes son datos estadísticos arrojados luego de haber realizado la evaluación física de los laboratorios de informática anteriormente descritos.

El 9% de los equipos están fuera de servicio.
El 19.6% tiene la tabla de soporte del teclado deteriorada.
El 100% presentan deficiencia en el acondicionamiento del cableado.
El 35.7% no cuentan con el espacio requerido entre máquinas.

En general el 100% de los laboratorios no cuentan con los requerimientos mínimos de seguridad que se describen a continuación:

No cuenta con piso elevado o cámara plena.
No existe un sistema de vigilancia las 24 horas a los centros de cómputo.
No existen alarmas para detección de fuego automática ni manual.
No cuentan con extintores.
No existen políticas para realizar simulacros en caso de tener que desalojar las instalaciones en caso de emergencia.
No se cuenta con máscaras contra gases o sistemas portátiles de oxígeno.

No se lleva un control sobre el número de violaciones en sucesión que la computadora ha tenido.

5.2 Evaluación lógica.

Se tomaron uno a uno, todos los host de los laboratorios de informática 209, 211 y 212, haciendo en cada uno de ellos un escaneo de vulnerabilidad con la ayuda del software especializado para tal fin, como es el MBSA (Microsoft Baseline Security Analizer), arrojando unos resultados donde se puede ver cada equipo con sus vulnerabilidades, tanto en idioma inglés como en español.

Éste informe, por su tamaño, nos obliga a anexarlo en medio magnético, donde se puede consultar por separado cada equipo con sus respectivos resultados de la evaluación, haciendo una descripción detallada de sus faltas críticas, paso de revisión, y demás datos arrojados.

A continuación encontraran un ejemplo de la evaluación lógica realizada al primer equipo del laboratorio 209, donde se describen las vulnerabilidades que este equipo tiene y el resultado donde paso la revisión, así como las recomendaciones a implementar, información adicional y las faltas no criticas.

	Nombre de computadora:	\ de LS6 - LS209 - de RGH 88	
	IP address:	192.168.1.107	
	Nombre de informe de seguridad:	LS6 - RGH - LS209 - 88 (16-06-2007 01-51 p.m..)	
	Escanee la fecha:	16/06/2007 las 01: 51 p.m..	
	Escanear con la versión de MBSA:	1.2.4013.0	
	Versión de base de datos de actualización de seguridad:	2007.6.12.0	
	Valoración de seguridad:	El riesgo grave (one or more cheques críticos fallaron.)	
	Resultados de examen de actualización de seguridad		
	Puntaje	Asunto	Resultado
		La seguridad de ventanas se actualiza	45 actualizaciones de seguridad críticas están faltantes. 7 actualizaciones de seguridad no podían ser confirmados.
			Lo que era el resultado escaneado detalla cómo corregir esto
		La seguridad de MV de Microsoft se actualiza	1 actualizaciones de seguridad críticas están faltantes.
			Lo que era el resultado escaneado detalla cómo corregir esto
		La jugador seguridad de medios de comunicación de ventanas se actualiza	1 actualizaciones de seguridad críticas están faltantes.
			Lo que era el resultado escaneado detalla cómo corregir esto
		Actualizaciones de seguridad de MSXML	2 productos están usando un paquete del servicio no en el más reciente versión o tener otras advertencias.
			Lo que era el resultado escaneado detalla cómo corregir esto
		Actualizaciones de seguridad de MDAC	Ninguna actualizacion de seguridad crítica está faltantes.
			Lo que fue escaneado
		Actualizaciones de seguridad de la oficina	Este examen puede ser llevado a cabo sobre una máquina local solamente.
	Resultados de examen de ventanas	Vulnerabilidades	
	Puntaje	Asunto	Resultado
		Prueba de contraseña de cuenta local	Algunas usuario cuentas (2 de 5) tienen contraseñas en blanco o simples, o no podían ser analizado.
			Lo que era el resultado escaneado detalla cómo corregir esto
		Autologon	Autologon es arreglado sobre esta computadora.
			Lo que fue escaneado cómo para corregir esto
		Restringir anónimo	La computadora está funcionando con = 0 de RestrictAnonymous. Este nivel previene la enumeración básica de usuario cuentas, políticas de cuenta, y información de sistema. Configure que = 2 de RestrictAnonymous asegure la seguridad máxima.
			Lo que fue escaneado cómo para corregir esto
		Expiración de contraseña	Algunas usuario cuentas (4 de 5) tienen contraseñas de non-expiring.
			Lo que era el resultado escaneado detalla cómo corregir esto
		Cortafuegos de ventanas	Este cheque fue pasado por alto porque no puede ser hecho remotamente.
		Actualizaciones automáticas	Las actualizaciones son descargadas automáticamente e instaladas sobre esta computadora.
			Lo que fue escaneado
		Sistema de ficheros	Todos drives de discos duros (2) están usando el sistema de ficheros de NTFS.
			Lo que era los detalles de Result escaneados
		Cuenta de invitado	La cuenta de invitado es minusválida sobre esta computadora.
			Lo que fue escaneado
		Administradores	Nada más que 2 administradores fueron encontrados sobre esta computadora.
			Lo que era los detalles de Result escaneados
		ES	
	Puntaje	Asunto	Resultado
		Auditoría	Permita la auditoría para eventos específicos como la entrada en el sistema / salga del sistema. Sea sure monitorear su diario de evento para estar atento al acceso no autorizado.
			Lo que fue escaneado cómo para corregir esto
		Servicios	Algunos servicios potencialmente superfluos son instalados.
			Lo que era el resultado escaneado detalla cómo corregir esto
		Acciones	3 acción (s) está presente sobre su computadora.
			Lo que era el resultado escaneado detalla cómo corregir esto
		Versión de ventanas	La computadora está operando Windows 2000 o más grande.
			Lo que fue escaneado
	Resultados de examen de servicios de información (el IIS) de Internet		
	Puntaje	Asunto	Resultado
		Estado de IIS	El IIS no está funcionando en esta computadora.
	Resultados de examen de SQL Server		
	Puntaje	Asunto	Resultado
		Estado de SQL Server / MSDE	SQL Server y/o MSDE no son instalado sobre esta computadora.
	Resultados de examen de aplicación		
	Vulnerabilidades		
	Puntaje	Asunto	Resultado
		Zonas de IE	Zonas de Explorer de Internet no tienen ajustes seguros para algunos usuarios.
			Lo que era el resultado escaneado detalla cómo corregir esto
		Seguridad de macro	4 producto de la oficina de Microsoft (s) es instalados. Algunos asuntos fueron encontrados.
			Lo que era el resultado escaneado detalla cómo corregir esto

Evaluación lógica - laboratorio 209

CONCLUSIONES

Luego de haber realizado la evaluación pertinente a los laboratorio de informática 209 – 211 – 212 de la Universidad Minuto de Dios sede principal (Bogotá), se llega a la conclusión que se deben implementar políticas de seguridad que sean acorde a una organización que quiere y hace esfuerzos por estar a la vanguardia en el manejo de la información por medios informáticos, pretendiendo automatizar cada vez mas las actividades que esta realiza para llegar a ser cada día mas eficientes, y poder mostrar con resultados y hechos los avances que en esta materia se vienen realizando.

Un buen método para poder medir el desempeño que ha tenido la Universidad Minuto de Dios en temas primordiales como el manejo de la información, es el realizado por los mismos estudiantes, pues quien mas si no ellos que son los que conocen y mantiene contacto permanente con los medios facilitados por la Universidad.

Basados en este concepto se realizo la evaluación física y lógica de los laboratorios de informática, con el fin de conocer a ciencia cierta las vulnerabilidades que pueden encontrarse en un laboratorio de informática de cualquier Universidad u Organización; Esperamos que la información suministrada este acorde con los principios informáticos que hablan sobre el buen manejo de la información y que sea un buen punto de partida a la hora de implementar políticas de seguridad que ayuden a llevar un control mas exacto sobre la administración de los recursos puestos a disposición de los estudiantes.

Anexo a este documento se encuentra un CD con los resultados de las vulnerabilidades que presentan los host (equipos) de los laboratorios de informática mencionados con anterioridad y que hay que tener en cuenta a la hora de realizar los correctivos pertinentes que lleven a mejorar el servicio prestado por los mismos.

Después de haber hecho la comparación de los resultados escaneo de los host de los laboratorios se puede ver que la totalidad de los equipos presentan vulnerabilidades en:

- Actualizaciones de seguridad. Actualizaciones de seguridad críticas están faltantes. Actualizaciones de seguridad no podían ser confirmadas.
- actualizaciones de seguridad críticas están faltantes.
- Varios productos están usando un paquete de servicio que no es la más reciente versión o tienen otras advertencias.
- Algunas usuario cuentas (2 de 5) tienen contraseñas en blanco o simplemente no pueden ser analizados.
- Autologin es arreglado sobre esta computadora.

La computadora está funcionando con = 0 de RestrictAnonymous. Este nivel previene la enumeración básica de usuario cuentas, políticas de cuenta, y información de sistema. Configure que = 2 de RestrictAnonymous asegure la seguridad máxima.
Zonas de Explorer de Internet no tienen ajustes seguros para algunos usuarios.
Restricción Anónima. Zonas de Explorer de Internet no tienen ajustes seguros para algunos usuarios.

Todos estos datos han sido sacados tomando como base la totalidad de los computadores de los tres laboratorios evaluados

Después de haber realizado la evaluación física al laboratorio de informática 209 se concluye lo siguiente:

Deficiencia en canaleta.

El host o computador número 94 cuya dirección ip debe ser la 192.168.1.113 no responde, no ejecuta orden y por consiguiente no se le puede hacer el escaneo correspondiente.

El host o computador número 95 cuya ip debe ser la 192.168.1.114 no responde, no ejecuta, aparece como no habilitado para conexión y por consiguiente no es posible hacerle el escaneo correspondiente.

El host o computador número 98 cuya ip debe ser la 192.168.1.117, el cable de poder que va desde la CPU (torre) hasta la toma de corriente no alcanza, es insuficiente para poderlo conectar.

El espacio entre los host (computador) no es suficiente ya que al pasar por entre estos en ocasiones se desconecta alguno de los cables conectados allí, ocasionando mal funcionamiento en los procesos que se estén realizando en los computador.

Cableado desordenado en un alto porcentaje (Estos cables comunican a los host con los puntos de red y con los puntos de de corriente regulada).

Tomas de corriente no regulada se encuentra en regular estado (Desprendida).

Interruptor para encender la luz del laboratorio (ubicado en la entrada del mismo), se encuentra en mal estado.

Los puntos de red no se encuentran bien marcados (marcación no visible o defectuosa).

Los equipos que se encuentran cerca de la ventana, están expuestos demasiado al sol.

Los equipos que se encuentran cerca de la ventana, están expuestos a posibles ataques.

No cuenta con piso elevado o cámara plena.

No existe un sistema de vigilancia las 24 horas a los centros de cómputo.

No existen alarmas para detección de fuego automática ni manual.

No cuentan con extintores.

No existen políticas para realizar simulacros en caso de tener que desalojar las instalaciones en caso de emergencia.

No se cuenta con máscaras contra gases o sistemas portátiles de oxígeno.

No se lleva un control sobre el número de violaciones en sucesión que la computadora ha tenido.

Después de haber realizado la evaluación física al laboratorio de informática 211 se concluye lo siguiente:

Cableado desordenado en un bajo porcentaje (Estos cables comunican a los host con los puntos de red y con los puntos de de corriente regulada).

Los muebles de cómputo del laboratorio informática se encuentran en regular estado a pesar de ser laboratorios nuevos y que deberían estar en perfecto estado, (Bandejas del teclado de los computadores se han ido estropeando frecuentemente).

Los puntos de red no se encuentran bien marcados (marcación no visible o defectuosa).

Los equipos que se encuentran cerca de la ventana, están expuestos demasiado al sol.

Los equipos que se encuentran cerca de la ventana están expuestos a posibles ataques.

No cuenta con piso elevado o cámara plena.

No existe un sistema de vigilancia las 24 horas a los centros de cómputo.

No existen alarmas para detección de fuego automática ni manual.

No cuentan con extintores.

No existen políticas para realizar simulacros en caso de tener que desalojar las instalaciones en caso de emergencia.

No se cuenta con máscaras contra gases o sistemas portátiles de oxígeno.

No se lleva un control sobre el número de violaciones en sucesión que la computadora ha tenido.

Después de haber realizado la evaluación física al laboratorio de informática 211 se concluye lo siguiente:

Cableado desordenado en un bajo porcentaje (Estos cables comunican a los host con los puntos de red y con los puntos de de corriente regulada).

Los muebles de cómputo del laboratorio informática se encuentran en regular estado a pesar de ser laboratorios nuevos y que deberían estar en perfecto estado, (Bandejas del teclado de los computadores se han ido estropeando frecuentemente).

Los puntos de red no se encuentran bien marcados (marcación no visible o defectuosa).

Los equipos que se encuentran cerca de la ventana, están expuestos demasiado al sol.

Los equipos que se encuentran cerca de la ventana están expuestos a posibles ataques.

No cuenta con piso elevado o cámara plena.

No existe un sistema de vigilancia las 24 horas a los centros de cómputo.

No existen alarmas para detección de fuego automática ni manual.

No cuentan con extintores.

No existen políticas para realizar simulacros en caso de tener que desalojar las instalaciones en caso de emergencia.

No se cuenta con máscaras contra gases o sistemas portátiles de oxígeno.

No se lleva un control sobre el número de violaciones en sucesión que la computadora ha tenido.

SUGERENCIAS

Laboratorio 209

	Fallas	Sugerencias
1	Cableado desordenado en un bajo porcentaje.	Ubicar ordenadores de cable.
2	Los muebles de cómputo del laboratorio informática se encuentran en regular estado	Dejar las bandejas estáticas y ponerles soportes adicionales, que logren evitar el constante deterioro de los muebles.
3	Los puntos de red no se encuentran bien marcados.	Realizar nueva marcación.
4	Los equipos que se encuentran cerca de la ventana, están expuestas demasiado al sol.	Realizar mantenimiento a las persianas que allí se encuentran.
5	Los equipos que se encuentran cerca de la ventana están expuestos a posibles ataques.	Poner rejillas o algún sistema que ayude a reducir este riesgo.
6	No cuenta con piso elevado o cámara plena.	Estudio de viabilidad para poder contar este requisito.
7	No existe un sistema de vigilancia las 24 horas a los centros de cómputo.	Estudio de viabilidad para poner controles como cámaras de seguridad, entre otros.
8	No existen alarmas para detección de fuego automática ni manual.	Estudio de viabilidad para la instalación de alarmas de detección de fuego y/o humo.
9	No existen políticas para realizar simulacros en caso de tener que desalojar las instalaciones en caso de emergencia.	Crear políticas que lleven a la realización de simulacros que prevengan contratiempos a la hora de presentarse una emergencia.
10	No se cuenta con máscaras contra gases o sistemas portátiles de oxígeno.	Estudio de viabilidad para poder contar con sistemas de seguridad como las máscaras contra gases tóxicos.
11	No se lleva un control sobre el número de violaciones en sucesión que la computadora ha tenido.	Llevar el control sobre el número de violaciones que pueda tener la computadora.

6.3.2 Laboratorio 211.

	Fallas	Sugerencias
1	Cableado desordenado en un bajo porcentaje.	Ubicar ordenadores de cable.
2	Los muebles de cómputo del laboratorio informática se encuentran en regular estado	Dejar las bandejas estaticas y ponerles soportes adicionales, que logren evitar el constante deterioro de los muebles.
3	Los puntos de red no se encuentran bien marcados.	Realizar nueva marcación.
4	Los equipos que se encuentran cerca de la ventana, están expuestas demasiado al sol.	Realizar mantenimiento a las persianas que allí se encuentran.
5	Los equipos que se encuentran cerca de la ventana están expuestos a posibles ataques.	Poner rejillas o algún sistema que ayude a reducir este riesgo.
6	No cuenta con piso elevado o cámara plena.	Estudio de viabilidad para poder contar este requisito.
7	No existe un sistema de vigilancia las 24 horas a los centros de cómputo.	Estudio de viabilidad para poner controles como cámaras de seguridad, entre otros.
8	No existen alarmas para detección de fuego automática ni manual.	Estudio de viabilidad para la instalación de alarmas de detección de fuego y/o humo.
9	No existen políticas para realizar simulacros en caso de tener que desalojar las instalaciones en caso de emergencia.	Crear políticas que lleven a la realización de simulacros que prevengan contratiempos a la hora de presentarse una emergencia.
10	No se cuenta con máscaras contra gases o sistemas portátiles de oxígeno.	Estudio de viabilidad para poder contar con sistemas de seguridad como las máscaras contra gases tóxicos.
11	No se lleva un control sobre el número de violaciones en sucesión que la computadora ha tenido.	Llevar el control sobre el número de violaciones que pueda tener la computadora.

6.3.3 Laboratorio 212.

	Fallas	Sugerencias
1	Cableado desordenado en un bajo porcentaje.	Ubicar ordenadores de cable.
2	Los muebles de cómputo del laboratorio informática se encuentran en regular estado	Dejar las bandejas estaticas y ponerles soportes adicionales, que logren evitar el constante deterioro de los muebles.
3	Los puntos de red no se encuentran bien marcados.	Realizar nueva marcación.
4	Los equipos que se encuentran cerca de la ventana, están expuestas demasiado al sol.	Realizar mantenimiento a las persianas que allí se encuentran.
5	Los equipos que se encuentran cerca de la ventana están expuestos a posibles ataques.	Poner rejillas o algún sistema que ayude a reducir este riesgo.
6	No cuenta con piso elevado o cámara plena.	Estudio de viabilidad para poder contar este requisito.
7	No existe un sistema de vigilancia las 24 horas a los centros de cómputo.	Estudio de viabilidad para poner controles como cámaras de seguridad, entre otros.
8	No existen alarmas para detección de fuego automática ni manual.	Estudio de viabilidad para la instalación de alarmas de detección de fuego y/o humo.
9	No existen políticas para realizar simulacros en caso de tener que desalojar las instalaciones en caso de emergencia.	Crear políticas que lleven a la realización de simulacros que prevengan contratiempos a la hora de presentarse una emergencia.
10	No se cuenta con máscaras contra gases o sistemas portátiles de oxígeno.	Estudio de viabilidad para poder contar con sistemas de seguridad como las máscaras contra gases tóxicos.
11	No se lleva un control sobre el número de violaciones en sucesión que la computadora ha tenido.	Llevar el control sobre el número de violaciones que pueda tener la computadora.

WEBGRAFÍA

[1] Wikipedia, URL http://es.wikipedia.org/wiki/ISO/IEC_17799.

[2] Tb.security, ISO 17799: La gestión de la seguridad de la información URL http:// http://www.tb-security.com/articles/iso_17799.pdf.

[3]ISO/IEC 17799:2005 e ISO/IEC 27001, URL http://www.seltika.com.co/index2.php?option=com_content&do_pdf=1&id=57 (Generated:27 July, 2007).

[4]Quality todas las referencias a los mejores documentos en el tema calidad, URL http://www.docquality.info/es/?f=40&d=12248&n=calidad+iso+17799+Introducci+a+la+Norma+ISO+17799+++UNLM.PDF&.

[5]Certificación, URL http://www.iso27000.es/doc_certificacion_all.htm

BIBLIOGRAFÍA.

UNIVERSIDAD DE LOS ANDES. Guía Para La Presentación De Propuestas De Tesis Y Proyectos De Grado. Facultad De Ingeniería. Departamento De Ingeniería Eléctrica Y Electrónica