ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

PROPUESTA PARA EL ANÁLISIS DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS LABORATORIOS DE COMPUTACIÓN DE LAS FACULTADES DE INGENIERÍA DE SISTEMAS DE LAS UNIVERSIDADES DE QUITO

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

CALDERÓN LÓPEZ DARÍO XAVIER

Mail: dx.calderon@gmail.com

SUNTAXI OÑA DIANA KARINA

Mail: uva_diana@yahoo.com

DIRECTOR: MSc. ING. JAIME NARANJO

Mail: jaime.naranjo@epn.edu.ec

QUITO, MARZO 2009

DECLARACIÓN

Nosotros, Diana Karina Suntaxi Oña y Darío Xavier Calderón López, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Diana Karina Suntaxi Oña

Darío Xavier Calderón López

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Diana Karina Suntaxi Oña y Darío Xavier Calderón López, bajo mi supervisión.

MSc. Ing. Jaime Naranjo

DIRECTOR DE PROYECTO

AGRADECIMIENTOS

A Dios por permitirme seguir compartiendo mi vida junto a mi familia y a las personas que amo, por ser mi guía durante todos estos años y darme fortaleza para seguir adelante en los momentos más difíciles, por mostrarme que ninguna tristeza es para siempre y que todo pasa por algo y será lo mejor para nosotros porque Él así lo quiere, porque aunque no me lo ha dicho sé que me quiere a pesar de todo ya que me lo demuestra cada día.

A mi mami María y a mi papi Juan quienes han confiado en mí y me han apoyado durante todos estos años. Con sus enseñanzas de fortaleza, humildad, trabajo y su amor me han demostrado que nada es imposible y que juntos con la bendición de Dios podremos alcanzar nuestros sueños.

A mi hermano Henry quien siempre me ha apoyado y ha estado pendiente de mí cuidándome, ha sido mi amigo, a quien quiero mucho y no lo cambiaría por nada del mundo.

Al Ing. Jaime Naranjo quien ha sido una guía, un amigo durante todo este trayecto, quien nos ha brindado su amistad, tiempo y paciencia. A él, al Ing. Francisco Villavicencio, Ing. Chicaiza, Ing. Pamela Flores, y a todos los ingenieros quienes nos mostraron su parte humana, nos sacaron una sonrisa, nos demostraron su humildad y su buen corazón, ellos me mostraron cómo debo ser; inclusive a los otros quienes por su arrogancia hacia la vida y hacia nosotros los alumnos me mostraron como no debo ser.

A Darío quien es mi mejor amigo, me ha tenido paciencia y con quien estamos logrando alcanzar una de nuestras metas, gracias por brindarme tu amistad, por ser humilde y sincero, gracias por no permitir que me rinda y por estar junto a mí.

DIANA

DEDICATORIA

Con mucho cariño para mis papás, mis abuelitos y toda mi familia, son lo mejor que tengo y le doy gracias a Dios porque aun puedo seguir compartiendo mi vida con ustedes.

A mis mejores amigos Daniel, Danilo, Charles y Henry quienes me han brindado su amistad y me han aceptado como soy con mis virtudes y muchos defectos. Sólo les puedo decir que sigan adelante sé que ustedes pueden alcanzar sus sueños yo por mi parte le apoyaré siempre.

A mis amigos de la universidad los Red Hat y RDS unos ya lograron esta meta mucho antes que yo, por quienes estoy muy feliz, ellos me demostraron que si se puede y a los otros que ya les falta poco, yo se que pueden no se rindan, todos podemos, se que pronto lo lograran.

A mis amigas de Betzy, Mery, Xime y todas las compañeras del fútbol quienes me brindaron su amistad, compartimos alegrías y tristezas, gracias por compartir conmigo una de mis más grandes ilusiones *el fútbol*.

A Darío, *lo logramos Daris* aunque parecía muy lejano lo logramos, por ti, por mi familia seguiré adelante, eres la mejor parte de mi vida, alcanzamos una meta pero aun faltan muchos sueños por cumplir, de todo corazón deseo que cumplas tus sueños y que Dios te bendiga, y me permita estar ahí junto a ti cuando lo logres.

DIANA

AGRADECIMIENTOS

Gracias a la vida que me ha dado todo.
Por enseñarme que: lo necesario fue hecho por el Señor y con eso es suficiente, ya que con ello puedo diferenciar entre la mediocridad y la excelencia.

A mi papi, Wilian Calderón, por ser la unión entre vida y sabiduría, por darme las lecciones de vida necesarias para poder llegar hasta aquí, viejo: NO SOY NADA MÁS QUE EL REFLEJO DE LO QUE HE APRENDIDO DE TI.

A mi mami, María López, por ser excelente madre por el ejemplo de entrega, dedicación, esmero y por ser el ejemplo para ponerme en los zapatos de otro y así renunciar a un poco de mí, pero para ganar mucho: TENEMOS MUY POCO EN LO MATERIAL, PERO TENEMOS LA UNIÓN Y AMOR DE TODA NUESTRA FAMILIA ASI QUE TERMINAMOS GANANDO.

A mis hermanos:
Santiago, por escucharme, por creerme en mi aunque me equivoque, por ser mi ingeniero de sonido (él sabe), por levantarse cuando cayó y ahora disfrutar de las lecciones de vida que aprendió. Pamelita, por ser la alegría de mis papás y por darme los abrazos inesperados justamente cuando los necesito.

A mis amigos:
Paúl, Franklin, Byron, John; por todos estos años en los cuales hemos vivido mucho, hemos aprendido de cada uno de nosotros, y siempre tomando de la mano a quien se quedaba atrás, ante todo el lema: "ENTRE TODO NO HACEMOS UNO" pero como dicta lo vivido y lo que vamos alcanzando, parece que somos mucho más, aunque el resto ni lo sospeche. Y a sus familias por abrirme las puertas de su hogar y por hacerte sentir parte de su familia.
Luchín, Tuki, Mix, Travieso, Kity, Geovy, Paty por ser mi segunda familia allá en la tierrita, y por su constante preocupación y apoyo, sin olvidarme de la Traviesa.

A toda mi familia:
Fanny, Luigi, Walter, Marlene, Enma; por el apoyo incondicional, por la mano extendida, por las conversaciones de donde aprendo mucho de ustedes por mostrarme la bello que es luchar por la familia y por sus consejos oportunos.
Mamá Charito, Papá Rafico; por criar a un hijo del que toda mi familia se siente orgulloso, y por su constante apoyo a nosotros directamente o indirectamente, a Ustedes: un Dios les pague.

Al Ingeniero Jaime Naranjo, por su apoyo y ayuda en el desarrollo de este proyecto de titulación, mil gracias.

A Uvis, mi regalo de Dios:
"Es poco lo que tengo para darte,
pero es mucho porque te lo doy todo,
puedo decirte por dónde hay que ir
pero no caminar por ti,
conmigo comerás poco pero soñarás mucho,
que es lo que importa
(la comida te sirve para hoy, el sueño para siempre)"

DARÍO

DEDICATORIA

Dedicado a mis padres: Wilian y María. Artífices de este objetivo.

A mis tíos Enma, Fanny, Walter y Luigi, por luchar cada día, y vencer las adversidades.

DARÍO

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

En el presente proyecto de titulación, Propuesta para el análisis de la Seguridad de la Información en los Laboratorios de Computación de las Facultades de Ingeniería de Sistemas de las universidades de Quito, desarrollado mediante las mejores prácticas de la Norma ISO 27001:2005; se tratarán varios aspectos importantes, los cuales se dividen en cada uno de los capítulos de la siguiente manera:

En el capítulo 1, se plantea que actualmente en las empresas tanto como las organizaciones, las universidades y sus Laboratorios, su más grande activo es la información; por esta razón la Seguridad de la Información posee una importancia decisiva en los Laboratorios para funcionar eficientemente. Se hace referencia a las diferentes metodologías para la evaluación de los sistemas informáticos y los estándares de seguridad. Se justifica el uso de la Norma ISO 27001:2005, junto con la exposición de sus propiedades más representativas, además se presenta las diferentes herramientas que se utilizarán para realizar la determinación del universo y de la muestra, y el análisis de la situación actual de los Laboratorios de Computación.

En el capítulo 2, se realiza el análisis del medio para lo cual se determina el universo de los Laboratorios de Computación de las Facultades de Ingeniería en Sistemas existentes en la ciudad de Quito, consecuentemente como el universo de Laboratorios de Computación es muy amplio, se selecciona una muestra representativa de la misma utilizando métodos estadísticos. Para finalizar se muestra la tabulación y el análisis de los resultados obtenidos mediante la aplicación de la encuesta.

En el capítulo 3, se desarrolla la propuesta basada en análisis del medio realizado en el segundo capítulo y en la Norma ISO 27001:2005. Además se detallan los

criterios, aplicabilidad y la manera del uso de la propuesta para la ejecución de la misma.
En el capítulo 4, se escoge un Laboratorio de Computación como caso de estudio y se aplica la propuesta en base al tercer capítulo.

Finalmente en el capítulo 5, se presentan las conclusiones y recomendaciones obtenidas tras la realización de este proyecto de titulación.

CAPÍTULO 1

FORMULACION DEL PROBLEMA Y SELECCIÓN DE HERRAMIENTAS

1.1 PLANTEAMIENTO DEL PROBLEMA

Las universidades como las empresas y organizaciones tienen información relevante, que son de suma importancia para el buen funcionamiento de las labores académicas y administrativas. Hoy en día las universidades y por ende en sus Laboratorios de Computación[1] no aplican medidas de seguridad consistentes para proteger la Confidencialidad, Integridad y Disponibilidad de la información y los datos, en esta época en que la información es el poder, esto se ve en las diferentes áreas u oficinas.

La seguridad de la Información posee una importancia decisiva en una organización para poder identificar y administrar cualquier tipo de actividad para funcionar eficientemente. A partir de esto se desarrollará la propuesta que nos permitirá realizar un análisis de la seguridad de la información, basada en las mejores prácticas de la Norma ISO 27001:2005, donde se analizará una muestra de las universidades de Quito para conocer cómo se está manejando actualmente la seguridad de la información y que a su vez permita conocer cómo se los debería manejar, ya que la seguridad de la información no es sólo problema tecnológico, sino además es un problema organizativo y de gestión. Esta propuesta permitirá que los Laboratorios de Computación de las universidades de Quito tengan una herramienta de ayuda al personal técnico, en caso de existir ataques a la información desde cualquier ángulo. Además, aportará a la seguridad

[1] Se entenderá como Laboratorio a toda la organización, cuya estructura está diseñada para que los recursos humanos, financieros, físicos, de información y otros, de forma coordinada, ordenada y regulada por un conjunto de normas, logren alcanzar ciertas metas y objetivos.

que deberían tener los Laboratorios de Computación de manera que puedan brindar continuidad, confiabilidad y servicio de calidad.

1.2 JUSTIFICACIÓN DEL USO DE LA NORMA ISO 27001:2005

El uso de estándares y metodologías para La seguridad de la Información es primordial para poder identificar y administrar cualquier tipo de actividad, ayudándonos además a organizar y gestionar la información. A continuación se definen algunas metodologías y la norma ISO 27001:2005, para comprender mejor cada una de ellas realizará un cuadro comparativo entre: ITIL, COBIT, y la NORMA ISO 27001:2005

ITIL

"La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (del inglés *Information Technology Infrastructure Library*), es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI). ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI." [2]

COBIT

"Objetivos de Control para la información y Tecnologías relacionadas (COBIT, en inglés: Control Objectives for Information and related Technology) es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información,(ISACA, en inglés: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute) en 1992."[3]

[2] Tomado de: http://es.wikipedia.org/wiki/ITIL
[3] Tomado de: http://es.wikipedia.org/wiki/COBIT

NORMA ISO 27001:2005

"El estándar para la seguridad de la información ISO/IEC 27001 (*Information technology - Security techniques - Information security management systems - Requirements*) fue aprobado y publicado como estándar internacional en Octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 17799 (actual ISO/IEC 27002) y tiene su origen en la revisión de la norma británica British Standard BS 7799-2:2002." [4]

Tabla 1: Tabla comparativa entre estándares

CARATERISTICAS	ITIL	COBIT	NORMA ISO 27001:2005
Ámbito	Gestión de Servicios TI, ITIL sintetiza un extenso conjunto de procedimientos de gestión, para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI.	Gobierno de TI, que es el sistema por el cual se dirigen y controlan las TI en la organización.	Seguridad de la Información.
Orientación	Definición de todos los procesos relacionados con la	Gobierno de TI que indica las reglas y procedimientos	Asegura la selección de los controles de seguridad

[4] Tomado de: http://es.wikipedia.org/wiki/ISO/IEC_27001

	administración de IT.	para la toma de decisiones sobre las TI.	adecuados y proporcionados para proteger la información.
Tamaño	Consta de: Dos libros centrales, que cubren las áreas de Soporte del Servicio y Prestación del Servicio.	Consta de: 4 dominios, 34 procesos de Tecnologías de Información y 318 objetivos de control.	Consta de: 39 objetivos de control y 133 controles.
Casos de Implementación	Cuando es necesario administrar eficientemente la infraestructura de IT, de manera de garantizar los niveles de servicio acordados entre la organización de IT y sus clientes.	Cuando es necesario asegurar la entrega del servicio y brindar una medida contra la cual poder juzgar cuando las cosas no vayan bien, ya que está enfocado fuertemente en el control y menos en la ejecución.	Cuando es necesario implantar o mantener controles para garantizar la Seguridad de la Información, ya que esta otorga una base común para el desarrollo de estándares de seguridad aplicables a una empresa en particular.
Fortalezas	Es independiente de los proveedores y de la tecnología. Está basado en los resultados de las mejores practicas	Se aplica a los sistemas de información de cualquier empresa, en sistemas distribuidos, computadoras	Diseñada para asegurar la selección de los controles de seguridad adecuados y proporcionados para

		personales y mini computadoras.	proteger la información y dar la confianza a partes interesadas incluyendo a los clientes de una empresa.
Debilidades	Lo complejo y costoso que resulta su implantación en grandes organizaciones, la gran dificultad tarea de mantener actualizada y perfectamente funcionando la CMDB Configuration Management Data Base), y el control de los cambios.	Está orientada al Gobierno de TI, por esta razón nos fuerte en seguridad.	Es necesario para su éxito el compromiso total de la Dirección y una definición clara del alcance.

La norma ISO/IEC 27001:2005, es la evolución certificable del código de buenas prácticas ISO 17799, la diferencia entre las dos radica en una nueva cláusula llamada *Gestión de Incidencias de Seguridad de la Información*. Asegura una adecuada implantación, gestión y operación de todo lo relacionado con la implantación de un SGSI (Sistema de Gestión de la seguridad de la Información), siendo la norma más completa que existe en para la implantación de controles, métricas e indicadores mediante la cual permite crear un marco adecuado de gestión de la seguridad de la información para las organizaciones.

Además, los motivos por los cuales se ha escogido la NORMA ISO 27001:2005, se deben principalmente al ámbito de la Norma que es la Seguridad de la Información, mientras que en COBIT es Gobierno de TI y en ITIL es la Gestión de Servicios TI, lo cual no está direccionado a nuestra propuesta.

Las universidades deben proteger su información y datos, para lograr un buen funcionamiento y eficiencia en los servicios que otorgan, la NORMA ISO 27001:2005 está diseñada para asegurar la selección de los controles de seguridad adecuados y proporcionados para proteger la información.

ORIGEN DE LAS NORMAS ISO 27001

"Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

1979 Publicación BS 5750 - ahora ISO 9001

1992 Publicación BS 7750 - ahora ISO 14001

1996 Publicación BS 8800 - ahora OHSAS 18001

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

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

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información." [5]

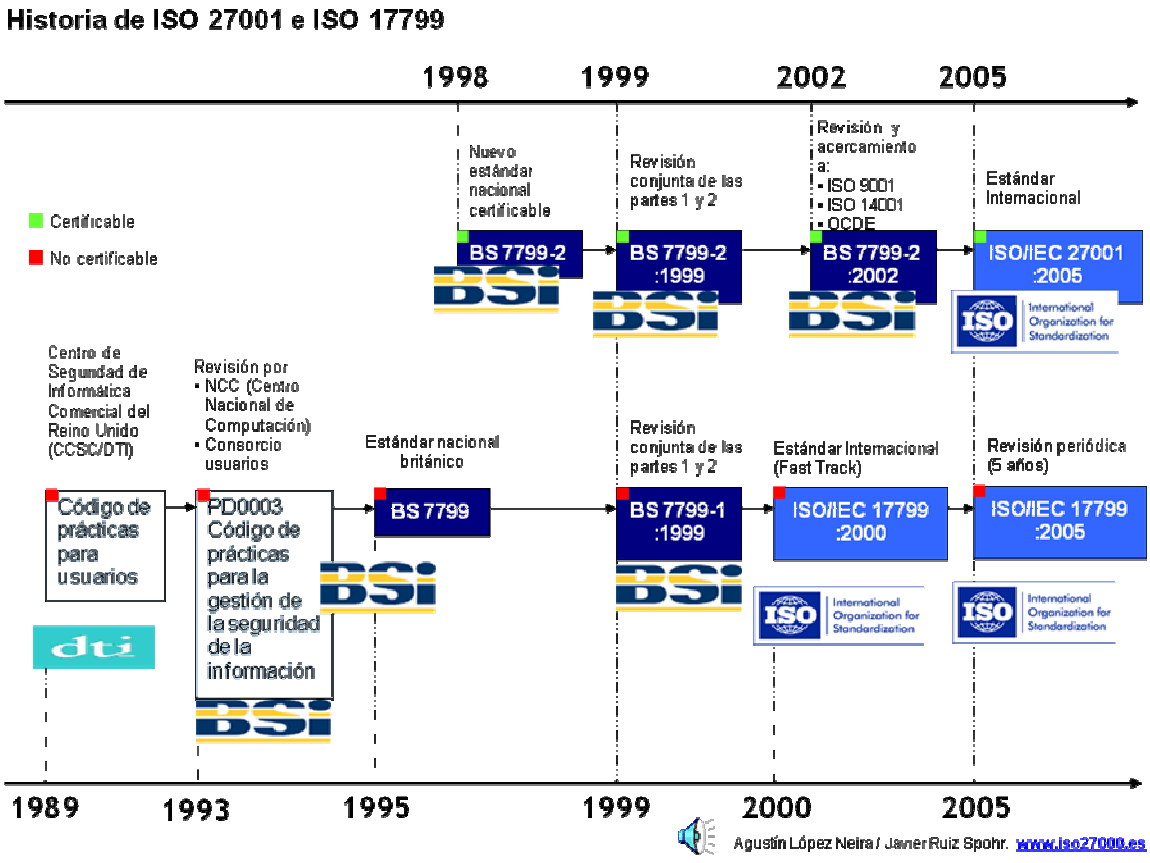


Gráfico 1: Historia de ISO 27001 e ISO 17799

[5] Tomado de http://www.iso27000.es/sgsi.html

DEFINICIÓN DE LAS NORMAS ISO 27000

La serie ISO 27000 es una Familia de Estándares internacionales para Sistemas de Gestión de Seguridad de la Información (SGSI), que propone requerimientos de sistemas de gestión de seguridad de la información, gestión de riesgo, métricas y medidas, guías de implantación, vocabulario y mejora continua.

ISO 27000

"La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

En este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001." [6]

ISO 27001

"Este Estándar Internacional abarca todos los tipos de organizaciones (por ejemplo; empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro). Este Estándar Internacional especifica los requerimientos para

[6] Tomado de: http://www.iso27000.es/iso27000.html

establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos comerciales generales de la organización. Especifica los requerimientos para la implementación de controles de seguridad personalizados para las necesidades de las organizaciones individuales o partes de ella." [7]

El SGSI está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes interesadas.

ESTABLECER Y GESTIONAR UN SGSI [8]

Para poder establecer y gestionar un SGSI, este Estándar Internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA- Círculo de Deming; **P**lan, **D**o, **C**heck, **A**ct), el cual se puede aplicar a todos los procesos SGSI, como lo muestra el Gráfico 2.

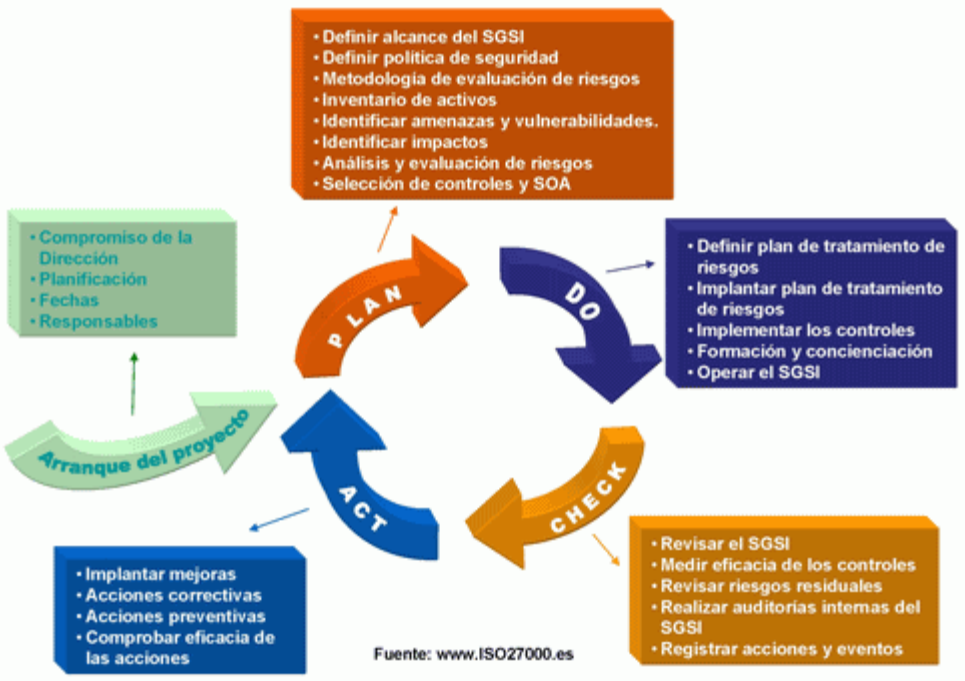


Gráfico 2: PDCA Establecer y gestionar un SGSI

[7] Tomado de: ESTÁNDAR INTERNACIONAL ISO/IEC 27001
[8] Tomado de: http://www.iso27000.es/iso27000.html

A continuación se describen los pasos a seguir para establecer y gestionar un SGSI:

Arranque del proyecto

- Compromiso de la Dirección
- Planificación, fechas, responsables

Planificación

- Definir alcance del SGSI (Sistema de Gestión de la seguridad de la Información)
- Definir política de seguridad
- Definir el enfoque de evaluación de riesgos
- Inventario de activos
- Identificar amenazas y vulnerabilidades
- Identificar los impactos
- Análisis y evaluación de los riesgos
- Identificar y evaluar opciones para el tratamiento del riesgo
- Selección de controles
- Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI
- Confeccionar una Declaración de Aplicabilidad

Implementación

- Definir plan de tratamiento de riesgos
- Implantar plan de tratamiento de riesgos
- Implementar los controles
- Formación y concienciación
- Desarrollo del marco normativo necesario
- Gestionar las operaciones del SGSI
- Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

Seguimiento

- Ejecutar procedimientos y controles de monitorización y revisión
- Revisar regularmente la eficacia del SGSI
- Medir la eficacia de los controles
- Revisar regularmente la evaluación de riesgos
- Realizar regularmente auditorías internas
- Revisar regularmente el SGSI por parte de la Dirección
- Actualizar planes de seguridad
- Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI

Mejora continua

- Implantar mejoras
- Acciones correctivas
- Acciones preventivas
- Comunicar las acciones y mejoras
- Asegurarse de que las mejoras alcanzan los objetivos pretendidos

1.3 SELECCIÓN DE HERRAMIENTAS

A continuación se exponen las herramientas que se utilizarán en esta propuesta para el análisis de la Seguridad de la Información en los Laboratorios de Computación de las Facultades de Ingeniería de Sistemas de las universidades de Quito.

1.3.1 HERRAMIENTAS PARA LA DETERMINACIÓN DEL UNIVERSO Y LA MUESTRA

DETERMINACIÓN DEL UNIVERSO

Se determinará el universo del cual se obtendrá la información necesaria para realizara la propuesta y la manera de cómo se obtendrá la muestra de dicha población, esto se lo realizará de la siguiente manera:

- ***Primer Paso.-*** Definir la unidad de análisis (qué va a ser medido, es decir, los objetos de estudio).

- ***Segundo Paso.-*** Delimitar la población, tomando solamente los casos que concuerdan con una serie de especificaciones, mediante criterios de definición.

DETERMINACIÓN DEL TAMAÑO DE LA MUESTRA

Para la determinación del tamaño la muestra se debe tener en cuenta varios factores: el tipo de muestreo, el parámetro a estimar, el error muestral admisible, la varianza poblacional y el nivel de confianza. Entonces, a continuación se explicará como delimitar estas variables:

- ***Primer Paso:*** *Determinar la probabilidad a favor (variable p) y probabilidad en contra (variable q).* Esto quiere decir, determinar la posibilidad de que un elemento de la población esté incluido o no en la muestra seleccionada.

- ***Segundo Paso:*** *Cálculo del error muestral (variable e).* Nos indica la variabilidad de las estimaciones de muestras repetidas en torno al valor de la población, nos da una noción clara de hasta dónde una muestra se aleja del valor que se hubiera obtenido por medio de un censo completo. Para poder obtener una muestra representativa el error debe oscilar entre el 10% y el 15%.

- ***Tercer Paso.-*** *Nivel de Confianza (variable* $Z_{\alpha/2}$*)*. Es la Probabilidad de que la estimación efectuada se ajuste a la realidad. $Z_{\alpha/2}$ es el nivel de confianza elegido, determinado por el valor de α. Es una

variable estandarizada y sus valores se muestran en la siguiente tabla[9] .

Tabla 2: Tabla de probabilidad acumulada de la Ley De Distribución Normal Estándar

Valores de $Z\,^{\alpha}/_{2}$ más utilizados, según el valor de α:

% Confianza	90%	95%	99%	99,9%
α/2	0,10	0,05	0,01	0,001
$Z_{\alpha/2}$	1,645	1,960	2,576	3,291

- ***Cuarto paso.-*** *Cálculo del tamaño de la muestra.* Para calcular el tamaño de la muestra se utilizará la siguiente Fórmula Matemática del muestreo Aleatorio. [10]

$$n = \frac{NZ_{\alpha/2}{}^{2}pq}{(N-1)e^{2} + Z_{\alpha/2}{}^{2}pq}$$

Donde:

$Z_{\alpha/2}$= Nivel de confianza (variable estandarizada)

N= Universo de investigación

p = Probabilidad a favor

q = Probabilidad en contra (1-p)

e = Error de estimación

n = Tamaño de la muestra

[9] Tomada de: http://www.isciii.es/htdocs/redes/investen/publicaciones/calculo_muestra.pdf

[10] Tomada de: Libro Estadística para la Administración y la Ingeniería, Galindo D. Edwin

1.3.2 HERRAMIENTAS PARA EL ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS LABORATORIOS DE COMPUTACIÓN

La herramienta escogida es la **encuesta**, ya que mediante ésta podemos obtener información precisa de cómo se está manejando la seguridad en los Laboratorios de Computación. Esto se lo realizará de la siguiente manera:

- ***Primer Paso.-*** *Seleccionar las universidades de acuerdo al tamaño de la muestra,* aquí se determinará que universidades son las más factibles y nos puedan brindar su colaboración sin mayor problema, en base a nuestros propios criterios.

- ***Segundo Paso.-*** *Elaboración de la encuesta*, la encuesta estará basada en otras presentadas en anteriores proyectos de titulación y en los aspectos más sobresalientes de la Norma ISO 27001 que nos ayuden a obtener una correcta y más asertiva información.

- ***Tercer Paso.-*** *Visita a las universidades seleccionadas,* a cada una de las universidades objeto de investigación, se realizará una entrevista previa a una persona considerada clave (director de la organización, jefe de Laboratorio) y de ser necesario se pedirá autorización al Decano de la Facultad; en la entrevista previa se realizará una exposición sobre los objetivos de nuestra propuesta y los resultados que se obtendrán al final de misma.

- ***Cuarto Paso.-*** *Entrega de Encuestas,* una vez obtenida la autorización para realizar la investigación se entregará las encuestas para que sean llenadas por el personal (es) a cargo de los Laboratorios de Computación, en los días y horas que ellos indiquen.

- ***Quinto Paso.-*** *Obtención de Resultados,* se retirará las encuestas llenadas de cada una de las universidades seleccionadas para la

investigación. Con esta información se podrá analizar los resultados. La información será clasificada e interpretada con la ayuda de gráficos para obtener un análisis más claro.

CAPÍTULO 2

ANÁLISIS DEL MEDIO

2.1 DETERMINACIÓN DEL UNIVERSO Y TAMAÑO DE LA MUESTRA

2.1.1 DETERMINACIÓN DEL UNIVERSO

El *primer paso* es definir la unidad de análisis, para esto ya tenemos planteado que serán los Laboratorios de Computación de las Universidades Quito.

El *segundo paso* es delimitar la población, la cual serán las facultades de Ingeniería en Sistemas de las Universidades de Quito. El tamaño de la población se determinará en base a los criterios señalados en la Tabla 3.

Tabla 3: Criterios utilizados para determinar la población

CATEGORIA	CRITERIOS	TAMAÑO
Universidades	• Que estén legalmente registradas en el CONESUP. • **Que se encuentren situadas en la ciudad de Quito.** • **Que tengan Carreras en Ingeniería en Sistemas.**	17

En consecuencia, se ha determinado que el tamaño de la población es 17 universidades, q**ue tienen la Facultad de Ingeniería en Sistemas en la ciudad**

de Quito y que están debidamente acreditadas en el CONESUP. (Ver Anexo 1)

2.1.2 DETERMINACION DEL TAMAÑO DE LA MUESTRA

Para definir el tamaño de la muestra se tomará en consideración los siguientes datos:

El Primer paso es tomar la probabilidad a favor, para esto se tomará como dato que el 98% de las universidades contestan las encuestas, lo que equivale a p = 0.98 y por lo tanto a un q= 0.02.

El Segundo paso es determinar el margen de error, el recomendado para este tipo de investigación es del 10%, el cual da como dato e = 0.10.

El Tercer paso es determinar el Nivel de Confianza como se indica en la tabla de probabilidad acumulada de la ley de distribución normal estándar *(ver tabla 2),* para una confianza del 90% el valor de $Z_{\alpha/2}$ es 1,645.

El Cuarto paso es determinar El tamaño de la Muestra, como ya se tiene el tamaño de la población obtenido del Universo de investigación definido anteriormente, N = 17 *(ver tabla 3)*; entonces procedemos a reemplazar en la fórmula los siguientes valores:

Tabla 4: Valores para determinar el tamaño de la muestra

VARIABLE	VALOR
Probabilidad a favor	0.98
Probabilidad en contra	0.02
Error	0.10

Nivel de confianza	1.645
Universo de investigación	17

$$n = \frac{1.645^2 0.98x0.02x17}{(17-1)0.1^2 + 1.645^2 0.90x0.10}$$

$$n = 4{,}233$$

Finalmente, el tamaño de la muestra resultante es de 4 universidades, las cuales van a ser evaluadas mediante encuestas para poder analizar de la situación actual de la seguridad de la información en sus Laboratorios de Computación.

2.2 ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN LOS LABORATORIOS DE COMPUTACIÓN

Primeramente se seleccionó a las cuatro universidades de *acuerdo* al tamaño de la muestra, que nos ayudarán a realizar la investigación. (Ver Anexo 2).

A continuación se elaboró una encuesta basada en otras presentadas en anteriores proyectos de titulación y en los aspectos más sobresalientes de la Norma ISO 27001 denominada ***ENCUESTA DE SEGURIDADES DE LA INFORMACIÓN*** (Ver Anexo 3).

Se realizó las visitas a las universidades seleccionadas para la investigación, se hizo la encuesta al Jefe de Laboratorio de cada uno de los Laboratorios de las universidades, no fue necesario pedir una autorización al Decano de la Facultad en ningunas de las universidades, en la entrevista previa se realizó una

exposición sobre los objetivos de nuestra propuesta y los resultados que se obtendrán al final de la misma.

En la mayoría de las universidades se nos entrego la encuesta debidamente llenada el mismo día, pero en las otras se nos pidió acudiéramos al día siguiente. Con esta información se analizará los resultados.

2.2.1 TABULACIÓN DE RESULTADOS

La encuesta planteada se ha divido en siete áreas tomadas de los temas más relevantes de seguridad de la información de la Norma ISO 27001:2005, para permitirnos un análisis global y son: *Control de Accesos, Organización de la Seguridad, Seguridad Física y del Ambiente, Seguridad de los Recursos Humanos, Gestión de Comunicaciones y Operaciones, Administración de los Activos y Administración de Incidentes.* Cada área tiene sus temas correspondientes los cuales fueron tomados de las preguntas de la encuesta. A continuación se detallan los resultados obtenidos en las encuestas realizadas a las 4 universidades:

Tabla 5: Tabulación de la Encuesta Elaborada

TEMA ENCUESTADO	**SI**		**PARCIALMENTE**		**NO**		**TOTAL**	
	Número	**%**	Número	**%**	Número	%	Número	**%**
Control de Accesos								
Controles de seguridad para el acceso a la información	2	**50%**	2	**50%**	0	**0%**	4	**100%**
Clasificación y monitoreo de tipos de acceso al	3	**75%**	1	**25%**	0	**0%**	4	**100%**

sistema de información								
Política de contraseñas seguras	3	**75%**	1	**25%**	0	**0%**	4	**100%**
Organización de la Seguridad								
Responsabilidades definidas para la protección de los equipos y control de cumplimiento de procesos de seguridad	3	**75%**	1	**25%**	0	**0%**	4	**100%**
Profesional a cargo de asegurar la consistencia y ayudar a la toma de decisiones	1	**25%**	1	**25%**	2	**50%**	4	**100%**
Seguridad Física y del Ambiente								
Controles de seguridad para impedir el acceso a terceros	3	**75%**	1	**25%**	0	**0%**	4	**100%**
Perímetros de seguridad en las áreas más vulnerables	1	**25%**	1	**25%**	2	**50%**	4	**100%**
Protección de los equipos contra apagones	1	**25%**	2	**50%**	1	**25%**	4	**100%**

Protección física de los equipos contra desastres naturales o creados por el hombre	0	**0%**	1	**25%**	3	**75%**	4	**100%**
Protección del cableado de energía y telecomunicación	3	**75%**	0	**0%**	1	**25%**	4	**100%**
Seguridad de los Recursos Humanos								
Roles y responsabilidades a empleados y terceros de acuerdo a políticas de seguridad	0	**0%**	2	**50%**	2	**50%**	4	**100%**
Verificación de antecedentes de los candidatos a empleados, contratista y terceros	2	**50%**	0	**0%**	2	**50%**	4	**100%**
Capacitación acerca de la seguridad de la información	0	**0%**	3	**75%**	1	**25%**	4	**100%**
Proceso disciplinario para los empleados	1	**25%**	1	**25%**	2	**50%**	4	**100%**

Gestión de Comunicaciones y Operaciones								
Licencias de Software	2	**50%**	2	**50%**	0	**0%**	4	**100%**
Actualización de Antivirus en todos los equipos	4	**100%**	0	**0%**	0	**0%**	4	**100%**
Política de obtención de copias de seguridad	1	**25%**	3	**75%**	0	**0%**	4	**100%**
Almacenamiento de los respaldos en lugar alejado y seguro	2	**50%**	0	**0%**	2	**50%**	4	**100%**
Medios de almacenamiento probados regularmente	1	**25%**	1	**25%**	2	**50%**	4	**100%**
Procedimientos para monitorear el uso de la información	3	**75%**	1	**25%**	0	**0%**	4	**100%**
Existencia de logs de auditoría	1	**25%**	2	**50%**	1	**25%**	4	**100%**
Planes de contingencia para recuperar la información	0	**0%**	3	**75%**	1	**25%**	4	**100%**
Revisión y actualización de los Planes de	1	**34%**	1	**33%**	1	**33%**	3	**100%**

contingencia								
Revisión y actualización Políticas de seguridad	1	**34%**	1	**33%**	1	**33%**	3	**100%**
Evaluación regular de los sistemas de información	2	**67%**	0	**0%**	1	**33%**	3	**100%**
Política de seguridad publicada y comunicada	2	**67%**	0	**0%**	1	**33%**	3	**100%**
Actividades para tratar sobre la seguridad de la información	2	**67%**	1	**33%**	0	**0%**	3	**100%**
Administración de los Activos								
Inventario de los activos	4	**100%**	0	**0%**	0	**0%**	4	**100%**
Reglas para el uso de la información y de los activos	4	**100%**	0	**0%**	0	**0%**	4	**100%**
Clasificación de la información en términos de su valor, confidencialidad y grado crítico	3	**75%**	1	**25%**	0	**0%**	4	**100%**

Control para impedir la salida de equipos, información o software de las instalaciones	2	**50%**	1	**25%**	1	**25%**	4	**100%**
Mantenimiento de los equipos	3	**100%**	0	**0%**	0	**0%**	3	**100%**
Administración de Incidentes								
Registros de incidentes de seguridad y de las acciones tomadas	0	**0%**	3	**75%**	1	**25%**	4	**100%**

2.2.2 ANÁLISIS DE RESULTADOS

Se realizará un análisis por las siete áreas y un análisis global para conocer cómo se maneja la seguridad de la información. Los gráficos y su respectivo análisis de cada una de las preguntas o temas mostrados en la *Tabla 5* se los presenta en el ANEXO 4.

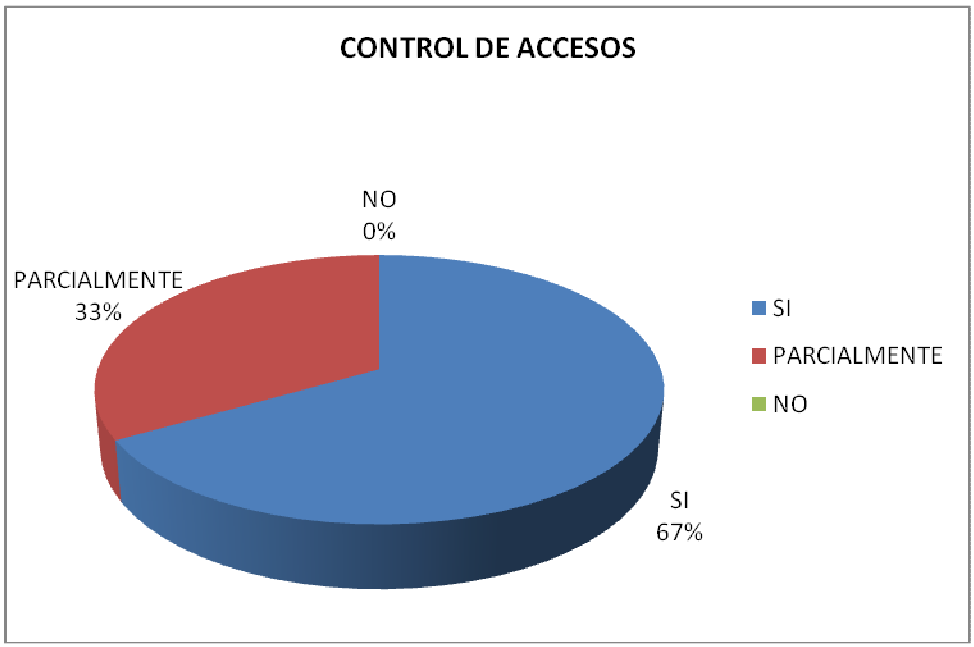
Para realizar el análisis de resultados se tomará como referencia el cuadro de interpretación conforme lo sugiere COSO Sponsoring Organizations of the Treadway Commission (Ver Anexo 5).

2.2.2.1 Control de Accesos

Esta área se refiere al Control de acceso a la información, al aseguramiento del acceso del usuario autorizado, evitar el acceso no autorizado a los sistemas de información y a evitar el acceso de usuarios no autorizados.

En la mayoría de los Laboratorios de Computación sí existe un Control de Accesos. Mediante este análisis se ha determinado que el grado de confianza que se tiene es A (Alto) y el nivel de riesgo es B (Bajo). Para el desarrollo de la propuesta en este punto se sugerirá su aplicación en caso de no considerarse aun en las normas o políticas de seguridad de la información de los Laboratorios, ya que una gran mayoría ya lo considera.

Gráfico 3: Control de Accesos



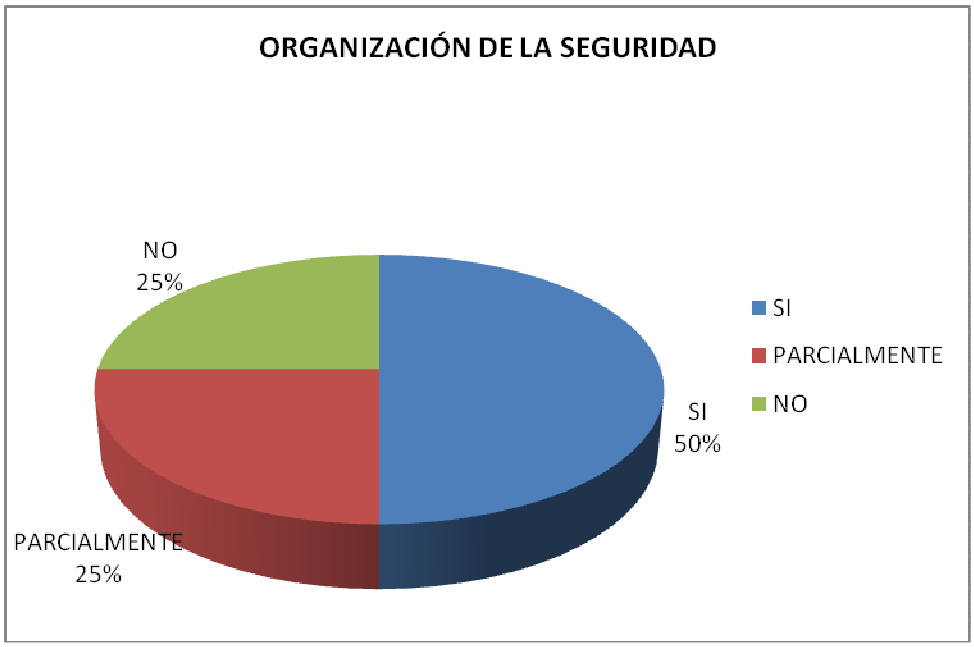
2.2.2.2 *Organización de la Seguridad*

Esta área se refiere al manejo de la seguridad de la información dentro de la organización, en este caso de los Laboratorios de Computación. Mantener la seguridad de la información de la organización y los medios de procesamiento de información.

En la mayoría de los Laboratorios de Computación sí existe Organización de la Seguridad o lo realiza parcialmente. Mediante este análisis se ha determinado que el grado de confianza que se tiene es M (Moderado) y el nivel de riesgo es M

(Moderado). Por lo tanto será tomado en cuenta con mayor énfasis para la elaboración de la propuesta.

Gráfico 4: Organización de la Seguridad

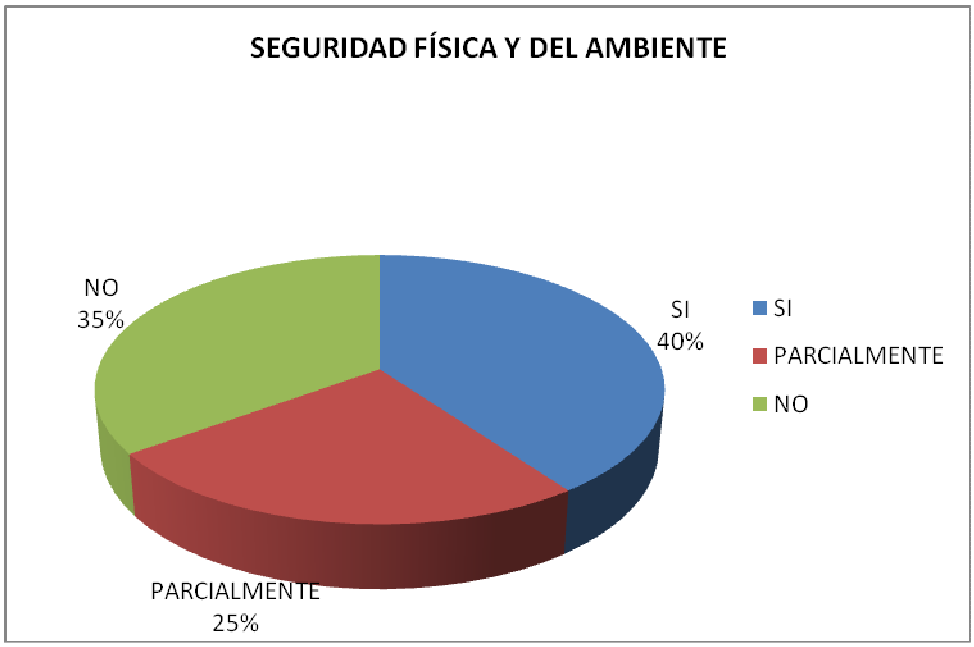


2.2.2.3 *Seguridad Física y del Ambiente*

En esta área se requiere evitar el acceso físico no autorizado, daño e interferencia al local y la información del Laboratorio. Evitar la pérdida, daño, robo o compromiso de los activos o información y la interrupción de las actividades del Laboratorio.

No todos los Laboratorios cuentan con una seguridad física y del ambiente, existe una parte considerable que no lo hace de la manera correcta. Mediante este análisis se ha determinado que el grado de confianza que se tiene es M (Moderado) y el nivel de riesgo es M (Moderado). Por lo tanto será tomado en cuenta con mayor énfasis para la elaboración de la propuesta.

Gráfico 5: Seguridad Física y del Ambiente

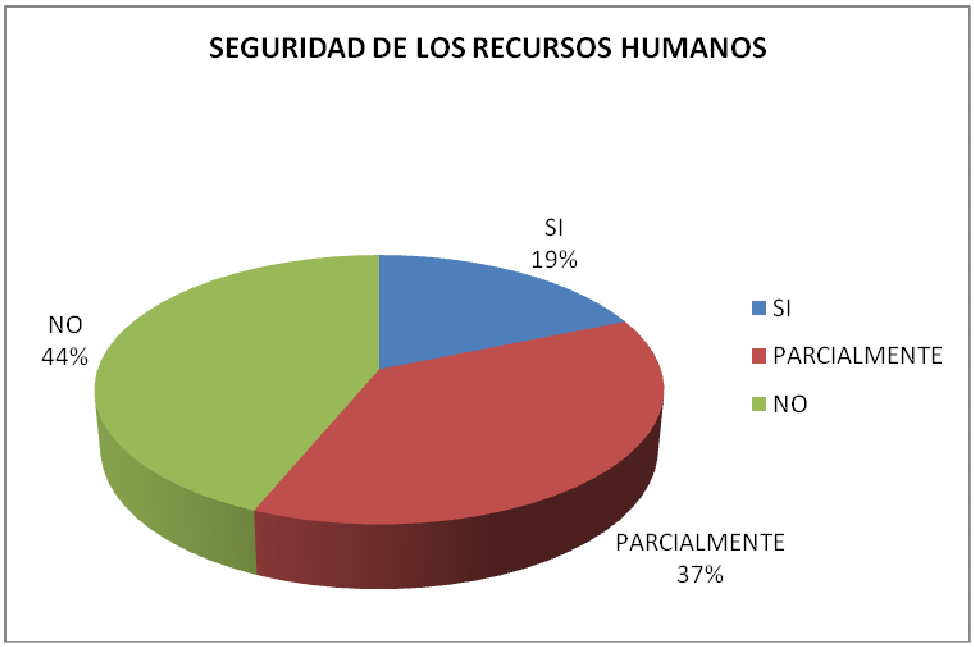


2.2.2.4 *Seguridad de los Recursos Humanos*

Esta área se refiere a asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; para así reducir el riesgo de robo, fraude o mal uso de los medios. Se requiere asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas e inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones.

Existe muy poca Seguridad de los Recursos Humanos, una considerable parte de los Laboratorios no lo hace como es correcto. Mediante este análisis se ha determinado que el grado de confianza que se tiene es B (Bajo) y el nivel de riesgo es A (Alto). Por lo tanto será tomado en cuenta con mayor énfasis para la elaboración de la propuesta.

Gráfico 6: Seguridad de los Recursos Humanos

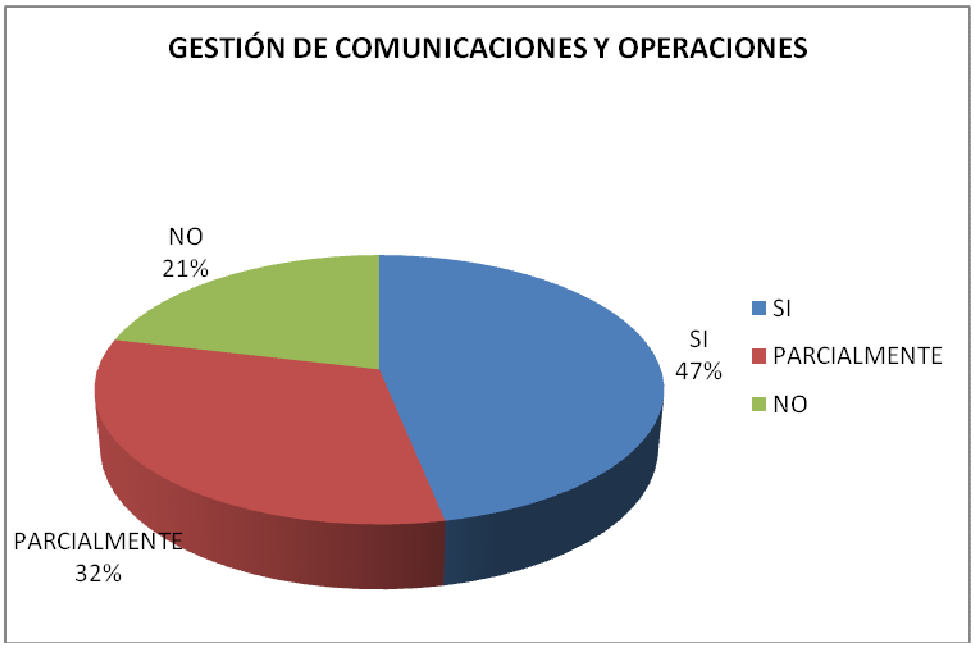


2.2.2.5 Gestión de Comunicaciones y Operaciones

Esta área se refiere a asegurar la operación correcta y segura de los medios de procesamiento de la información.

La mayor parte de los Laboratorios realiza la Gestión de Comunicaciones y Operaciones, una mínima parte no lo hace. Mediante este análisis se ha determinado que el grado de confianza que se tiene es M (Moderado) y el nivel de riesgo es M (Moderado). Por lo tanto será tomado en cuenta con mayor énfasis para la elaboración de la propuesta.

Gráfico 7: Gestión de Comunicaciones y Operaciones

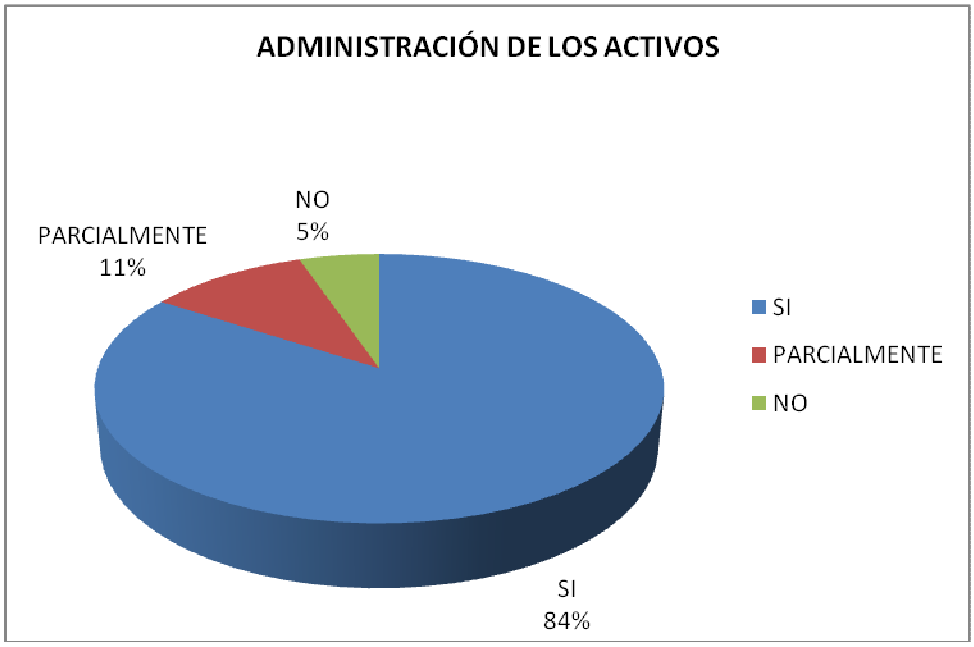


2.2.2.6 Administración de los Activos

Esta área se refiere a lograr y mantener la protección apropiada de los activos organizacionales y asegurar que la información reciba un nivel de protección apropiado.

La mayoría de los Laboratorios cuentan con una Administración de los Activos, una pequeña parte no lo hace de la manera correcta. Mediante este análisis se ha determinado que el grado de confianza que se tiene es A (Alto) y el nivel de riesgo es B (Bajo). Para el desarrollo de la propuesta en este punto se sugerirá su aplicación en caso de no considerarse aun en las normas o políticas de seguridad de la información de los Laboratorios, ya que una gran mayoría ya lo considera.

Gráfico 8: Administración de los Activos

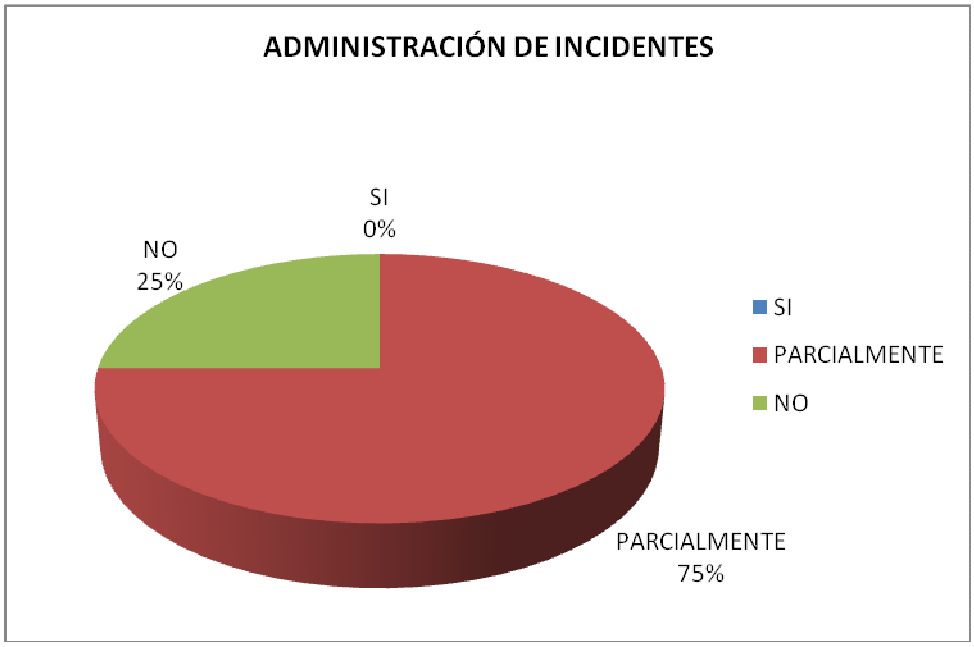


2.2.2.7 *Administración de Incidentes*

Esta área se refiere a asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.

Ninguno de los Laboratorios realiza una Administración de Incidentes, la mayoría lo realiza parcialmente. Mediante este análisis se ha determinado que el grado de confianza que se tiene es B (Bajo) y el nivel de riesgo es A (Alto). Por lo tanto será tomado en cuenta con mayor énfasis para la elaboración de la propuesta.

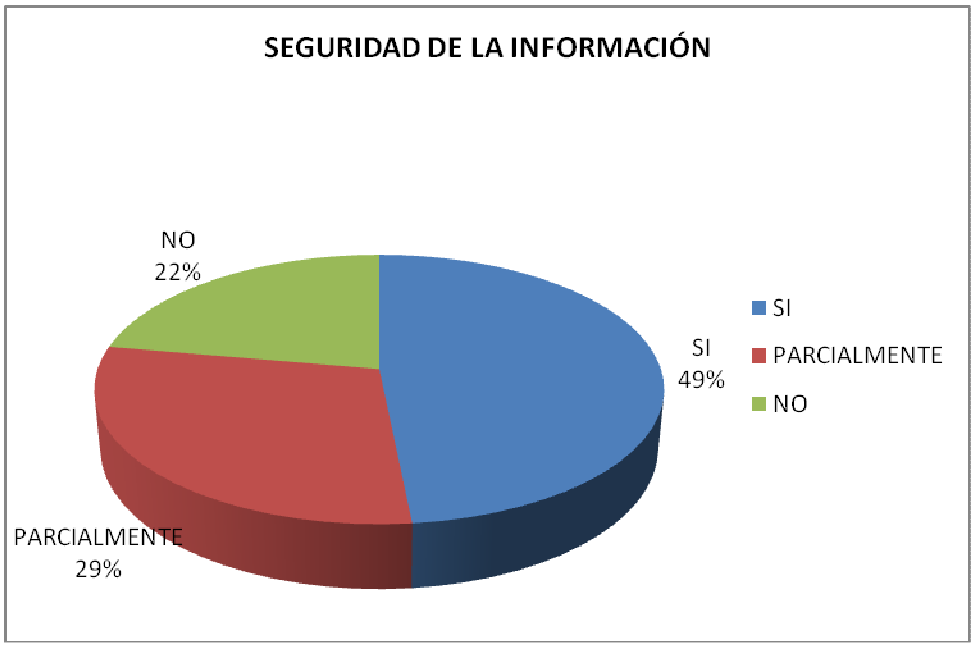
Gráfico 9: Administración de Incidentes



2.2.2.8 *Consolidación de Resultados*

Por los resultados obtenidos se realiza un análisis global de la Seguridad de la Información y se pude decir que existe una cantidad considerable de actividades o políticas de seguridades de la información que si se aplican en Laboratorios, pero también se puede observar que la mayoría de actividades o políticas se lo realiza parcialmente o no se lo hace. Mediante este análisis se puede determinar que el grado de confianza que se tiene es M (Moderado) y el nivel de riesgo es M (Moderado). Por lo tanto esto confirma la necesidad de tener una guía para mejorar la seguridad de la información en los Laboratorios de Computación.

Gráfico 10: Consolidación de Resultados del Análisis de la Seguridad de la Información



CONCLUSIONES

- Al realizar el análisis global de la seguridad e la información en los Laboratorios de Computación, se puede decir que de las preguntas realizadas en la encuesta de acuerdo a los diferentes temas de seguridad no supera el 50% de su cumplimiento, por lo tanto se puede notar que existen vacios que deben ser tomados en cuenta con respecto a la seguridad de la información.

- Es indispensable que los Laboratorios de Computación tomen conciencia de la importancia de la Seguridad de la Información, para poder otorgar un buen servicio y evitar futuros inconvenientes.

- En vista de los resultados obtenidos, una guía que permita llevar una adecuada Seguridad de la Información basada en los problemas o

deficiencias reales de nuestro medio, será de gran utilidad para los diferentes Laboratorios de Computación.

CAPÍTULO 3

DESARROLLO DE LA PROPUESTA

3.1 CONSIDERACIONES PARA EL DESARROLLO DE LA PROPUESTA

La propuesta para el análisis de la Seguridad de la Información en los Laboratorios de Computación de las Facultades de Ingeniería de Sistemas de las universidades de Quito está orientada a servir como una herramienta de ayuda al personal técnico que administra los Laboratorios de Computación que brindan servicios académicos, además permitirá conocer como se están manejando actualmente estos servicios.

La propuesta se basará en:

- La Norma ISO/IEC 27001:2005.
- En el ciclo continuo PDCA analizado en el Capítulo 1.
- En el Análisis de la Situación Actual de los Laboratorios de Computación realizado en el Capítulo 2.

La presente propuesta se ajustará a las necesidades de los Laboratorios de Computación, basándose en los problemas o deficiencias reales de nuestro medio con respecto a la seguridad de la información, además se basará y apoyará en las mejores prácticas de la Norma ISO 27001:2005, lo cual será de gran utilidad para los diferentes Laboratorios de Computación.

La propuesta pretende servir de ayuda para que los Laboratorios de Computación puedan realizar un correcto análisis del manejo de la seguridad de la información y a su vez aportar a la seguridad que deberían tener los Laboratorios, de manera que puedan brindar continuidad, confiabilidad y servicio de calidad.

3.2 ELABORACIÓN DE LA PROPUESTA

De acuerdo a las consideraciones mencionadas anteriormente se establece la siguiente estructura base para el desarrollo de la propuesta:

INTRODUCCIÓN

1. ALCANCE
2. OBJETIVOS DE LA PROPUESTA
3. ASPECTO CLAVE FUNDAMENTAL
4. PLANIFICACIÓN
   4.1 ESTABLECIMIENTO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN
5. IMPLEMENTACIÓN
   5.1 IMPLEMENTACIÓN Y OPERARACIÓN DEL SGSI
6. SEGUIMIENTO
   6.1 MONITOREO Y REVISACIÓN DEL SGSI
7. MEJORA CONTINUA
   7.1 MANTENIMIENTO Y MEJORA EL SGSI

INTRODUCCIÓN

Una organización, tanto como las universidades y sus Laboratorios necesitan identificar y manejar muchas actividades para poder funcionar de una manera efectiva, llegando a ser la adopción de esta propuesta una decisión estratégica. Sabiendo lo importante que son los requerimientos de seguridad de la información y la necesidad de establecer una política y objetivos para la seguridad de la información, así mismo la implementación y operación de controles para manejar los riesgos de la seguridad de la información; monitorear y revisar el desempeño y la efectividad del SGSI; y del mejoramiento continúo. Se adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se aplicará a los procesos SGSI.

3.2.1 ALCANCE

Esta propuesta pretende convertirse en una herramienta para realizar el análisis de la seguridad de la información en los Laboratorios de computación, específicamente para los Laboratorios de computación de las Facultades de Ingeniería en Sistemas, en base a la norma ISO/IEC 27001:2005 la cual se ajustará a las necesidades de la situación actual de los Laboratorios de Computación.

La elaboración de esta propuesta está enfocada para el uso al personal técnico que administra los Laboratorios de Computación de las Facultades de Ingeniería de Sistemas, ya que servirá como una herramienta, para conocer como se están manejando actualmente la Seguridad de la Información y como se la debería manejar en base a la norma ISO/IEC 27001:2005 . Con el fin de mostrar su uso se presenta un caso práctico.

3.2.2 OBJETIVOS DE LA PROPUESTA

- Servir como una herramienta de ayuda al personal técnico que administra los Laboratorios de Computación de las Facultades de Ingeniería de Sistemas que brindan servicios académicos en las universidades de Quito.

- Conocer como se están manejando actualmente los servicios académicos en los Laboratorios de Computación de las Facultades de Ingeniería de Sistemas de las universidades de Quito y relacionarlo con la Norma ISO 27001:2005.

- Aportar a la seguridad que deberían tener los Laboratorios de Computación de las Facultades de Ingeniería de Sistemas de las universidades de Quito, de manera que puedan brindar continuidad, confiabilidad y servicio de calidad.

3.2.3 ASPECTO CLAVE FUNDAMENTAL

Para poder utilizar esta propuesta como una herramienta que permita analizar o mejorar la Seguridad de la Información es importante el compromiso de la gerencia, es decir, del Jefe de Laboratorio y personal administrativo, ya que deben proporcionar evidencia de su compromiso para poder obtener la información correcta y necesaria para el análisis de la seguridad; el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI al:

- Establecer una política SGSI.
- Establecer roles y responsabilidades para la seguridad de información.
- Comunicar al personal de Laboratorio la importancia de lograr los objetivos de seguridad de la información, cumplir la política de seguridad de la información y la necesidad de un mejoramiento continuo.
- Proveer los recursos necesarios para desarrollar, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI.
- Decidir el criterio para la aceptación del riesgo y los niveles de riesgo aceptables.
- Asegurar que se realicen las auditorías internas SGSI.

3.2.4 PLANIFICACIÓN

3.2.4.1 ESTABLECIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Laboratorio de Computación debe establecer, implementar, operar, monitorear, y mejorar continuamente un SGSI documentado los procesos utilizados que se basan en el modelo PDCA (Ver Capítulo 1).

En primera instancia se debe establecer el SGSI en caso de aun no tenerlo, en caso de contar con un SGSI sebe analizar si cumple con lo siguiente:

a) Definición del alcance y los límites del SGSI

Para definir el alcance se debe identificar los procesos del negocio, una vez hecho esto se determinará el alcance del SGSI en base a un método que brinde una identificación clara de las dependencias, relaciones entre las divisiones, áreas, procesos de la organización. Es decir, se debe identificar los procesos principales de la organización, así como las organizaciones internas y externas a los mismos, y la relación de estas con los procesos. Todo esto términos de las características del negocio, la organización, su ubicación, activos, tecnología, la justificación de cualquier exclusión del alcance que no afecten la capacidad y/o responsabilidad de la organización, para proporcionar seguridad de la información que satisfaga los requerimientos de seguridad determinados por la evaluación de riesgo y los requerimientos reguladores aplicables.

Criterios a considerar para el cumplimiento de este proceso:

- Definir el alcance y los límites del Sistema de Gestión de Seguridad de la Información en términos de las características del negocio, la organización, activos, ubicación, tecnología.
- Identificar los procesos del negocio que forman parte del Laboratorio.
- Justificar cualquier exclusión del alcance que no afecten la capacidad y/o responsabilidad del Laboratorio.

b) Definición de una política SGSI

Se debe tener definida una política para el SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología. Donde se tome en cuenta los requerimientos operativos y legales o

reguladores, y las obligaciones de la seguridad establecidas; establezca el criterio con el que se evaluará el riesgo, y haya sido aprobada por la gerencia.

NOTA: La política SGSI es considerada como un super-conjunto de la política de seguridad de la información. Estas políticas se pueden describir en un documento.[11]

Criterios a considerar para el cumplimiento de este proceso:

- Definir una política para el SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología.
- Tomar en cuenta los requerimientos operativos y legales o reguladores, y las obligaciones de la seguridad establecidas.
- Establecer el criterio con el que se evaluará el riesgo.
- Aprobar la política por la gerencia, en este caso por el Jefe del Laboratorio.

c) Definición del enfoque de evaluación del riesgo

Se debe definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable. Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente las cuales son: OCTAVE (Cert), EBIOS; ISO 13335-1:2004, NIST SO 800-30 u otras que son mencionadas por ISO 270001 donde se pueden encontrar enlaces a diferentes herramientas[12], y recursos relacionados con sistemas de gestión de seguridad de la información. El Laboratorio puede optar por una de ellas, hacer una combinación de varias o crear la suya propia.

Criterios a considerar para el cumplimiento de este proceso:

- Identificar una metodología de cálculo del riesgo adecuada.

[11] Tomado de: ESTÁNDAR INTERNACIONAL ISO/IEC 27001

[12] Ver http://www.iso27000.es/herramientas.html

- Desarrollar criterios de aceptación de los riesgos e identificar los niveles de riesgo aceptables.
- Tener una metodología de estimación del riesgo que asegure que los cálculos del riesgo produzcan resultados comparables y reproducibles.

d) Identificación de los riesgos

Se identificará los riesgos y su causa, en los procesos, productos o servicios en cada una de las áreas del Laboratorio.

Criterios a considerar para el cumplimiento de este proceso:

- Identificar los activos y su valor en términos de Confidencialidad, Integridad, Disponibilidad y tener asignado personal responsable a cargo de estos activos.
- Identificar las amenazas para los activos por: desastres naturales, de origen industrial accidental o deliberada, errores y fallos no intencionados, ataques intencionados.
- Identificar las vulnerabilidades que podrían ser explotadas por las amenazas.

e) Análisis y evaluación el riesgo

Se debe evaluar el daño resultante de un fallo de seguridad y la probabilidad de ocurrencia del fallo; además se debe estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable en función de los niveles definidos previamente o si este requiere tratamiento.

Criterios a considerar para el cumplimiento de este proceso:

- Determinar el cálculo del impacto que podría resultar de una falla, teniendo en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos.
- Determinar el cálculo de la probabilidad que ocurra dicha falla.
- Establecer el cálculo de los niveles de riesgo.
- Determinar si el riesgo es aceptable o requiere tratamiento utilizando el criterio de aceptación del riesgo establecido en el literal *c.*

f) Identificación y evaluación de las opciones para el tratamiento de los riesgos

El riesgo puede ser reducido, mitigado mediante controles o eliminado, aceptado o transferido. Se deben seleccionar e implementar los objetivos de control y controles para cumplir con los requerimientos identificados por el proceso de evaluación del riesgo y tratamiento del riesgo. Esta selección debe tomar en cuenta el criterio para aceptar los riesgos (ver literal c), así como los requerimientos legales, reguladores y contractuales. Se deben seleccionar los objetivos de control y los controles del Anexo A como parte de este proceso conforme sea apropiado para cubrir estos requerimientos.

Criterios a considerar para el cumplimiento de este proceso:

- Aplicar los controles apropiados como:

Política de seguridad de la información

1. Tener un documento de la política de la seguridad de la información, aprobado por el Jefe de Laboratorio publicado y comunicado a todos los empleados y entidades externas relevantes.
2. Revisar regularmente la política de seguridad de la información a intervalos planeados o si ocurren cambios significativos.

Organización de la seguridad de la información

Organización interna

1. Tener el apoyo activo de parte de la gerencia o Jefe de Laboratorio referente a la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado y reconocimiento de las responsabilidades de la seguridad de la información.
2. Coordinar las actividades de seguridad de la información por representantes de las diferentes partes del Laboratorio con las funciones y roles laborales relevantes.

3. Definir claramente las responsabilidades de la seguridad de la información.
4. Definir e implementar un proceso de autorización gerencial para la adquisición o ingreso de los nuevos medios de procesamiento de información.
5. Identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no divulgación.
6. Mantener contactos apropiados con las autoridades relevantes.
7. Mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.

Entidades externas

1. Identificar los riesgos que corren la información y los medios de procesamiento de información del Laboratorio e implementar los controles apropiados antes de otorgar acceso.
2. Establecer requerimientos de seguridad relevantes, para un correcto tratamiento de la seguridad con respecto a los acuerdos que involucren el acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información o los medios de procesamiento de información de la organización.

Gestión de activos

Responsabilidad por los activos

1. Identificar claramente los activos; elaborar y mantener un inventario de todos los activos importantes.
2. Establecer una persona o entidad que tenga la responsabilidad gerencial para controlar la producción, desarrollo, mantenimiento, uso y seguridad de toda la información y los activos asociados con los medios de procesamiento de la información.

3. Identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.

Clasificación de la información

1. Clasificar la información en términos de su valor, requerimientos legales, confidencialidad y grado crítico para el Laboratorio.

Seguridad de los recursos humanos

Antes del empleo

1. Definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.
2. Llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, proporcionales a la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
3. Establecer las responsabilidades de los empleados, contratistas, terceros y las de la organización para la seguridad de la información en el contrato de empleo, donde deben aceptar y firmar los términos y condiciones establecidos.

Durante el empleo

1. Requerir por parte de la gerencia o Jefe de Laboratorio que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.
2. Proporcionar el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos a todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, de acuerdo a la función laboral.

3. Definir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.

Terminación o cambio del empleo

1. Definir y asignar claramente las responsabilidades para realizar la terminación o cambio del empleo.
2. Establecer que todos los empleados, contratistas y terceros deben devolver todos los activos del Laboratorio u organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.
3. Eliminar o ajustar al cambio los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información a la terminación de su empleo, contrato o acuerdo.

Seguridad física y ambiental

Áreas seguras

1. Utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.
2. Proteger las diferentes áreas del Laboratorio mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.
3. Diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastres naturales o creados por el hombre.

Seguridad del equipo

1. Ubicar o proteger los equipos de manera que se pueda reducir los riesgos de las amenazas y peligros ambientales, y de las oportunidades para el acceso no autorizado.

2. Proteger los equipos de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.
3. Proteger el cableado de la energía y las telecomunicaciones que llevan datos o sostienen los servicios de información de la intercepción o el daño.
4. Dar un mantenimiento correcto a los equipos para permitir su continua disponibilidad e integridad.
5. Chequear para asegurar que se haya removido o sobrescrito de manera segura cualquier dato confidencial y software con licencia antes de la eliminación de cualquier medio de almacenaje de los equipos.
6. Controlar que los equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización.

Gestión de las comunicaciones y operaciones

Procedimientos y responsabilidades operacionales

1. Documentar y mantener los procedimientos de operación, y poner a disposición de todos los usuarios que los necesiten.
2. Controlar los cambios en los medios y sistemas de procesamiento de la información.
3. Separar los medios de desarrollo, prueba y operación para reducir los riesgos de accesos no autorizados.

Gestión de la entrega del servicio de terceros

1. Asegurar que terceros cumplan con los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el contrato.
2. Monitorear, revisar y realizar las auditorías regularmente de los servicios, reportes y registros provistos por terceros.

Protección contra software malicioso

1. Implementar controles de detección (antivirus actualizados), prevención y recuperación para protegerse de códigos malicioso.

Respaldo (back-up)

1. Realizar copias de back-up o respaldo de la información que se considere más importante o irremplazable y software esencial y se debe ser probada regularmente.

Gestión de seguridad de redes

1. Manejar y controlar las redes adecuadamente para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.

Gestión de medios

1. Establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.
2. Proteger la documentación de un acceso no autorizado.

Intercambio de información

1. Establecer acuerdos para el intercambio de información y software entre la organización y entidades externas o terceros.
2. Proteger los medios que contienen información contra un acceso no autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos del Laboratorio.
3. Proteger adecuadamente los mensajes electrónicos.

Servicios de comercio electrónico

1. Proteger la información involucrada en el comercio electrónico que se trasmite a través de redes públicas de cualquier actividad fraudulenta, disputa contractual y divulgación y modificación no autorizada.

2. Proteger la integridad de la información disponible públicamente para evitar la modificación no autorizada.

Monitoreo

1. Producir registros de las actividades de auditoría, eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.
2. Proteger los medios de registro y la información del registro contra alteraciones y acceso no autorizado.
3. Registrar las actividades del administrador y operador del sistema, además debe existir una correcta sincronización de relojes de los sistemas de procesamiento de información relevantes.

Control de acceso

Gestión del acceso del usuario

1. Debe existir un procedimiento formal para la inscripción y el retiro de la inscripción de la otorgación del acceso a todos los sistemas y servicios de información.
2. Restringir y controlar la asignación y uso de los privilegios.
3. Controlar la asignación de claves a través de un proceso de gestión formal.

Responsabilidades del usuario

1. Requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.

Control de acceso a redes

1. Establecer que los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
2. Utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
3. Controlar el acceso físico y lógico.

Control de acceso al sistema de operación

1. Establecer que todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la identidad del usuario.
2. Establecer que las sesiones inactivas deben cerrarse después de un período de inactividad definido.

Control de acceso a la información

1. Restringir el acceso de los usuarios y personal de soporte a la información relevante y confidencial en concordancia con la política de control de acceso definida.
2. Tener un ambiente de cómputo dedicado (asignado solo para dicha función) para la información más importante y sensible.

Adquisición, desarrollo y mantenimiento de los sistemas de información

Procesamiento correcto en las aplicaciones

1. Validar la fuente de datos para asegurar que los datos sean correctos y apropiados.

Controles criptográficos

1. Desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

Seguridad de los archivos del sistema

1. Contar con procedimientos para controlar la instalación de software en los sistemas operacionales.

Seguridad en los procesos de desarrollo y soporte

1. Revisar y probar las aplicaciones para asegurar que no exista un impacto adverso en las operaciones del Laboratorio o de sus usuarios cuando se cambian los sistemas operativos.

Gestión de incidentes en la seguridad de la información

Reporte de eventos y debilidades en la seguridad de la información

1. Reportar los eventos de seguridad de la información a la gerencia o Jefe de Laboratorio lo más rápidamente posible.
2. Requerir que todos los empleados, contratistas y terceros, usuarios del Laboratorio y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.

Gestión de incidentes y mejoras en la seguridad de la información

1. Establecer las responsabilidades y procedimientos para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.

Gestión de la continuidad de los Servicios

Aspectos de la seguridad de la información de la gestión de la continuidad

1. Identificar los eventos que causan interrupciones en los procesos de los servicios que ofrece el Laboratorio, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
2. Desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información después de la interrupción o falla en los procesos más críticos.
3. Mantener un solo marco referencial de planes de continuidad de servicios para asegurar que todos los planes sean consistentes.

4. Probar y actualizar los planes de continuidad de servicios regularmente para asegurar que estén actualizados y sean efectivos.

Cumplimiento

Cumplimiento con requerimientos legales

1. Implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.

Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico

1. Establecer que el gerente o Jefe de Laboratorio, ayudante de Laboratorio asegure que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.

Consideraciones de auditoría de los sistemas de información

1. Planear cuidadosamente los requerimientos y actividades de las auditorías que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos de servicio.
2. Proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.

- Aceptar los riesgos consciente y objetivamente, siempre que satisfagan claramente las políticas y el criterio de aceptación del riesgo (Ver literal c).
- Evitar los riesgos, mediante cualquier acción donde las actividades del Laboratorio se modifiquen, para así poder evitar la ocurrencia del riesgo.

- Transferir los riesgos operativos asociados a otras entidades; por ejemplo: aseguradoras, proveedores.
- Seleccionar objetivos de control y controles para el tratamiento de riesgos.

g) Preparación de la Declaración de Aplicabilidad

Se debe preparar una Declaración de Aplicabilidad, el cual proporciona un resumen de las decisiones concernientes con el tratamiento del riesgo, además se debe justificar las exclusiones para asegurar que ningún control haya sido omitido inadvertidamente.

Criterios a considerar para el cumplimiento de este proceso:

- Establecer razones para la selección de los controles, la exclusión de cualquier control y la justificación para su exclusión.

3.2.5 IMPLEMENTACIÓN

3.2.5.1 IMPLEMENTACIÓN Y OPERARACIÓN DEL SGSI

Para poder implementar y operar el SGSI, la organización debe hacer lo siguiente:

a) Definición del plan de tratamiento de riesgo

Se debe definir un plan de tratamiento de riesgos el cual identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

Criterios a considerar para el cumplimiento de este proceso:

- Identificar la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información.

b) Implementación del plan de tratamiento de riesgo

Se debe implementar el plan de tratamiento de riesgos para poder alcanzar los objetivos de control identificados.

Criterios a considerar para el cumplimiento de este proceso:

- Implementar el plan de tratamiento de riesgos.

c) Implementación de los controles

Se debe implementar los controles seleccionados en *literal h* para satisfacer los objetivos de control.

Criterios a considerar para el cumplimiento de este proceso:

- Implementar los controles.

***d)* Definición de cómo medir la efectividad de los controles.**

La medición de la efectividad de los controles permite a los Jefes de Laboratorio o gerentes y personal determinar lo bien que los controles logran los objetivos de control planeados.

Criterios a considerar para el cumplimiento de este proceso:

- Especificar cómo se van a medir la efectividad de los controles y como se va a utilizar estas mediciones para producir resultados comparables y reproducibles.

e) Implementación de los programas de capacitación y conocimiento.

Formación y concienciación de todo el personal del Laboratorio en lo relativo a la seguridad de la información.

Criterios a considerar para el cumplimiento de este proceso:

- Implementar los programas de capacitación y conocimiento en lo relativo a la seguridad de la información.

3.2.6 SEGUIMIENTO

3.2.6.1 MONITOREO Y REVISIÓN DEL SGSI

Para poder monitorear y revisar el SGSI, el Laboratorio debe hacer lo siguiente:

a) Ejecución de procedimientos de monitoreo y revisión, y otros controles

Se debe ejecutar procedimientos y controles de monitorización y revisión para poder detectar errores en los resultados de procesamiento, además para identificar brechas e incidentes de seguridad.

Criterios a considerar para el cumplimiento de este proceso:

- Detectar prontamente los errores en los resultados de procesamiento.
- Identificar prontamente los incidentes y violaciones de seguridad fallidas y exitosas.
- Tener ayuda del personal, tecnología, software o indicadores que permita ayudar a detectar los eventos de seguridad, evitando así los incidentes de seguridad.
- Determinar si son efectivas las acciones tomadas para resolver una violación de seguridad.

b) Revisiones regulares de la efectividad del SGSI

Se debe revisar regularmente la eficacia del SGSI en función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y retroalimentación de todos los interesados, incluyendo satisfacer la política y objetivos de seguridad del SGSI.

Criterios a considerar para el cumplimiento de este proceso:

- Realizar revisiones regulares de la efectividad del SGSI mediante auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y retroalimentación.

c) Medición de la efectividad de los controles

Se debe medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.

Criterios a considerar para el cumplimiento de este proceso:

- Medir la efectividad de los controles.

d) Revisión de las evaluaciones del riesgo

Se debe revisar regularmente la evaluación de riesgos ya que los cambios en: la organización, la tecnología, los procesos y los objetivos del negocio; así como las amenazas, la eficacia de los controles o el entorno; tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.

Criterios a considerar para el cumplimiento de este proceso:

- Revisar la evaluación de riesgos tomando en cuenta los cambios en: la organización, tecnología, objetivos y procesos, amenazas identificadas, efectividad de los controles implementados; y eventos externos, como cambios en el ambiente legal o regulador, y cambios en el clima social.

e) Auditorías internas del SGSI a intervalos planeados

Se deben realizar auditorías internas, algunas veces llamadas auditorías de primera persona, son realizadas por la organización misma para propósitos internos, en los objetivos de control, controles, procesos y procedimientos del SGSI.

Criterios a considerar para el cumplimiento de este proceso:

- Realizar auditorías internas para conocer si los controles, procesos y procedimientos del SGSI cumplen con los requerimientos de seguridad de la información identificados.
- Realizar auditorías internas para conocer si los controles, procesos y procedimientos del SGSI se implementan y mantienen de manera efectiva.
- Realizar auditorías internas para conocer si los controles, procesos y procedimientos del SGSI se realizan conforme lo esperado.

f) Actualización de los planes de seguridad

Se deben actualizar los planes de seguridad teniendo en cuenta los resultados de la monitorización y las revisiones.

Criterios a considerar para el cumplimiento de este proceso:

- Actualizar los planes de seguridad teniendo en cuenta los resultados de la monitorización y las revisiones.

3.2.7 MEJORA CONTINUA

3.2.7.1 MANTENIMIENTO Y MEJORA DEL SGSI

Para mantener y mejorar el SGSI el Laboratorio debe realizar regularmente lo siguiente:

a) Implementación de las mejoras identificadas en el SGSI y asegurar que las mejoras logren sus objetivos señalados.

Se deben implementar las mejoras identificadas en el SGSI, por ejemplo, las que se determinaron en la fase de seguimiento, asegurar que las mejoras alcancen los objetivos pretendidos; siempre debe comprobarse la eficacia de cualquier acción, medida o cambio.

Criterios a considerar para el cumplimiento de este proceso:

- Implementar las mejoras identificadas en el SGSI.
- Asegurar que las mejoras alcancen los objetivos pretendidos.

b) Tomar las acciones correctivas y preventivas apropiadas

El Laboratorio debe realizar las *acciones correctivas* para eliminar la causa de las inconformidades con los requerimientos del SGSI para poder evitar la irregularidad, se debe determinar la acción para eliminar la causa de las

inconformidades potenciales de los requerimientos SGSI para evitar su ocurrencia. Las acciones *preventivas tomadas* deben ser apropiadas para el impacto de los problemas potenciales. El procedimiento documentado para la acción preventiva debe definir los requerimientos para:

Criterios a considerar para el cumplimiento de este proceso:

Correctivas

- Identificar las inconformidades con los requerimientos del SGSI.
- Determinar las causas de las inconformidades.
- Evaluar la necesidad de ejecutar acciones que permitan eliminar la causa de las inconformidades para asegurar que éstas no vuelvan a ocurrir.
- Determinar e implementar la acción correctiva necesaria.
- Registrar los resultados de la acción correctiva tomada.
- Revisar la acción correctiva tomada.

Preventivas

- Identificar las inconformidades potenciales con los requerimientos del SGSI y sus causas.
- Evaluar la necesidad de acciones que permitan eliminar la causa de las inconformidades para asegurar que éstas no vuelvan a ocurrir.
- Determinar e implementar la acción preventiva necesaria.
- Registrar los resultados de la acción preventiva tomada.
- Revisar la acción preventiva tomada.

c) Comunicación de los resultados y acciones

Se debe comunicar los resultados y acciones a todas las partes interesadas con un nivel de detalle apropiado de acuerdo a las circunstancias y, cuando sea relevante, acordar cómo proceder.

Criterios a considerar para el cumplimiento de este proceso:

- Comunicar los resultados y acciones a todas las partes interesadas.

3.3 APLICABILIDAD DE LA PROPUESTA

Esta propuesta ha sido desarrollada en base a la Norma Internacional ISO 27001: 2005, los requerimientos y procesos establecidos en esta propuesta están diseñados para ser aplicables a todos los Laboratorios de Computación de las Facultades de Ingeniería en Sistemas de las diferentes universidades, sin importar su tamaño. Se podría generalizar esta propuesta para los diferentes Laboratorios de Computación de las diferentes universidades.

Con el fin de convertirse en una herramienta de ayuda para realizar el análisis de la seguridad de la información en los Laboratorios de computación, en la siguiente sección se sugerirá una manera de fijar criterios que ayuden a cuantificar los resultados obtenidos en la aplicación de la misma.

Se espera que la utilización de la propuesta además de permitirnos realizar el análisis de la seguridad de la información, sea una herramienta de ayuda para el personal técnico de los Laboratorios para poder manejar correctamente la seguridad de la información. Como es de esperarse si un Laboratorio ya cuenta con un sistema de gestión de la seguridad de la información o de procesos, en la mayoría de los casos es preferible satisfacer los requerimientos y procesos de esta propuesta dentro del sistema de gestión existente.

3.4 USO DE LA PROPUESTA

Con el fin de establecer un correcto uso de la propuesta se empleará la teoría de valores ponderados para poder fijar un criterio que ayude a hacer cuantificable los resultados obtenidos.

Cada criterio de la propuesta está asociado a un puntaje de la siguiente manera:

Tabla 6: Asignación de puntajes

VERIFICACIÓN	**PUNTAJE ASOCIADO (PUNTOS)**
NO	0
PARCIALMENTE	0.5
SI	1

Fuente: Guía Práctica para Auditar la Gestión de Redes de área Local, Autores: Pablo Santiago Reyes Villalva, Franklin Estaban Valdivieso Burbano – 2004

Cada uno de los criterios serán agrupados a sus respectivas fases (cada fase cubierta en la propuesta) con el fin de enfocar la importancia de cada uno y poder cuantificar la totalidad de los puntajes obtenidos, de esta manera poder realizar el análisis de los resultados de aplicar la propuesta.

En las siguientes tablas se mostrará la manera de cómo se van a cuantificar[13] los resultados:

PLANIFICACIÓN

ESTABLECIMIENTO DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN

Tabla 7: Asignación de Puntajes para el Establecimiento del Sistema de Gestión De Seguridad de la Información

[13] Tomado de: Guía Práctica para Auditar la Gestión de Redes de área Local, Autores: Pablo Santiago Reyes Villalva, Franklin Estaban Valdivieso Burbano – 2004

PUNTAJE TOTAL OBTENIDO (puntos)	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
De 0 a 10.5	0%- 50%	Bajo
De 11 a 15.5	52.4%-73.9%	Moderado
De 16 a 21	76.19%-100%	Alto

APLICACIÓN DE CONTROLES

Política y Organización de seguridad de información

Tabla 8: Asignación de Puntajes para la Política y Organización de la seguridad de la información

PUNTAJE TOTAL OBTENIDO (puntos)	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
De 2 a 7	0%- 50%	Bajo
De 7.5 a 10.5	53.6%-75%	Moderado
De 11 a 14	78.6%-100%	Alto

Seguridad de los recursos humanos

Tabla 9: Asignación de Puntajes para la Seguridad de los recursos humanos

PUNTAJE TOTAL OBTENIDO (puntos)	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
De 0 a 4.5	0%- 50%	Bajo
De 5 a 6.5	55.56%-72.22%	Moderado
De 7 a 9	77.78%-100%	Alto

Seguridad física y ambiental

Tabla 10: Asignación de Puntajes para la Seguridad física y ambiental

PUNTAJE TOTAL OBTENIDO (puntos)	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
De 0 a 4.5	0%- 50%	Bajo
De 5 a 6.5	55.56%-72.22%	Moderado
De 7 a 9	77.78%-100%	Alto

Gestión de comunicaciones y operaciones

Tabla 11: Asignación de Puntajes para la Gestión de comunicaciones y operaciones

PUNTAJE TOTAL OBTENIDO (puntos)	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
De 0 a 8	0%- 50%	Bajo
De 8.5 a 12	53.13%-75%	Moderado
De 12.5 a 16	78.1%-100%	Alto

Control de acceso

Tabla 12: Asignación de Puntajes para el Control de acceso

PUNTAJE TOTAL OBTENIDO (puntos)	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
De 0 a 5.5	0% - 50%	Bajo

De 6 a 8	54.5%-72.7%	Moderado
De 8.5 a 11	77.2%-100%	Alto

Adquisición, desarrollo y mantenimiento de los sistemas de información

Tabla 13: Asignación de Puntajes para la Adquisición, desarrollo y mantenimiento de los sistemas de información

PUNTAJE TOTAL OBTENIDO (puntos)	**PORCENTAJE ASOCIADO %**	**INTERPRETACIÓN**
De 0 a 1.5	0%- 50%	Bajo
De 2	66.67%	Moderado
De 2.5 a 3	83.3%-100%	Alto

Gestión de incidentes en la seguridad de la información

Tabla 14: Asignación de Puntajes de Gestión de incidentes en la seguridad de la información

PUNTAJE TOTAL OBTENIDO (puntos)	**PORCENTAJE ASOCIADO %**	**INTERPRETACIÓN**
De 0 a 1.5	0%- 50%	Bajo
De 2	66.67%	Moderado
De 2.5 a 3	83.3%-100%	Alto

Gestión de la continuidad de los servicios

Tabla 15: Asignación de Puntajes de Gestión de la continuidad de los servicios

PUNTAJE TOTAL OBTENIDO (puntos)	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
De 0 a 2	0%- 50%	Bajo
De 2.5 a 3	62.5%-75%	Moderado
De 3.5 a 4	87.5%-100%	Alto

Cumplimiento

Tabla 16: Asignación de Puntajes para el Cumplimiento

PUNTAJE TOTAL OBTENIDO (puntos)	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
De 0 a 2	0%- 50%	Bajo
De 2.5 a 3	62.5%-75%	Moderado
De 3.5 a 4	87.5%-100%	Alto

IMPLEMENTACIÓN

IMPLEMENTACIÓN Y OPERACIÓN DEL SGSI

Tabla 17: Asignación de Puntajes para la Implementación Y Operación del SGSI

PUNTAJE TOTAL OBTENIDO (puntos)	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
De 0 a 2.5	0%- 50%	Bajo
De 3 a 3.5	60%-70%	Moderado
De 4 a 5	80%-100%	Alto

SEGUIMIENTO

SEGUIMIENTO Y REVISIÓN DEL SGSI

Tabla 18: Asignación de Puntajes para el Seguimiento y Revisión del SGSI

PUNTAJE TOTAL OBTENIDO (puntos)	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
De 0 a 5.5	0% - 50%	Bajo
De 6 a 8	54.5%-72.7%	Moderado
De 8.5 a 11	77.2%-100%	Alto

MEJORA CONTINUA

MANTENIMIENTO Y MEJORA DEL SGSI

Tabla 19: Asignación de Puntajes para el Mantenimiento y Mejora del SGSI

PUNTAJE TOTAL OBTENIDO (puntos)	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
De 0 a 7	0%- 50%	Bajo
De 7.5 a 10.5	53.5%-75%	Moderado
De 11 a 14	78.5%-100%	Alto

Mediante los porcentajes anteriores y sus interpretaciones asignadas a cada uno se plantea lo siguiente:

- Si la interpretación es **Bajo**, implica que se debe tomar medidas que permitan mejorar la seguridad de la información ya que se encuentran grandes brechas de seguridad que pueden atraer graves problemas al Laboratorio, se deberá poner énfasis al criterio o los criterios que se encuentren en ese estado para así poder mejorar la seguridad.

- Si la interpretación es **Moderado,** implica que se debe mantener el estado de los criterios que se están cumpliendo correctamente, siempre es posible mejorar los criterios que tienen un alto puntaje. Se debe poner énfasis en los que nos se cumplen para poder aplicar las medidas necesarias para poder mejorar la seguridad de la información.

- Si la interpretación es **Alto,** implica que la seguridad de la información se está llevando de una manera correcta y que es preciso mantenerla de esa manera, sin embargo se deberá comprobar el cumplimiento de todos los criterios para así poder tener una correcta seguridad de la información.

CAPÍTULO 4

APLICACIÓN DE LA PROPUESTA EN UN CASO PRÁCTICO

4.1 SELECCIÓN DE LA ORGANIZACIÓN DONDE SE APLICARÁ LA PROPUESTA

El Laboratorio[14] que se seleccionó es COMISIÓN DE VINCULACIÓN Y MEDIO EXTERNO DEL DICC Y UNISIG de la Escuela Politécnica Nacional, por los siguientes motivos:

- El Laboratorio es un proveedor de servicios y productos de Tecnologías de la Información, por tal motivo es necesario mantener un adecuado manejo de la Seguridad de Información para poder brindar continuidad y calidad en estos servicios.
- Es un Laboratorio de nuestra facultad donde las personas que lo administran con seguridad nos puede brindar la ayuda que necesitamos para aplicar la propuesta.
- El Laboratorio cuenta varios equipos, servidores y tiene información relevante que necesita mantener segura.
- Se quiere aplicar la propuesta en este Laboratorio para que el análisis que realizamos pueda servir al personal administrativo como una herramienta para conocer el estado actual del manejo de la Seguridad de la Información.

A continuación se indica aspectos[15] relevantes del Laboratorio:

[14] Se entenderá como Laboratorio a la COMISIÓN DE VINCULACIÓN Y MEDIO EXTERNO DEL DICC Y UNISIG de la Escuela Politécnica Nacional
[15] Información otorgada por Ing. Pamela Flores

Visión:

La Facultad de Sistemas, el DICC y sus carreras tienen la posibilidad de convertirse en proveedores de servicios y productos de Tecnologías de la Información, de manera que puedan soportar iniciativas del Gobierno Central y de los Gobiernos locales así como también de clientes del sector privado. ***Los estudiantes y los profesores son capaces de diseñar, desarrollar, construir, probar e implementar sistemas de información e infraestructuras de TI.***

Para facilitar el logro de nuestra visión se potencia la vinculación de la Facultad y el DICC con el medio externo y las alianzas estratégicas con distintos actores del área de Tecnologías de la Información, tanto locales como internacionales,

Objetivos:

- Mantener un modelo de formación académica con una ventaja competitiva respecto a otras universidades pues estará íntimamente relacionada con aplicaciones reales y permitirá obtener profesionales mejor preparados con un mayor nivel de experiencia práctica y que por lo tanto, estarán mejor cotizados en el mercado de trabajo nacional e internacional.
- Potenciar alianzas estratégicas con empresas de Tecnologías de la Información.

Productos y Servicios:

Proyectos de Tecnologías de la Información

- Formulación y administración de proyectos utilizando estándares PMBOK y herramientas informáticas.
- Asesoría para definición de líneas base de proyectos, definición de requerimientos de sistemas, ayuda para monitoreo y medición de beneficios.
- Personalización y comercialización de productos de software desarrollados como tesis de grado.
- Planificación informática.

- Peritajes informáticos.
- Análisis, desarrollo e implementación de sistemas.
- Análisis, diseño e implementación de redes de información.
- Asesoría informática en diferentes áreas de interés del departamento como:
    - repositorios de datos,
    - datamarts,
    - datawarehouse,
    - datamining,
    - informática lingüística,
    - médica,
    - legal,
    - automatización de procesos,
    - evaluaciones forenses,
    - aplicaciones Web,
    - sistemas de información de apoyo a planificación territorial,
    - sistemas de manejo de desastres,
    - educación virtual,
    - bibliotecas digitales,
    - entre otros.
- Desarrollo de sistemas usando Sistemas de Información Geográfica.

Plataformas virtuales

- Implementación de plataformas virtuales en distintas instituciones del Estado y en empresas privadas.
- Diseño e implementación de CD´s interactivos simuladores de plataforma virtual.
- Preparación de facilitadores que contarán con facilidades en el uso de la plataforma virtual y los contenidos de los módulos de formación.
- Cursos virtuales abiertos dirigidos a la comunidad en diferentes áreas de Tecnologías de la Información y Sistemas de Información Geográfica. Uso de plataforma Moodle y video en demanda.

Capacitación

- Como un aporte a la comunidad, la Comisión de Vinculación del DICC ofrece cursos de distintos tópicos de Tecnologías de la Información y Sistemas de Información Geográfica en las siguientes modalidades:

Cursos abiertos

- La Comisión de Vinculación del DICC organiza periódicamente cursos abiertos, estos cursos están dirigidos a estudiantes universitarios, profesionales y público en general, para ver mayor información de los cursos disponibles haga clic aquí Ver cursos disponibles...

Cursos personalizados a la medida

- También existe la posibilidad de definir cursos específicos a la medida de acuerdo a las aplicaciones de cada carrera, empresas, organizaciones, instituciones o público en general. Se pueden escoger módulos individuales de los cursos ofrecidos o se puede definir el contenido y las características de los cursos de acuerdo a las necesidades de las áreas que los solicitan.

Inscripciones

- Las inscripciones están abiertas para todo público, empresas y organismos interesados.
- Para reservar cupos solo tienen que enviar un e-mail a la dirección (poner direcciones de mail de contacto) o favor comunicarse con los teléfonos de la Comisión de Vinculación.

4.1.1 APLICACIÓN DE LA PROPUESTA

PLANIFICACIÓN

Tabla 20: Establecimiento del Sistema de Gestión de Seguridad de la Información

FACTORES A CONSIDERAR PARA EL ESTABLECIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)	SI	PARCIALMENTE	NO
Se tiene definido el alcance y los límites del SGSI en términos de las características del negocio, la organización, activos, ubicación, tecnología.	X		
Se tiene identificados los procesos del negocio que forman parte del Laboratorio.	X		
Se tiene justificada cualquier exclusión del alcance que no afecten la capacidad y/o responsabilidad del Laboratorio.	X		
Se tiene definida una política para el SGSI en términos de las características del negocio, la organización, su ubicación, activos y tecnología.		X	
Se toman en cuenta los requerimientos operativos y legales o reguladores, y las obligaciones de la seguridad establecidas.		X	
Se tiene aprobada la política por la gerencia, en este caso por el Jefe del Laboratorio.	X		
Se tiene identificada una metodología de cálculo del riesgo adecuada.			X
Se ha desarrollado criterios de aceptación de los riesgos e identificado los niveles de riesgo aceptables.		X	
Se tiene una metodología de estimación del riesgo que asegure que los cálculos del riesgo produzcan resultados comparables y reproducibles.			X

Se identifican los activos y su valor en términos de Confidencialidad, Integridad, Disponibilidad y se tiene asignado personal responsable a cargo de estos activos.	X		
Se identifican las amenazas para los activos por: desastres naturales, de origen industrial accidental o deliberada, errores y fallos no intencionados, ataques intencionados.		X	
Se identifican las vulnerabilidades que podrían ser explotadas por las amenazas.		X	
Se tiene determinado el cálculo del impacto que podría resultar de una falla, teniendo en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos.			X
Se tiene determinado el cálculo de la probabilidad que ocurra dicha falla.			X
Se tiene establecido el cálculo de los niveles de riesgo.			X
Se puede determinar si el riesgo es aceptable o requiere tratamiento utilizando el criterio de aceptación del riesgo establecido anteriormente.			X
Se aceptan los riesgos consciente y objetivamente, siempre que satisfagan claramente las políticas y el criterio de aceptación del riesgo	X		
Se evita los riesgos.		X	
Se transfiere los riesgos operativos asociados a otras entidades; por ejemplo: aseguradoras, proveedores.			X
Se seleccionan objetivos de control y controles para el tratamiento de riesgos.		X	
Se establecen razones para la selección de los controles, la exclusión de cualquier control y la justificación para su exclusión.		X	

Tabla 21: Factores a considerar para la aplicación de los controles

Política de seguridad de información	SI	PARCIALMENTE	NO
Se tiene un documento de la política de la seguridad de la información, aprobado por el Jefe de Laboratorio publicado y comunicado a todos los empleados y entidades externas relevantes.			X
Se revisa regularmente la política de seguridad de la información a intervalos planeados o si ocurren cambios significativos.			X

Organización de la seguridad de la información	SI	PARCIALMENTE	NO
Se tiene el apoyo activo de parte de la gerencia o Jefe de Laboratorio referente a la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado y reconocimiento de las responsabilidades de la seguridad de la información.	X		
Se coordinan las actividades de seguridad de la información por representantes de las diferentes partes del Laboratorio con las funciones y roles laborales relevantes.	X		
Se tiene claramente definidas las responsabilidades de la seguridad de la información.	X		
Se define e implementa un proceso de autorización gerencial para la adquisición o ingreso de los nuevos medios de procesamiento de información.	X		
Se identifican y revisan regularmente los requerimientos de confidencialidad o los acuerdos de no divulgación.			X
Se mantienen contactos apropiados con las autoridades relevantes.	X		
Se mantienen contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.			X

Se identifican los riesgos que corren la información y los medios de procesamiento de información del Laboratorio y se implementan los controles apropiados antes de otorgar acceso.		X	
Se tienen identificado claramente los activos; se elabora y mantiene un inventario de todos los activos importantes.	X		
Se establece una persona o entidad que tenga la responsabilidad gerencial para controlar la producción, desarrollo, mantenimiento, uso y seguridad de toda la información y los activos asociados con los medios de procesamiento de la información.	X		
Se identifican, documentan e implementan las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.	X		
Se clasifica la información en términos de su valor, requerimientos legales, confidencialidad y grado crítico para el Laboratorio.			X

Seguridad de los recursos humanos	SI	PARCIALMENTE	NO
Se define y documenta los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.		X	
Se lleva a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, proporcionales a la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.	X		

Se establecen las responsabilidades de los empleados, contratistas, terceros y las de la organización para la seguridad de la información en el contrato de empleo, donde deben aceptar y firmar los términos y condiciones establecidos.		X	
Se requiere por parte de la gerencia o Jefe de Laboratorio que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.	X		
Se proporcionar el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos a todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, de acuerdo a la función laboral.		X	
Se define un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.			X
Se tiene definido y asignado claramente las responsabilidades para realizar la terminación o cambio del empleo.	X		
Se establece que todos los empleados, contratistas y terceros deben devolver todos los activos del Laboratorio u organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.	X		
Se eliminan o ajustan al cambio los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información a la terminación de su empleo, contrato o acuerdo.		X	

Seguridad física y ambiental	SI	PARCIALMENTE	NO
Se utilizan perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.	X		
Se protegen las diferentes áreas del Laboratorio mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.	X		
Se diseña y aplica protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastres naturales o creados por el hombre.	X		
Se ubica o protege los equipos de manera que se pueda reducir los riesgos de las amenazas y peligros ambientales, y de las oportunidades para el acceso no autorizado.		X	
Se protegen los equipos de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.		X	
Se protege el cableado de la energía y las telecomunicaciones que llevan datos o sostienen los servicios de información de la intercepción o el daño.		X	
Se da un mantenimiento correcto a los equipos para permitir su continua disponibilidad e integridad.	X		
Se chequea para asegurar que se haya removido o sobrescrito de manera segura cualquier dato confidencial y software con licencia antes de la eliminación de cualquier medio de almacenaje de los equipos.			X
Se controla que los equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización.	X		

Gestión de las comunicaciones y operaciones	SI	PARCIALMENTE	NO
Se documenta y mantiene los procedimientos de operación, y se ponen a disposición de todos los usuarios que los necesiten.		X	
Se controlan los cambios en los medios y sistemas de procesamiento de la información.		X	
Se separan los medios de desarrollo, prueba y operación para reducir los riesgos de accesos no autorizados.	X		
Se asegurar que terceros cumplan con los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el contrato.		X	
Se monitorea, revisa y realiza las auditorías regularmente de los servicios, reportes y registros provistos por terceros.			X
Se implementan controles de detección (antivirus actualizados), prevención y recuperación para protegerse de códigos malicioso.	X		
Se realizan copias de back-up o respaldo de la información que se considere más importante o irremplazable y software esencial y se debe ser probada regularmente.		X	
Se manejan y controlan las redes adecuadamente para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito.		X	
Se establecen procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.		X	
Se protege la documentación de un acceso no autorizado.		X	

Se protegen los medios que contienen información contra un acceso no autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos del Laboratorio.		X	
Se protegen adecuadamente los mensajes electrónicos.		X	
Se protege la integridad de la información disponible públicamente para evitar la modificación no autorizada.	X		
Se produce registros de las actividades de auditoría, eventos de seguridad de la información y se mantienen durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.			X
Se protegen los medios de registro y la información del registro contra alteraciones y acceso no autorizado.			X
Se registran las actividades del administrador y operador del sistema, además existe una correcta sincronización de relojes de los sistemas de procesamiento de información relevantes.			X

Control de acceso	SI	PARCIALMENTE	NO
Se tiene un procedimiento formal para la inscripción y el retiro de la inscripción de la otorgación del acceso a todos los sistemas y servicios de información.		X	
Se restringe y controla la asignación y uso de los privilegios.		X	
Se controla la asignación de claves a través de un proceso de gestión formal.	X		
Se requiere que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.	X		
Se establece que los usuarios sólo deben tener acceso a los servicios para los cuales han sido			X

específicamente autorizados a usar.			
Se utilizan métodos de autenticación para controlar el acceso de usuarios remotos.			X
Se controla el acceso físico y lógico a las redes.	X		
Se establece que todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se elige una técnica de autenticación adecuada para verificar la identidad del usuario.		X	
Se establece que las sesiones inactivas deben cerrarse después de un período de inactividad definido.	X		
Se restringe el acceso de los usuarios y personal de soporte a la información relevante y confidencial en concordancia con la política de control de acceso definida.			X
Se tiene un ambiente de cómputo dedicado (asignado solo para dicha función) para la información más importante y sensible.	X		

Adquisición, desarrollo y mantenimiento de los sistemas de información	SI	PARCIALMENTE	NO
Se valida la fuente de datos para asegurar que los datos sean correctos y apropiados.	X		
Se desarrolla e implementa una política sobre el uso de controles criptográficos para la protección de la información.			X
Se cuenta con procedimientos para controlar la instalación de software en los sistemas operacionales.			X
Se revisa y prueba las aplicaciones para asegurar que no exista un impacto adverso en las operaciones del Laboratorio o de sus usuarios cuando se cambian los sistemas operativos.		X	

Gestión de incidentes en la seguridad de la información	SI	PARCIALMENTE	NO
Se reportan los eventos de seguridad de la información a la gerencia o Jefe de Laboratorio lo más rápidamente posible.	X		
Se requiere que todos los empleados, contratistas y terceros, usuarios del Laboratorio y de los servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.		X	
Se establecen responsabilidades y procedimientos para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.		X	

Gestión de la continuidad de los Servicios	SI	PARCIALMENTE	NO
Se identifican los eventos que causan interrupciones en los procesos de los servicios que ofrece el Laboratorio, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.		X	
Se desarrollan e implementan planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información después de la interrupción o falla en los procesos más críticos.			X
Se mantiene un solo marco referencial de planes de continuidad de servicios para asegurar que todos los planes sean consistentes.			X
Se prueba y actualiza los planes de continuidad de servicios regularmente para asegurar que estén actualizados y sean efectivos.			X

Cumplimiento	SI	PARCIALMENTE	NO
Se implementan procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.			X
Se establece que el gerente o Jefe de Laboratorio, ayudante de Laboratorio asegure que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.		X	
Se planea cuidadosamente los requerimientos y actividades de las auditorías que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos de servicio.			X
Se protege el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.			X

IMPLEMENTACIÓN

Tabla 22: Implementación y Operación del SGSI

FACTORES A CONSIDERAR PARA LA IMPLEMENTACIÓN Y OPERARACIÓN DEL SGSI	SI	PARCIALMENTE	NO
Se identifica la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información.	X		
Se implementa el plan de tratamiento de riesgos.		X	
Se implementan los controles.		X	
Se especifica cómo se van a medir la efectividad de los controles y como se va a utilizar estas			X

mediciones para producir resultados comparables y reproducibles.			
Se implementan los programas de capacitación y conocimiento en lo relativo a la seguridad de la información.			X

SEGUIMIENTO

Tabla 23: Monitoreo y Revisión del SGSI

FACTORES A CONSIDERAR PARA EL MONITOREO Y REVISIÓN DEL SGSI	SI	PARCIALMENTE	NO
Se detecta prontamente los errores en los resultados de procesamiento.	X		
Se identifica prontamente los incidentes y violaciones de seguridad fallidas y exitosas.		X	
Se tiene ayuda del personal, tecnología, software o indicadores que permita ayudar a detectar los eventos de seguridad, evitando así los incidentes de seguridad.		X	
Se determina si son efectivas las acciones tomadas para resolver una violación de seguridad.		X	
Se realizan revisiones regulares de la efectividad del SGSI mediante auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y retroalimentación.			X
Se mide la efectividad de los controles.			X
Se revisa la evaluación de riesgos tomando en cuenta los cambios en: la organización, tecnología, objetivos y procesos, amenazas identificadas, efectividad de los controles implementados; y eventos externos, como cambios en el ambiente legal o regulador, y cambios en el clima social.		X	

Se realizan auditorías internas para conocer si los controles, procesos y procedimientos del SGSI cumplen con los requerimientos de seguridad de la información identificados.			X
Se realizan auditorías internas para conocer si los controles, procesos y procedimientos del SGSI se implementan y mantienen de manera efectiva.			X
Se realizan auditorías internas para conocer si los controles, procesos y procedimientos del SGSI se realizan conforme lo esperado			X
Se actualizan los planes de seguridad teniendo en cuenta los resultados de la monitorización y las revisiones.			X

MEJORA CONTINUA

Tabla 24: Mantenimiento y Mejora del SGSI

FACTORES A CONSIDERAR PARA EL MANTENIMIENTO Y MEJORA DEL SGSI	SI	PARCIALMENTE	NO
Se implementan las mejoras identificadas en el SGSI, por ejemplo; las que se determinaron en la fase seguimiento.		X	
Se aseguran de que las mejoras alcanzan los objetivos pretendidos	X		
Se identifican las inconformidades con los requerimientos del SGSI.			X
Se determinan las causas de las inconformidades.			X
Se evalúa la necesidad de ejecutar acciones correctivas que permitan eliminar la causa de las inconformidades para asegurar que éstas no vuelvan a ocurrir.		X	
Se determinan e implementan las acciones correctivas necesarias.		X	

Se registran los resultados de la acción correctiva tomada.			X
Se revisa la acción correctiva tomada.		X	
Se identifican las inconformidades potenciales con los requerimientos del SGSI y sus causas			X
Se determina e implementa la acción preventiva necesaria.		X	
Se registran los resultados de la acción preventiva tomada.			X
Se revisa la acción preventiva tomada.		X	
Se comunican los resultados y acciones a todas las partes interesadas.	X		

4.2 ANÁLISIS DE RESULTADOS

Para el análisis de resultados se lo hará como se planteó en la sección 4.3, para poder entregar un informe del análisis se lo realizará utilizando dos tipos de tablas: *Interpretación de puntajes obtenidos* y *Presentación de criterios con puntajes altos y bajos*[16], para que de esta manera se puedan establecer las medidas necesarias.

PLANIFICACIÓN

ESTABLECIMIENTO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Tabla 25: Interpretación de Puntajes obtenidos del Establecimiento del Sistema de Gestión de Seguridad de la Información

ASPECTO	PORCENTAJE OBTENIDO	INTERPRETACIÓN
ESTABLECIMIENTO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE	47.6%	BAJO

[16] Tomado de: Guía Práctica para Auditar la Gestión de Redes de área Local, Autores: Pablo Santiago Reyes Villalva, Franklin Estaban Valdivieso Burbano – 2004

LA INFORMACIÓN		

Tabla 26: Presentación de criterios con puntajes altos y bajos del Establecimiento del Sistema de Gestión de Seguridad de la Información

CRITERIOS CON BAJO PUNTAJE	CRITERIOS CON ALTO PUNTAJE
• Identificar una metodología de cálculo del riesgo adecuada. • Tener una metodología de estimación del riesgo que asegure que los cálculos del riesgo produzcan resultados comparables y reproducibles. • Determinar el cálculo del impacto que podría resultar de una falla, teniendo en cuenta las consecuencias de una pérdida de confidencialidad, integridad o disponibilidad de los activos. • Determinar el cálculo de la probabilidad que ocurra dicha falla. • Establecer el cálculo de los niveles de riesgo. • Determinar si el riesgo es aceptable o requiere tratamiento utilizando el criterio de aceptación del riesgo establecido • Transferir los riesgos operativos asociados a otras entidades; por ejemplo: aseguradoras, proveedores.	• Definir el alcance y los límites del Sistema de Gestión de Seguridad de la Información en términos de las características del negocio, la organización, activos, ubicación, tecnología. • Identificar los procesos del negocio que forman parte del Laboratorio. • Justificar cualquier exclusión del alcance que no afecten la capacidad y/o responsabilidad del Laboratorio. • Aprobar la política por la gerencia, en este caso por el Jefe del Laboratorio. • Identificar los activos y su valor en términos de Confidencialidad, Integridad, Disponibilidad y se tiene asignado personal responsable a cargo de estos activos. • Aceptar los riesgos consciente y objetivamente, siempre que satisfagan claramente las políticas y el criterio de aceptación del riesgo.

OBSERVACIÓN.- El Laboratorio debe tomar acciones inmediatas que permitan mejorar la seguridad de la información ya que se encuentran grandes brechas de seguridad que pueden atraer graves problemas al Laboratorio, debido a que se tiene identificado los límites, alcances y política del SGSI pero no se cuenta con una metodología de evaluación y mitigación de riesgos definida.

APLICACIÓN DE LOS CONTROLES

POLÍTICA Y ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Tabla 27: Interpretación de Puntajes obtenidos de la Política y Organización de la Seguridad de la Información

ASPECTO	PORCENTAJE OBTENIDO	INTERPRETACIÓN
POLÍTICA Y ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	64.3%	MODERADO

Tabla 28: Presentación de criterios con puntajes altos y bajos de la Política y Organización de la Seguridad de la Información

CRITERIOS CON BAJO PUNTAJE	CRITERIOS CON ALTO PUNTAJE
• Tener un documento de la política de la seguridad de la información, aprobado por el Jefe de Laboratorio publicado y comunicado a todos los empleados y entidades externas relevantes. • Revisar regularmente la política de seguridad de la información a intervalos planeados o si ocurren cambios significativos. • Identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no divulgación. • Mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales. • Clasificar la información en términos	• Tener el apoyo activo de parte de la gerencia o Jefe de Laboratorio referente a la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado y reconocimiento de las responsabilidades de la seguridad de la información. • Coordinar las actividades de seguridad de la información por representantes de las diferentes partes del Laboratorio con las funciones y roles laborales relevantes. • Definir claramente las responsabilidades de la seguridad de la información. • Definir e implementar un proceso de autorización gerencial para la adquisición o ingreso de los nuevos

de su valor, requerimientos legales, confidencialidad y grado crítico para el Laboratorio	medios de procesamiento de información. • Mantener contactos apropiados con las autoridades relevantes. • Identificar claramente los activos; elaborar y mantener un inventario de todos los activos importantes. • Establecer una persona o entidad que tenga la responsabilidad gerencial para controlar la producción, desarrollo, mantenimiento, uso y seguridad de toda la información y los activos asociados con los medios de procesamiento de la información. • Identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.

OBSERVACIÓN.- El Laboratorio debe mantener el estado de los criterios que se están cumpliendo correctamente o tienen alto puntaje como la Gestión de Activos. Además debe cumplir en su totalidad los criterios como la Organización de la Seguridad de la Información y Clasificación de la Información; finalmente, debe poner énfasis en la documentación de la Política de Seguridad de la Información.

SEGURIDAD DE LOS RECURSOS HUMANOS

Tabla 29: Interpretación de Puntajes obtenidos de la Seguridad de los Recursos Humanos

ASPECTO	PORCENTAJE OBTENIDO	INTERPRETACIÓN
SEGURIDAD DE LOS RECURSOS HUMANOS	66.7%	MODERADO

Tabla 30: Presentación de criterios con puntajes altos y bajos de la Seguridad de los Recursos Humanos

CRITERIOS CON BAJO PUNTAJE	CRITERIOS CON ALTO PUNTAJE
• Definir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.	• Llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, proporcionales a la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos. • Requerir por parte de la gerencia o Jefe de Laboratorio que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización. • Definir y asignar claramente las responsabilidades para realizar la terminación o cambio del empleo. • Establecer que todos los empleados, contratistas y terceros deben devolver todos los activos del Laboratorio u organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.

OBSERVACIÓN.- El Laboratorio debe mantener el estado de los criterios que se están cumpliendo correctamente o tienen alto puntaje. Debe poner énfasis en la documentación de Roles, Responsabilidades de Seguridad de los Empleados y además definir procesos disciplinarios formales cuando alguien ha cometido una

violación en la seguridad, en concordancia con la Política de la Seguridad de la Información.

SEGURIDAD FÍSICA Y AMBIENTAL

Tabla 31: Interpretación de Puntajes obtenidos de la Seguridad Física y Ambiental

ASPECTO	PORCENTAJE OBTENIDO	INTERPRETACIÓN
SEGURIDAD FÍSICA Y AMBIENTAL	72.2%	MODERADO

Tabla 32: Presentación de criterios con puntajes altos y bajos de la Seguridad Física y Ambiental

CRITERIOS CON BAJO PUNTAJE	CRITERIOS CON ALTO PUNTAJE
• Chequear para asegurar que se haya removido o sobrescrito de manera segura cualquier dato confidencial y software con licencia antes de la eliminación de cualquier medio de almacenaje de los equipos.	• Utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información. • Proteger las diferentes áreas del Laboratorio mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado. • Diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastres naturales o creados por el hombre. • Dar un mantenimiento correcto a los equipos para permitir su continua disponibilidad e integridad.

OBSERVACIÓN.- El Laboratorio debe mantener el estado de los criterios que se están cumpliendo correctamente tal como el proceso: Áreas Seguras, aunque deberá aplicar las medidas necesarias para mejorar la Seguridad del Equipo y cumplir en su totalidad con los controles de este criterio.

GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

Tabla 33: Interpretación de Puntajes obtenidos de la Gestión de las Comunicaciones y Operaciones

ASPECTO	PORCENTAJE OBTENIDO	INTERPRETACIÓN
GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES	46.9%	BAJO

Tabla 34: Presentación de criterios con puntajes altos y bajos de la Gestión de las Comunicaciones y Operaciones

CRITERIOS CON BAJO PUNTAJE	CRITERIOS CON ALTO PUNTAJE
• Monitorear, revisar y realizar las auditorías regularmente de los servicios, reportes y registros provistos por terceros. • Producir registros de las actividades de auditoría, eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso. • Proteger los medios de registro y la información del registro contra alteraciones y acceso no autorizado. • Registrar las actividades del administrador y operador del sistema, además debe existir una correcta sincronización de relojes de los sistemas de procesamiento de	• Separar los medios de desarrollo, prueba y operación para reducir los riesgos de accesos no autorizados. • Implementar controles de detección (antivirus actualizados), prevención y recuperación para protegerse de códigos malicioso. • Proteger la integridad de la información disponible públicamente para evitar la modificación no autorizada.

información relevantes	

OBSERVACIÓN.- El Laboratorio debe tomar medidas inmediatas que permitan mejorar la seguridad de la información ya que se encuentran grandes brechas de seguridad que pueden atraer graves problemas al Laboratorio, ya que los procedimientos y responsabilidades se cumplen parcialmente. Tendrá que optimizar procesos tales como: respaldos, gestión de seguridad de la información, gestión de medios, intercambio de información e implementar una gestión de la entrega de servicios de terceros y monitoreo del administrador y operador del sistema.

CONTROL DE ACCESO

Tabla 35: Interpretación de Puntajes obtenidos del Control de Acceso

ASPECTO	**PORCENTAJE ASOCIADO %**	**INTERPRETACIÓN**
CONTROL DE ACCESO	59%	Moderado

Tabla 36: Presentación de criterios con puntajes altos y bajos del Control de Acceso

CRITERIOS CON BAJO PUNTAJE	**CRITERIOS CON ALTO PUNTAJE**
• Establecer que los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar. • Utilizar métodos de autenticación para controlar el acceso de usuarios remotos. • Restringir el acceso de los usuarios y personal de soporte a la información relevante y confidencial	• Controlar la asignación de claves a través de un proceso de gestión formal. • Requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves. • Controlar el acceso físico y lógico. • Establecer que las sesiones inactivas deben cerrarse después

en concordancia con la política de control de acceso definida.	de un período de inactividad definido. • Tener un ambiente de cómputo dedicado (asignado solo para dicha función) para la información más importante y sensible.

OBSERVACIÓN.- El Laboratorio debe mantener el estado de los procesos que se están cumpliendo correctamente o tienen alto puntaje como las Responsabilidades del Usuario, deberá aplicar las medidas necesarias para poder tener una correcta Gestión del Acceso del Usuario, del Control de Acceso a Redes y del Control de Acceso a la Información. Además, se debe cumplir en su totalidad los procesos como el Control de Acceso al Sistema de operación que se cumplen parcialmente, para con esto tener un correcto manejo de la seguridad de la información.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

Tabla 37: Interpretación de Puntajes obtenidos de la Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

ASPECTO	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	50%	Bajo

Tabla 38: Presentación de criterios con puntajes altos y bajos de la Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

CRITERIOS CON BAJO PUNTAJE	CRITERIOS CON ALTO PUNTAJE
• Desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. • Contar con procedimientos para controlar la instalación de software en los sistemas operacionales.	• Valida la fuente de datos para asegurar que los datos sean correctos y apropiados.

OBSERVACIÓN.- El Laboratorio debe mantener el estado del criterio que se está cumpliendo correctamente el cual es: Validar la fuente de datos para asegurar que los datos sean correctos y apropiados. Debe tomar medidas inmediatas que permitan mejorar la Seguridad de la Información ya que se encuentran grandes brechas de seguridad que pueden atraer graves problemas al Laboratorio, ya que no se cuenta con Controles Criptográficos, ni Seguridad de los Archivos del Sistema. Se debe cumplir a cabalidad los procesos que se aplican parcialmente como la Seguridad en los Procesos de Desarrollo y Soporte.

GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

Tabla 39: Interpretación de Puntajes obtenidos de la Gestión de Incidentes en la Seguridad de la Información

ASPECTO	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE	66.67%	Moderado

LA INFORMACIÓN.		

Tabla 40: Presentación de criterios con puntajes altos y bajos de la Gestión de Incidentes en la Seguridad de la Información

CRITERIOS CON BAJO PUNTAJE	CRITERIOS CON ALTO PUNTAJE
	• Se reportan los eventos de seguridad de la información a la gerencia o Jefe de Laboratorio lo más rápidamente posible.

OBSERVACIÓN.- El Laboratorio si reporta los eventos de seguridad de la información al Jefe de Laboratorio lo más rápido posible, por lo que se debe seguir cumpliendo este criterio correctamente como se lo ha hecho hasta ahora, existen procesos que se cumplen parcialmente que se deben cumplir a cabalidad como: la Realización de Reportes de Eventos y Debilidades en la Seguridad de la Información; la Gestión de Incidentes y Mejoras en la Seguridad de la Información.

GESTIÓN DE LA CONTINUIDAD DE LOS SERVICIOS

Tabla 41: Interpretación de Puntajes obtenidos de la Gestión de la Continuidad de los Servicios

ASPECTO	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
GESTIÓN DE LA CONTINUIDAD DE LOS SERVICIOS.	12.5%	Bajo

Tabla 42: Presentación de criterios con puntajes altos y bajos de la Gestión de la Continuidad de los Servicios

CRITERIOS CON BAJO PUNTAJE	CRITERIOS CON ALTO PUNTAJE
• Desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información después de la interrupción o falla en los procesos más críticos. • Mantener un solo marco referencial de planes de continuidad de servicios para asegurar que todos los planes sean consistentes. • Probar y actualizar los planes de continuidad de servicios regularmente para asegurar que estén actualizados y sean efectivos.	

OBSERVACIÓN.- El Laboratorio debe tomar medidas inmediatas que permitan mejorar la seguridad de la información ya que no se cumplen los siguientes criterios: Planes para mantener la disponibilidad de la información, Mantener un solo marco referencial que permita que los planes sean consistentes, Probar y actualizar los planes de continuidad de los servicios. Se debe cumplir a cabalidad el criterio que se aplica parcialmente el cual es: Identificar los eventos que causan interrupciones en los procesos de los servicios, para con esto tener un correcto manejo de la seguridad de la información.

CUMPLIMIENTO

Tabla 43: Interpretación de Puntajes obtenidos del Cumplimiento

ASPECTO	PORCENTAJE ASOCIADO %	INTERPRETACIÓN

CUMPLIMIENTO	12.5%	Bajo

Tabla 44: Presentación de criterios con puntajes altos y bajos del Cumplimiento

CRITERIOS CON BAJO PUNTAJE	CRITERIOS CON ALTO PUNTAJE
• Implementar procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados. • Planear cuidadosamente los requerimientos y actividades de las auditorías que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos de servicio. • Proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.	

OBSERVACIÓN.- El Laboratorio debe tomar medidas inmediatas que permitan mejorar la seguridad de la información debido a que no se cumplen los siguientes procesos: Cumplimiento con los Requerimientos Legales y las Consideraciones para la Auditoría de los Sistemas de Información. Se debe cumplir a cabalidad los criterios que se aplican parcialmente como: Cumplimiento con las Políticas y Estándares de la Seguridad, y el Cumplimiento Técnico.

IMPLEMENTACIÓN

IMPLEMENTACIÓN Y OPERACIÓN DEL SGSI

Tabla 45: Interpretación de Puntajes obtenidos de la Implementación y Operación del SGSI

ASPECTO	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
IMPLEMENTACIÓN Y OPERACIÓN DEL SGSI.	40%	Bajo

Tabla 46: Presentación de criterios con puntajes altos y bajos de la Implementación y Operación del SGSI

CRITERIOS CON BAJO PUNTAJE	CRITERIOS CON ALTO PUNTAJE
• Especificar cómo se van a medir la efectividad de los controles y cómo se va a utilizar estas mediciones para producir resultados comparables y reproducibles. • Implementar los programas de capacitación y conocimiento en lo relativo a la seguridad de la información.	• Identificar la acción gerencial apropiada, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información.

OBSERVACIÓN.- El Laboratorio si identifica la acción gerencial apropiada por lo que debe seguir cumpliendo este criterio correctamente como lo ha realizado hasta ahora. Debe tomar medidas inmediatas que permitan mejorar la seguridad de la información ya que no se cumplen los siguientes procesos: Definición de cómo medir la efectividad de los controles e Implementación de Programas de Capacitación y Conocimiento. Deberá cumplir a cabalidad los procesos que se

cumplen parcialmente como: la Implementación del Plan de Tratamiento de Riesgos e Implementación de Controles, para con esto tener un correcto manejo de la seguridad de la información.

SEGUIMIENTO

SEGUIMIENTO Y REVISIÓN DEL SGSI

Tabla 47: Interpretación de Puntajes obtenidos del Seguimiento y Revisión del SGSI

ASPECTO	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
SEGUIMIENTO Y REVISIÓN DEL SGSI.	27,27%	Bajo

Tabla 48: Presentación de criterios con puntajes altos y bajos del Seguimiento y Revisión del SGSI

CRITERIOS CON BAJO PUNTAJE	CRITERIOS CON ALTO PUNTAJE
• Realizar revisiones regulares de la efectividad del SGSI mediante auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y retroalimentación. • Medir la efectividad de los controles. • Realizar auditorías internas para conocer si los controles, procesos y procedimientos del SGSI cumplen con los requerimientos de seguridad de la información identificados. • Realizar auditorías internas	• Detectar prontamente los errores en los resultados de procesamiento.

para conocer si los controles, procesos y procedimientos del SGSI se implementan y mantienen de manera efectiva. • Realizar auditorías internas para conocer si los controles, procesos y procedimientos del SGSI se realizan conforme lo esperado. • Actualizar los planes de seguridad teniendo en cuenta los resultados de la monitorización y las revisiones.	

OBSERVACIÓN.- El Laboratorio si detecta prontamente los errores en los resultados de procesamiento, pero debe tomar medidas inmediatas ya que no se cumplen los siguientes procesos: Revisiones Regulares de la Efectividad del SGSI, Medición de la Efectividad de los Controles, Auditorías Internas del SGSI a Intervalos Planeados, Actualización de los Planes de Seguridad. Deberá cumplir a cabalidad los procesos que se aplican parcialmente como: la Ejecución de Procedimientos de Monitoreo y Revisión, y otros Controles; la Revisión de las Evaluaciones del Riesgo, para con esto tener un correcto manejo de la seguridad de la información.

MEJORA CONTINUA

MANTENIMIENTO Y MEJORA DEL SGSI

Tabla 49: Interpretación de Puntajes obtenidos del Mantenimiento y Mejora del SGSI

ASPECTO	PORCENTAJE ASOCIADO %	INTERPRETACIÓN
MANTENIMIENTO Y MEJORA DEL	35,71%	Bajo

SGSI.		

Tabla 50: Presentación de criterios con puntajes altos y bajos del Mantenimiento y Mejora del SGSI

CRITERIOS CON BAJO PUNTAJE	CRITERIOS CON ALTO PUNTAJE
• Se identifican las inconformidades con los requerimientos del SGSI. • Se determinan las causas de las inconformidades. • Se registran los resultados de la acción correctiva tomada. • Se identifican las inconformidades potenciales con los requerimientos del SGSI y sus causas. • Se registran los resultados de la acción preventiva tomada.	• Se aseguran que las mejoras alcanzan los objetivos pretendidos. • Se comunican los resultados y acciones a todas las partes interesadas.

OBSERVACIÓN.- El Laboratorio si asegura que las mejoras alcanzan los objetivos pretendidos, comunica los resultados y acciones a todas las partes interesadas, pero debe tomar medidas inmediatas que permitan mejorar la seguridad de la información ya que no se cumplen el siguiente proceso: Tomar las acciones correctivas y preventivas apropiadas. Deberá cumplir a cabalidad el criterio que se cumple parcialmente como es la Implementación de las Mejoras Identificadas en el SGSI.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- De los Laboratorios de Computación encuestados de las diferentes Facultades de Ingeniería en Sistemas el área en la que se ejerce mayor control en el manejo de la seguridad de la información es en la Administración de Activos, es decir, dan prioridad a los procesos de: Inventario de los activos, *Reglas para el uso de la información y de los activo; y Mantenimiento de los equipos.* Sin embargo, existen otros procesos en esta área que no los cumplen a cabalidad, lo que implica que no necesariamente las medidas que se aplican sean efectivas para lograr un correcto manejo de la seguridad de la información.

- Para esta propuesta se realizó la evaluación a 4 Laboratorios de Computación de las diferentes universidades de Quito, del análisis de las evaluaciones se obtuvo que de acuerdo a las preguntas realizadas en la encuesta de los diferentes temas de seguridad no supera el 50% de su cumplimiento, por lo tanto se puede notar que en la actualidad no existe un correcto manejo de la seguridad de la información, en las áreas que existe un menor control en el manejo de la seguridad son: la Seguridad de los Recursos Humanos y la Administración de Incidentes.

- De acuerdo al criterio de los usuarios del Laboratorio los resultados obtenidos del análisis son válidos y son el reflejo actual del mismo, por esta razón se puede decir que la propuesta es un documento que propone criterios de evaluación confiables. La propuesta resulta una herramienta de análisis actual permitiendo con ello identificar los riesgos de seguridad de la información.

- Las observaciones realizadas en el análisis de resultados mediante la propuesta deben ser aplicadas para poder mejorar la seguridad de la

información. Se debe tener en cuenta que para aplicar la propuesta como una herramienta que permita mejorar el manejo de la seguridad de la información, es necesario el apoyo y compromiso de la gerencia o Jefe del Laboratorio.

- Se puede decir que la aplicación de la propuesta es sencilla y rápida, puede ser utilizada por cualquier miembro del Laboratorio que tenga conocimiento del manejo de la información del Laboratorio.

- Esta propuesta está basada en la Norma ISO 27000:2005, la cual es la norma más completa que existe para la implantación de controles, la gestión y la operación de todo lo relacionado con un SGSI, mediante la cual se pretende lograr una correcta gestión de la seguridad de la información para los Laboratorios.

- La seguridad absoluta no existe, lo que se trata es de reducir el riesgo a niveles aceptables. La seguridad es una actividad continua y la aplicación de la propuesta para mejorar la seguridad requiere el soporte del Laboratorio para tener éxito.

- Existen riesgos que se deben tener en cuenta:
  - ✓ La resistencia del personal, debido al temor al cambio.
  - ✓ No asumir que la seguridad de la información es inherente a los procesos del Laboratorio.
  - ✓ Establecer Planes inadecuados concienciación sobre la importancia de la seguridad de la información.
  - ✓ No comunicar las mejoras identificadas en el SGSI al personal del Laboratorio.

RECOMENDACIONES

- Se recomienda el uso de esta propuesta como una herramienta para realizar el análisis de la seguridad de la información en los Laboratorios para el personal técnico que los administra, de manera que puedan conocer cómo se está manejando actualmente la seguridad de la información y cómo se debería manejarla correctamente.

- Es conveniente el uso de esta propuesta como una herramienta, no solo para el análisis sino para la mejora del manejo de la seguridad de la información. Debe ser considerada como un proceso de mejoramiento continuo y no estático, donde se implementen las mejoras identificadas en el SGSI, lo que permitirá asegurar que dichas mejoras alcancen los objetivos pretendidos y que los requerimientos de seguridad se ajusten a los cambios del Laboratorio.

- Se recomienda la aplicación de la propuesta en los diferentes Laboratorios de las universidades, de manera que puedan conocer como se está manejando la Seguridad de la Información, paran que identifiquen los factores críticos a los que se enfrentan y apliquen las medidas necesarias.

- Es necesaria la concienciación del empleado por la importancia de la seguridad.

- Luego de la aplicación de la propuesta se recomienda tomar medidas sobre las observaciones emitidas en el análisis de resultados del caso práctico.

BIBLIOGRAFÍA

- http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas.shtml#cobi

- http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n#Conceptos_Importantes

- Paulina Rosita Galindo Hidalgo, Elaboración de una Guía Práctica para la Implantación de Seguridades Lógicas en el software, Quito, 2001.

- José Luis Villagomes Menéndez, Análisis de la Aplicabilidad de los Planes de Contingencia en las universidades informáticas de Quito, Quito, 2000

- http://www.unjbg.edu.pe/coin/pdf/01010801404.pdf

- http://www.iso27000.es/iso27000.html

- http://www.palisade.com/trials.asp

- http://www.isciii.es/htdocs/redes/investen/publicaciones/calculo_muestra.pdf

- http://ingenieria.url.edu.gt/boletin/URL_02_BAS02.pdf
- http://catarina.udlap.mx/u_dl_a/tales/documentos/lhr/carranza_a_a/capitulo3.pdf
- http://www.monografias.com/trabajos63/control-interno-auditoria/control-interno-auditoria2.shtml

- Mantillas Guayasamín Salome Rosa, Pazos Constante Xavier Renán, Guía para la Aplicación de las Técnicas de Auditoría Informática en las empresas de Quito, Quito Junio 2003.

- Angélica Janeth Caiza Ávila, Margarita Isabel Matute Macías, Evaluación de Riesgos en empresas desarrolladoras de software utilizando la herramienta MSAT, Quito octubre 2007