UTEG
UNIVERSIDAD TECNOLÓGICA EMPRESARIAL DE GUAYAQUIL

Tesis en Opción al Título de:

INGENIERO EN GESTION EMPRESARIAL MENCION GESTION INFORMATICA

Título de la Tesis:

Diseño de Estandares de Seguridad para la UTEG Aplicando la Norma ISO-17799

Autores:

Robert Swanton

Ricardo Guzmán

TUTOR:

Ing. César Bustamante

Octubre del 2007

Guayaquil - Ecuador

INDICE

Agradecimiento *Ricardo Guzmán*

Agradezco infinitamente a mis padres, por todo lo que han hecho por mi, por la confianza que me tienen, por todo su esfuerzo desplegado para hacer de mi un hombre de bien. A mi amigo y compañero Robert Swanton, de quien he aprendido muchas cosas durante este tiempo de amistad. Gracias....

Agradecimiento *Robert Swanton*

Quiero agradecer infinitamente a mis padres que siempre me brindaron su apoyo de manera incondicional, y que siempre creyeron en mi. A mis hermanos Johny y Karen por ser un ejemplo digno a seguir. De manera muy especial a mi amigo y compañero de tesis Ricardo Guzmán.

Dedicatoria *Ricardo Guzmán*

Quiero dedicar este trabajo en primer lugar a Dios, por darme la fortaleza espiritual que me ha hecho superar todos y cada uno de los obstáculos que se me han presentado en la vida. Indudablemente a la mujer, que con su inagotable amor, cariño, paciencia, ternura y muchísima comprensión, ha sido el mas grande soporte en el transcurso de mi vida, mi madre.... .A mi padre, por apoyarme y enseñarme los valores, principios e innumerables cosas que simplemente resultan imposibles de mencionar por su compleja esencia. A mi hermana, por estar siempre conmigo y sus siempre acertados consejos...Y finalmente a Pepin, a quien quiero muchísimo y siempre tengo presente.... Gracias...

Dedicatoria *Robert Swanton*

Este trabajo se lo dedico a mi esposa Judith y en especial a mis dos adoradas hijas Nicole y Michelle . Que esta tesis sea un hermoso ejemplo a seguir para estas dos lindas criaturas del Señor. A mi madre que siempre se esforzó y lucho por que sus hijos sean unos profesionales de bien. A mi padre por ser un pilar de honradez y que supo transmitir y enseñar los valores y principios que todo buen hombre debe poseer.

Resumen

Esta Tesis hace referencia a la aplicación de los 11 dominios de la ISO 17799:2005 en la UTEG, nos valimos de la metodología para el desarrollo del SGSI, auto diagnostico, definición de activos y vulnerabilidades, etc... Lo cual permite al lector pasar de manera ordenada y pormenorizada el despliegue de la norma (hasta donde las limitaciones del proyecto están previstas)

Para finalizar expone informes de cada una de los entregables definidos en la norma (aplicando los alcances y limitaciones) de los 11 secciones que servirán de autoevaluación para determinar cual es el nivel de la organización frente a este tema. Como él mismo dice "los niveles adquieren relevancia dentro del marco estratégico, táctico y operativo de la UTEG"

Resume

This Thesis makes reference to the application of the 11 domains of ISO 17799:2005 in the UTEG, we used ourselves the methodology for the development of the SGSI, self diagnose, definition of assets and vulnerabilities, etc... Which allows the reader to happen of way ordered and detailed the unfolding of the norm (to where the limitations of the project are predicted).

In order to finalize it exposes information of each one of the delivers defined in the norm (applying to the reaches and limitations) of the 11 sections that will serve as self evaluation to determine as it is the level of the organization as opposed to this subject. As he himself says "the levels acquire relevance within the strategic frame, tactical and operative of the UTEG"

1. INTRODUCCION

1.1 Presentación y evolución del problema de investigación

1.1.1 Problemática de seguridad y orígenes de ISO 17799.

La problemática de la seguridad en los sistemas de información surge del acelerado desarrollo e implantación de este tipo de tecnologías, denominadas comúnmente TICs. La rápida implantación que ha tenido Internet en nuestras vidas ha conllevado que cantidades enormes de información (en muchos casos confidencial) estén a disposición de cualquiera. Esta escasa seguridad que hubo en los orígenes del boom de Internet hizo saltar la alarma, de tal forma que la seguridad de la información empezó a tomarse en serio, tanto en el ámbito empresarial, como comercial y por supuesto jurídico-legal.

Pero esta seguridad no afecta sólo al tráfico que circula por la red. Debe entenderse la seguridad como algo integral. Debe abordar problemas desde tráfico en red, hasta seguridad física de servidores y bases de datos de información.

Los gerentes de seguridad de la información han esperado mucho tiempo a que alguien tomara el liderazgo para producir un conjunto de normas de seguridad de la información que estuviera sujeto a auditoría y fuera reconocido globalmente. Se cree que un código de normas de la seguridad apoyaría los esfuerzos de los gerentes de tecnología de la información en el sentido que facilitaría la toma de decisión de compra, incrementaría la cooperación entre los múltiples departamentos por ser la seguridad el interés común y ayudaría a consolidar la seguridad como prioridad empresarial.

Desde su publicación por parte de la Organización Internacional de Normas en diciembre de 2000, ISO 17799 surge como la norma técnica de seguridad de la información reconocida a nivel mundial. ISO 17799 se define como "un completo conjunto de controles que incluye las prácticas exitosas de seguridad de la información".

Durante más de un siglo, el Instituto Británico de Normas Técnicas (BSI) y la Organización Internacional de Normas Técnicas (ISO) han brindado parámetros globales a las normas técnicas de operación, fabricación y desempeño. Solo faltaba que BSI e ISO propusieran una norma técnica para la seguridad de la información.

Finalmente en 1995, el BSI publicó la primera norma técnica de seguridad, BS 7799, la cual fue redactada con el fin de abarcar los asuntos de seguridad relacionados con el ecommerce.

Tras 1995, problemas como el Y2K (año 2000 o efecto 2000) y la Unidad Monetaria Europea (EMU por su sigla en inglés) prevalecieron sobre otros. Para empeorar las cosas, la norma BS 7799 se consideraba inflexible y no tuvo gran acogida. No se presentó la norma técnica en un momento oportuno y los problemas de seguridad no despertaron mucho interés en ese entonces. La escasa implantación de accesos a Internet entre la población tampoco mejoraba esta situación.

Cuatro años después en mayo de 1999, el BSI intentó de nuevo publicar su segunda versión de la norma BS 7799, la que fue una revisión más amplia de la primera publicación. Esta edición sufrió muchas mejoras y perfeccionamientos desde la versión de 1995. En este momento la ISO se percató de estos cambios y comenzó a trabajar en la revisión de la norma técnica BS 7799.

En diciembre de 2000, la Organización Internacional de Normas Técnicas (ISO) adoptó y publicó la primera parte de su norma BS 7799 bajo el nombre de ISO 17799. Alrededor de la misma época, se adoptó un medio formal de acreditación y certificación para cumplir con la norma técnica. Los problemas Y2K y EMU y otros similares se habían solucionado o reducido en 2000 y la calidad total de la norma técnica había mejorado considerablemente. La adopción por parte de ISO de los criterios de la norma técnica BS 7799 recibió gran aceptación por parte del sector internacional y fue en este momento en el que el grupo de normas técnicas de seguridad tuvo amplio reconocimiento.

1.1.2 Definición de ISO 17799.

ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.

ISO 17799 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del

negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la información se define como la preservación de:

- **Confidencialidad:** Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
- **Integridad:** Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.
- **Disponibilidad:** Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad.

ISO 17799 hoy en día es una compilación de recomendaciones para las prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector. La norma técnica fue redactada intencionalmente para que fuera flexible y nunca indujo a las personas que la cumplían para que prefirieran una solución de seguridad específica.

Las recomendaciones de la norma técnica ISO-17799 son neutrales en cuanto a la tecnología y no ayudan a evaluar y entender las medidas de seguridad existentes. Así, la norma discute la necesidad de contar con firewalls, pero no profundiza sobre los tipos de firewalls.

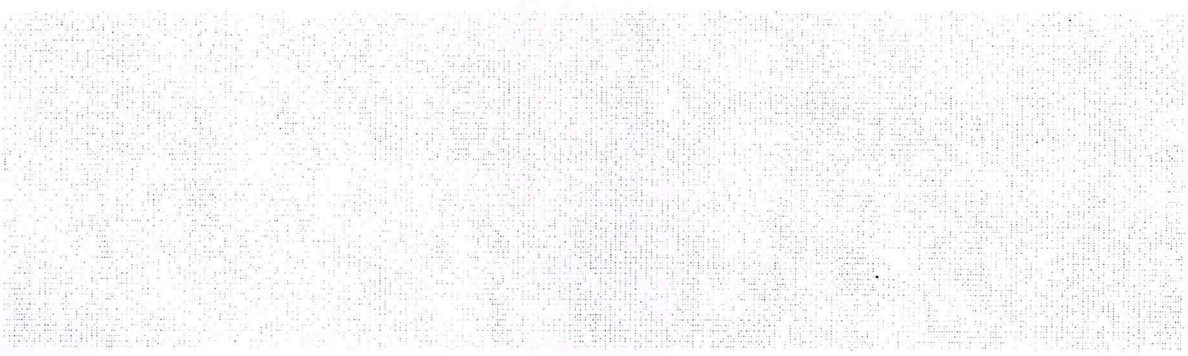
La flexibilidad e imprecisión de ISO-17799 es intencional por cuanto es difícil contar con una norma que funcione en una variedad de entornos de tecnología de la información y que sea capaz de desarrollarse con el cambiante mundo de la tecnología. ISO-17799 simplemente ofrece un conjunto de reglas a un sector donde no existían.

1.1.3 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.

La primera edición fue publicada en 1996; la segunda edición en 1998; la tercera edición en 2000 (la edición on-line estuvo disponible en 2003); y la cuarta edición en Diciembre de 2005, y la versión 4.1 está disponible desde Mayo de 2007.

En su cuarta edición, COBIT tiene 34 objetivos de alto nivel que cubren 318 objetivos de control (específicos o detallados) clasificados en cuatro dominios: Planificación y Organización, Adquisición e Implementación, Entrega y Soporte, y, Supervisión y Evaluación. En inglés: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.

La misión de COBIT es "investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados (dados por alguien con autoridad), actualizados, e internacionales para el uso del día a día de los gestores de negocios (también directivos) y auditores." Gestores, auditores, y usuarios se benefician del desarrollo de COBIT porque les ayuda a entender sus Sistemas de Información (o tecnologías de la información) y decidir el nivel de seguridad y control que es necesario para proteger los activos de sus compañías mediante el desarrollo de un modelo de administración de las tecnologías de la información.



COBIT e ISO/IEC 17799:2005

COBIT fue desarrollado y utilizado sobre todo por la comunidad de IT y se ha convertido en el marco internacionalmente aceptado para el gobierno y control de las TI. ISO/IEC 17799:2005 (el código de la práctica para la gerencia de la seguridad de la información) es también un estándar internacional y es la mejor práctica para poner a la gerencia de la seguridad en ejecución. Los dos estándares no compiten entre si y no complementan realmente uno a otro. COBIT cubre típicamente un área más amplia mientras que ISO/IEC 17799 se enfoca profundamente en el área de la seguridad.

La tabla abajo describe la correlación de los dos estándares:

COBIT DOMAIN	1	2	3	4	5	6	7	8	9	10	11	12	13
Planeación y Organización	-	+	-	-	+	+	+	+	-	-	0	.	.
Adquisición e Implementación	+	0	0	-	0	+	.	.	.	.	.	.	.
Entrega y Soporte	-	+	0	+	+	.	+	0	0	0	+	0	0
Monitoreo y Evaluación	-	0	-	0	.	.	.	.	.	.	.	.	.

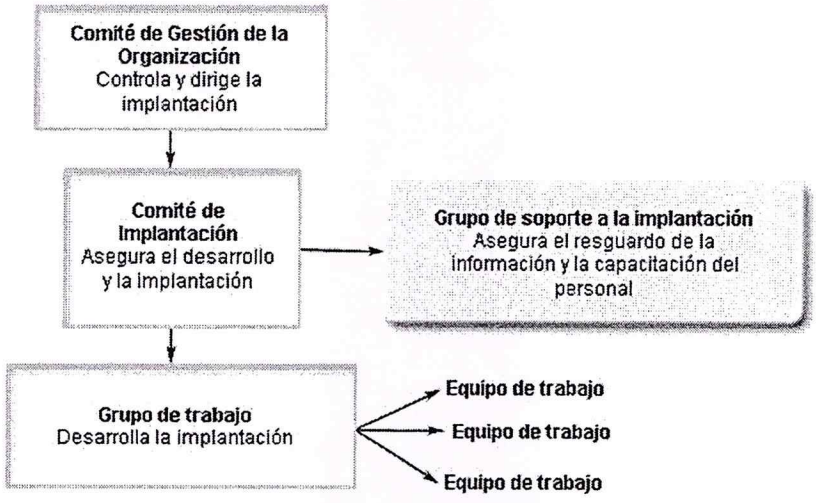
(+) Correlación Total (más de dos objetivos ISO/IEC 17799:2005 mapeados en los procesos de control COBIT)
(0) Correlación Parcial (uno o dos objetivos ISO/IEC 17799:2005 mapeados en los procesos de control COBIT)
(-) Correlación Menor (ningún objetivo ISO/IEC 17799:2005 ha sido mapeados en los procesos de control COBIT)
(.) No existe

1.1.4 Factores críticos del éxito para el desarrollo de la norma ISO-17799 al interior de la UTEG

1. Política de seguridad, objetivos y actividades que reflejen los objetivos de la UTEG
2. Una estrategia de implementación de seguridad que sea consecuente con la cultura organizacional de la UTEG
3. Apoyo y compromiso manifiestos por parte de los directivos.
4. Un claro entendimiento de los requerimientos de seguridad, la evaluación de riesgos y la administración de los mismos.
5. Comunicación eficaz de los temas de seguridad a todos los empleados.
6. Distribución de guías sobre políticas y estándares de seguridad de la información a todos los empleados y contratistas.
7. Instrucción y entrenamiento adecuados.
8. Un sistema integral y equilibrado de medición que se utilice para evaluar el desempeño de la gestión de la seguridad de la información y para brindar sugerencias tendientes a mejorarlo.

1.1.5 Equipo de Planificación del Proyecto: Se formo un comité de dirección del proyecto. Generalmente estará compuesto por el director de tesis, los tesistas y los representantes de la diferentes unidades operativas implicadas.

El director de tesis dirigió las operaciones y fijo prioridades. Los diferentes comités y equipos asociados al proyecto se sugiere tengan la siguiente estructura:



1.2 Definición precisa y resumida del problema

Objetivo General del proyecto

Establecer detalladamente, en función de los controles de seguridad de la norma los activos de información con sus respectivas vulnerabilidades.

Objetivos Específicos:

1. Definir un Sistema de Gestión de Seguridad de la Información (SGSI, o ISMS por sus siglas en inglés) que efectivamente se puede auditar.
2. Proponer recomendaciones sobre el uso de 133 controles de seguridad diferentes aplicados en 11 áreas de control.
3. Exponer a la UTEG los controles necesarios para que establezca y adecue los controles propios de la ISO 17799 a su realidad.

Hipótesis o Ideas a defender

Dado las características propias de la UTEG, como organización de prestación de servicio, es necesario que para un desarrollo sostenido considere el cumplimiento de la normativa de seguridad de la información ISO-17799.

1.2.2 Alcances y Limitaciones

1. Este emprendimiento tuvo un giro (avalado por el Decano de la Facultad de la Tecnología de la Información Ing. Xavier Mosquera) el cual implica hacer el diseño de los estándares en el actual Campus y no en el Campus a construir.

2. El proceso de aplicación de la norma se inicia con:

- Una primera fase que será el desarrollar el SGSI
- Autodiagnóstico
- Definición de aplicabilidad
- Aplicación de los cuestionarios estándar
- Relevamiento de activos lo cual permite establecer vulnerabilidades

3. El presente trabajo no implica mitigación de riesgo, ya que corresponde a decisiones de carácter estratégico (directivos de la organización) y que conllevan más tiempo de asimilación por parte de cualquier organización.

4. Este trabajo se plantea mostrar la realidad del cumplimiento del propio SGSI y recomendaciones (asociadas a las vulnerabilidades e impacto de cada activo) que la UTEG debería tomar en materias de seguridad de la información.

1.3. Descripción del proceso investigativo desarrollado

1.3.1 Inicio del proyecto

Como inicio del proyecto es identificar las direcciones departamentales propias de la UTEG

Dominios de ISO 17799	Dirección y gestión	Finanzas y contabilidad	Recursos humanos	TI/SIG y comunicación	Aspectos legales	Control interno	Terceras partes	Edificios
Política de seguridad	■	■	■	■	■	■	■	■
Seguridad de la UTEG	■	■	■	■	■	■	■	■
Clasificación y control de activos	■	■	■	■	■	■	■	■
Seguridad del personal	■	■	■	■	■	■	■	■
Seguridad física y ambiental	■	■	■	■	■	■	■	■
Gestión de comunicaciones y operaciones	■	■	■	■	■	■	■	■
Control de accesos	■	■	■	■	■	■	■	■
Desarrollo y mantenimiento de sistemas	■	■	■	■	■	■	■	■
Incidentes de la Seguridad	■	■	■	■	■	■	■	■
Administración de la continuidad del negocio	■	■	■	■	■	■	■	■
Cumplimiento	■	■	■	■	■	■	■	■

El Control de la ISO 17799, Comité de Seguridad de la Información, trata en detalle este aspecto.

A definir informante en:

- Dirección y gestión:
- Finanzas y Contabilidad
- Recursos Humanos
- TI/SIG y comunicación
- Aspectos legales
- Edificios

1.3.2 Definición del SGSI

Una vez que se ha creado el comité de dirección se debe definir el alcance del entorno en materia de seguridad de la información para poder centrarse en lo esencial. El perímetro de seguridad puede cubrir los departamentos de la UTEG seleccionados o a toda la UTEG. Se debe tener en cuenta que el SGSI debe someterse a un control interno. Si la UTEG no controla el SGSI, será imposible gestionarlo eficientemente.

Para definir con detalle el SGSI se debe identificar claramente:

Meta / Objetivo	Adopción de la norma
Alcance	¿Qué unidades operativas y actividades estarán cubiertas por el entorno de seguridad de la información? ▪ Respuesta asociada a un mapeo de procesos y la identificación de procesos críticos y de apoyo ▪ Así como una clara representación de las actividades más importantes de la UTEG.
Límites / Limitaciones	Los límites del alcance del SGSI se definen de acuerdo a: ▪ Las características específicas de la UTEG (tamaño, campo de acción, etc.), ▪ Ubicación de la UTEG, ▪ Activos (inventario de todos los datos críticos), ▪ Tecnología
Interfaces	La UTEG debe tener en cuenta las relaciones con otros sistemas, otras organizaciones y proveedores externos. Nota: Todas las relaciones relativas a servicios o actividades no incluidas completamente en la definición del alcance del SGSI deben considerarse a la hora de adoptar la norman y formar parte de la evaluación de riesgos
Dependencias	El SGSI tiene que cumplir ciertos requerimientos de seguridad. Estos requerimientos pueden ser de naturaleza legal o de negocio.
Exclusiones y Justificación de éstas	Todos los elementos y dominios (zona de una red o unidad operativa) definidos en el SGSI no cubiertos todavía por una política de seguridad o medidas de seguridad, deberían estar identificados y las razones para su exclusión claramente justificadas.
Contexto Estratégico	Las medidas de seguridad planificadas deben tener en cuenta la posición actual y futura de la UTEG para alcanzar las metas fijadas por la Dirección General. La adquisición de una nueva compañía, la fusión de infraestructuras existentes o la decisión de contratar sistemas de información a un tercero, son ejemplos de estos objetivos.
Contexto Organizativo	El entorno organizativo afecta a las medidas implantadas para conseguir los objetivos de control fijados por la Dirección. Por ejemplo, las propuestas relativas al acceso remoto a servidores de la compañía para el teletrabajo requieren medidas de seguridad específicas.

1.3.3 Recopilación de la Documentación Existente

Es necesaria una revisión de la documentación existente para evaluar el alcance de las medidas existentes. Los enlaces de cada departamento implicado en la definición del SGSI deberán redactar un inventario de todos los documentos relativos a la seguridad de la información dentro de su propio departamento. A continuación se proporciona una lista de los documentos:

1. Documentos de la política de seguridad,
2. Normas y procedimiento de las políticas (administrativos o técnicos),
3. Informes de evaluación de riesgos
4. Planes de tratamiento de riesgos
5. Documentos que indiquen la existencia de controles de seguridad y su gestión; por ejemplo, informes y pistas de auditoria, informes de incidencias, etc.

1.3.4 Evaluación del riesgo

Cumplimiento de los controles de la ISO 17799: Diagnóstico Preliminar

El diagnóstico preliminar puede usarse para hacer una evaluación inicial del estado de la seguridad del entorno, en relación con los controles, procesos y procedimientos requeridos por la norma ISO 17799. Además, el análisis de las preguntas contribuye a incrementar el conocimiento de la norma y su código de prácticas. El diagnóstico se puede llevar a cabo antes o después de la implementación en caso de que el objetivo de éste sea revisar las diferencias iníciales y medir el nivel de mejora. Además, se puede generar un informe del cumplimiento de la norma ISO 17799 en formato Web.

1.3.5 Identificación y Evaluación de Activos

Datos a proteger

La primera fase del proceso de evaluación del riesgo es la identificación de los datos sensibles y/o críticos. La UTEG debe realizar un inventario de toda la información necesaria para el funcionamiento adecuado del negocio, de las estrategias de marketing, etc. La información puede tener diferentes grados de importancia y debe tratarse de acuerdo éstos (confidencial, sólo para uso interno, público, etc.)

- Respuesta asociada a un mapeo de procesos y la identificación de procesos críticos y de apoyo
- Así como una clara representación de las actividades más importantes de la UTEG.

Puesto que la información es un activo intangible, se debe gestionar, procesar, almacenar, imprimir, eliminar y transmitir a través de medios tangibles. Por lo tanto, de deben identificar los activos intangibles de la UTEG e identificar su valor como una función de los criterios de confidencialidad, integridad, disponibilidad y requerimientos legales). Por ejemplo, una información financiera almacenada en un disco duro puede tener un alto valor confidencial, medio de integridad y medio de disponibilidad, algunas de las siguientes categorías:

- edificios y equipamiento,
- documentos,

- software,
- equipamiento informático,
- recursos humanos,
- servicios.

Categorías	Riesgo	Cantidad
Aplicaciones	0	0
Datos	0	0
Personal	0	0
Servicios	0	0
Tecnología	0	0
Documento electrónico	0	0
Documento en papel	0	0
Equipamiento	0	0
Equipamiento de protección del edificio	0	0
Equipo de protección informático	0	0
Hardware	0	0
Infraestructura	0	0
Instalaciones	0	0
Medios de soporte	0	0
Mobiliario y equipamiento	0	0
Recurso externo	0	0
Recurso interno	0	0
Servicio externo	0	0
Servicio interno	0	0
Software comercial	0	0
Software desarrollado internamente	0	0
Soporte informático	0	0
Telecomunicaciones	0	0

1.3.6 Identificación y Evaluación de Amenazas y Vulnerabilidades

Es importante identificar las vulnerabilidades de todos los activos que den soporte a la información crítica de la UTEG. Dichas vulnerabilidades son sensibles ante amenazas y pueden por lo tanto tener un impacto negativo en la información (revelación, corrupción, pérdida, etc.).

Las restricciones del negocio, las legales en campos específicos y las derivadas de las ubicaciones geográficas deberían estar identificadas. Por ejemplo, una compañía que desarrolle negocios relacionados con la banca en los Estados Unidos está sujeta a las provisiones del "Gram-Leach-Bliley Act." (GLBA).

1.3.7Tratamiento del riesgo

Opciones para el Tratamiento del Riesgo

Una vez que se han identificado y valorado los riesgos, se debe tomar una decisión respecto a la gestión de estos riesgos.

Generalmente hay cuatro opciones para el tratamiento del riesgo:

Reducir el Riesgo	La UTEG implementa o adopta las medidas necesarias para reducir el riesgo a un nivel considerado como aceptable.
Aceptar el Riesgo	La UTEG acepta el riesgo calculado y está preparada para asumir las consecuencias teniendo un conocimiento completo de estos hechos.
Evitar el Riesgo	Ignorar el riesgo nunca es la solución. Sin embargo, los riesgos pueden evitarse moviendo activos potencialmente amenazados fuera de las áreas de riesgo o abandonando por completo las actividades del negocio que generan esas vulnerabilidades en materia de seguridad.
Transferencia del Riesgo	La UTEG transfiere el riesgo mediante la contratación de un seguro o la contratación a terceros por ejemplo.

Selección de Controles

En la mayoría de los casos, la reducción del riesgo es la opción elegida. En consecuencia, se deben fijar los objetivos de control e implementar los controles.

Plan de Tratamiento del Riesgo

El plan de tratamiento del riesgo contiene toda la información requerida para la implementación: funciones y responsabilidades de la gestión, los nombres de los responsables, las prioridades en la gestión de riesgos, etc.

Podrían requerirse medidas adicionales no incluidas en la norma. Una evaluación del riesgo adecuada, así como la asistencia de un consultor externo, podrían ser útiles.

Implementación de Controles

La UTEG ahora debe implementar el plan de tratamiento del riesgo y realizar un seguimiento de la implementación de los controles requeridos en cada uno de los entornos de la información a proteger. Es en esta fase cuando la UTEG implementa los controles administrativos, técnicos-lógicos, físicos y del entorno de acuerdo a sus capacidades de prevención, detección, corrección, recuperación y compensación.

Controles	Componentes	Medidas*
Administrativos	Políticas y procedimientos, Supervisión del personal, Concienciación y formación, Pruebas.	Políticas, normas, procedimientos, guías de acción, procedimientos de selección del personal, procedimientos de finalización de contratos, clasificación y etiquetado de activos, programa de concienciación en materia de seguridad.
Técnicos o Lógicos	Accesos al sistema, Accesos a las redes, Protocolos de cifrado, Áreas de control, Auditoría y verificación	Controles de acceso lógico, cifrado, programas antivirus, tarjetas inteligentes, procedimiento de rellamada, cortafuegos, routers, sistemas de detección de intrusión (IDS).
Físicos	Separación de redes, Perímetros de seguridad, Aislamiento de las áreas de producción, Ordenadores de respaldo, Cableado	Puertas, candados, sistemas de vigilancia, controles del entorno, detección de intrusión o movimiento, alarmas, tarjetas de identificación, medidas biométricas.

Interpretación de las medidas y sus definiciones.

- Disuasión.- Reducir la probabilidad de la amenaza.
- Prevención.- Proteger o reducir la vulnerabilidad del activo.
- Corrección.- Reducir el riesgo o el impacto producido.
- Detección.- Detectar ataques o vulnerabilidades de la seguridad y llevar a cabo las acciones preventivas y correctivas.
- Recuperación.- Restablecer los recursos y capacidades.
- Compensación.- Proporcionar soluciones alternativas u otros controles.

Preparación para la auditoría

Diagnóstico de Cumplimiento del SGSI

La aplicación de la norma ISO-17799 requiere la verificación del cumplimiento de las especificaciones del entorno de gestión.

1.3.8 Declaración de Aplicabilidad

La declaración de aplicabilidad debe producir antes de la auditoría. Este documento proporciona la justificación para la aplicabilidad o no aplicabilidad de cada control de la norma ISO 17799 para el SGSI considerado. Éste además incluye, cuando sea aplicable, el estado de implementación de cada control.

En resumen, los objetivos, controles seleccionados y los motivos para la selección están explicados en él, así como las razones para la exclusión de todas las medidas indicadas en la norma ISO 17799.

Control y mejora continua

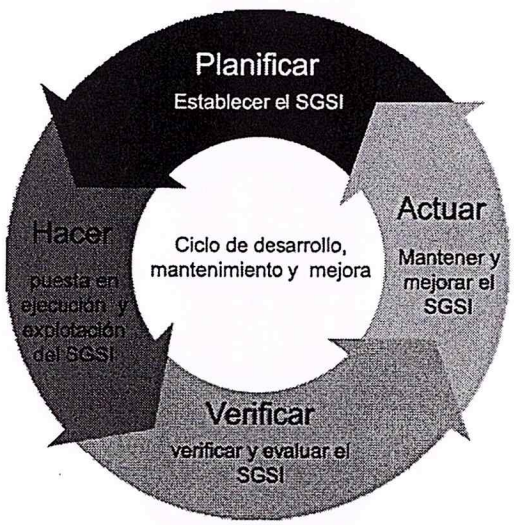
Tanto si está certificado según la norma BS 7799-2 como si no, es importante verificar periódicamente y mejorar su entorno de gestión una vez que se haya implementado. Las inspecciones y actualizaciónes deberían llevarse a cabo regularmente porque la seguridad es un campo sometido a un cambio continuo. Por ejemplo, lo programas antivirus obsoletos o no actualizados no tienen demasiada utilidad.

1.3.9 El Modelo de Gestión PDCA

La edición de 2002 de la norma BS 7799-2 adopta el modelo "Planificar – Hacer – Verificar – Actuar" ("Plan – Do – Check – Act") para ser consistente con las demás normas que ya se estén aplicando como, por ejemplo, la ISO 9001 y las ISO 14001.

Una vez que se ha aplicado al entorno de gestión del SGSI, este modelo pone énfasis en la importancia del hecho de que la gestión del riesgo requiere la implementación de un proceso de gestión cíclico para conseguir la mejora continua del SGSI.

Modelo PHVA



A continuación se muestra una visión general de las cuatro fases:

PDCA	Acción	Explicación
Planificar	Definición del SGSI	- Durante la fase de planificación, es importante considerar el entorno del negocio de la UTEG que implementará el SGSI (Sistema de Gestión de los Sistemas de Información). Se deberían identificar, por ejemplo, directrices corporativas aplicables y requisitos legales. Además de esto, el contexto del negocio de la UTEG debería quedar reflejado en las políticas y objetivos de seguridad y se debería considerar al definir el alcance del SGSI. - Durante la fase de planificación, la UTEG también diseña un procedimiento formal para la continua identificación y evaluación de riesgos y la selección de los objetivos de control y controles que le permitirán gestionar estos riesgos. Al final de este proceso, la UTEG prepara la declaración de aplicabilidad.
Ejecutar	Implementación del SGSI	- A la hora de implementar el SGSI, es importante centrarse inicialmente en el desarrollo e implementación de un plan efectivo y a largo plazo para la mitigación de los riesgos. Durante esta fase, los controles seleccionados en la fase de planificación se implementarán para alcanzar los objetivos de control. Además, se inicia un plan de formación para incrementar la concienciación y conocimiento del personal que garantice la correcta implementación de los controles.
Verificar	Seguimiento y revisión del SGSI	- Durante esta fase, la UTEG lleva a cabo periódicamente auditorías internas del SGSI y realiza un seguimiento regular de la eficiencia del SGSI. Las compañía también revisa el nivel de los riesgos residuales. Esta fase incluye, además, una auditoría de la seguridad por parte del organismo certificador. Esta auditoría, que será realizada por un equipo de auditoría externo cualificado, a menudo va precedida por una auditoría previa. Los consultores cualificados por la BS 7799 pueden proporcionar una ayuda muy útil durante esta fase.
Actuar	Mantenimiento y mejora del SGSI	- Cuando se han identificado las vulnerabilidades y debilidades, se deben llevar a cabo las medidas correctivas y preventivas apropiadas para mejorar el SGSI. Se deben establecer las planificaciones temporales de estas mejoras. Finalmente, durante esta fase, es importante mantener la comunicación con todos los accionistas y continuar proporcionando una formación continua del personal.

Seguimiento y Mejora Continua

En este punto, deben iniciarse los dos pasos restantes del ciclo: seguimiento y mejora del SGSI.

Seguimiento y Revisión del SGSI

En la práctica, para realizar un seguimiento y revisión del SGSI, una UTEG debe realizar las siguientes tareas:

a) Llevar a cabo procedimientos y otros controles de seguimiento para:
   - detectar los errores en los resultados lo antes posible,
   - identificar las incidencias en materia de seguridad lo antes posible,
   - capacitar a la dirección para determinar si las actividades de seguridad de la información implementadas o delegadas se están llevando a cabo como se espera,
   - determinar las acciones a realizar para solucionar las violaciones en materia de seguridad en función de las prioridades del negocio.

b) Realizar revisiones regulares de la eficiencia del SGSI (incluyendo política, objetivos y controles de seguridad) teniendo en cuenta los resultados de las auditorías de seguridad, incidencias, sugerencias e información recogida de todas las partes implicadas.

c) Revisar los niveles de aceptación de riesgos y los riesgos residuales, considerando los cambios en:
   - la UTEG,
   - la tecnología,
   - los objetivos y procesos del negocio,
   - las amenazas identificadas,;
   - los sucesos externos, como cambios en la legislación.

d) Realizar auditorías internas del SGSI periódicamente.

e) Llevar a cabo una revisión de la gestión del SGSI de una manera periódica (al menos una vez al año) para garantizar que el alcance continua siendo adecuado y que las mejoras en los procesos se han identificado. Fomentar una correcta documentación de las revisiones de la gestión del SGSI.

f) Registrar las acciones y situaciones que pueden representar un impacto en la eficiencia o el rendimiento del SGSI.

Mantenimiento y Mejora del SGSI

Para garantizar la gestión continua del SGSI, la UTEG debe:

a) Implementar las mejoras del SGSI identificadas.

b) Llevar a cabo las acciones correctivas y preventivas adecuadas. Aplicar las lecciones aprendidas de las experiencias propias o de otras organizaciones. Documentar las mejoras del SGSI.

c) Comunicar los resultados y las acciones y llegar a acuerdos con todas las partes implicadas.

d) Garantizar que las mejoras consigan los objetivos propuestos.

Revisión de la Gestión del SGSI

General

La Dirección deberá revisar el SGSI de la UTEG a intervalos planificados para garantizar su continua actualización y eficiencia. Esta revisión deberá incluir la evaluación de la oportunidades de mejora y las necesidades de cambios en el SGSI, incluyendo la política y objetivos de seguridad. Los resultados de las revisiones deberán estar claramente documentados y se deben conservar los registros de éstos (véase el control de los registros).

Revisión de las Entradas

La entrada para la revisión de la gestión deberá incluir información sobre:

a) resultados de las auditorías y revisiones del SGSI,

b) feedback de las partes interesadas,

c) técnicas, productos o procedimientos que podrían utilizarse en la UTEG para mejorar el SGSI, performance and effectiveness;

d) estado de las acciones preventivas y correctivas,

e) vulnerabilidades o amenazas no tratadas en los planes de gestión del riesgo previos,

f) acciones de seguimiento indicadas en revisiones previas,

g) cambios que podrían afectar al SGSI,

h) recomendaciones para la mejora.

Revisión de la Salida

El resultado de la revisión de la gestión deberá incluir todas las decisiones y acciones relativas a lo siguiente:

a) Mejora de la efectividad del SGSI,

b) Modificaciones de los procedimientos que afecten a la seguridad de la información cuando estos sean necesarios para poder responder ante sucesos, tanto internos como externos. Se incluirán los cambios en:

- requerimientos de negocio,
- requerimientos de seguridad,
- procesos de negocio que afecten a los requerimientos de negocio existentes,
- entornos legales o normativos,
- niveles de riesgo y/o niveles de aceptabilidad de éstos.

c) Necesidades relativas a los recursos.

Auditorías internas del SGSI

La UTEG deberá realizar auditorías internas del SGSI siguiendo una planificación periódica para determinar si los objetivos de control, controles, procesos y procedimientos de su SGSI:

a) cumplen los requerimientos de esta norma y la legislación y normativa aplicable,
b) cumplen los requerimientos de seguridad de la información identificados,
c) están implementados y son mantenidos eficientemente,
d) funciona de la manera esperada.

Se deberá planificar un programa de auditoría, teniendo en cuenta el estado y la importancia de los procesos y áreas a auditar, así como los resultados de las auditorías previas. Se definirán los criterios para la auditoría, alcance, frecuencia y métodos. La selección de los auditores y el desarrollo de estas auditorías garantizarán la objetividad e imparcialidad del proceso de auditoría. Los auditores no podrán auditar su propio trabajo.

Las responsabilidades y requerimientos para la planificación y desarrollo de las auditoría, y para la comunicación de los resultados y mantenimiento de los registros (véase 4.3.3) deberán estar definidas mediante un procedimiento documentado.

La dirección responsable del área auditada garantizará que se llevan a cabo las acciones propuestas sin retraso para eliminar las no conformidades detectadas y sus causas. Las actividades de mejora incluirán la verificación de las acciones llevadas a cabo y la comunicación de los resultados de estas verificaciones (véase la cláusula 7).

Mejora del SGSI

Mejora Continua

La UTEG mejorará continuamente la eficiencia del SGSI mediante el uso de la política de seguridad de la información, objetivos de control, resultados de auditorías, análisis de las incidencias registradas, acciones preventivas y correctivas, y revisiones de la gestión.

Acción Correctiva

La UTEG llevará a cabo acciones para eliminar las causas de las no conformidades asociadas a la implementación y operativa del SGSI para evitar su recurrencia.

La UTEG llevará a cabo acciones para eliminar las causas de las no conformidades asociadas a la implementación y operativa del SGSI para evitar su recurrencia. Los procedimientos documentados para las acciones correctivas definirán los requerimientos para:

a) identificar las no conformidades de la implementación y/o la operatividad del SGSI,
b) identificar las causas de las no conformidades,
c) evaluar la necesidad de acciones para garantizar que las no conformidades no son recurrentes,
d) identificar e implementar las acciones correctivas necesarias,
e) registrar los resultados de las acciones realizadas (véase el control de registros);
f) revisar las acciones correctivas llevadas a cabo.

Acción Preventiva

La UTEG determinará las acciones para la prevención ante futuras no conformidades. Las acciones preventivas realizadas deberán ser adecuadas para el impacto potencial de éstas. El procedimiento documentado para las acciones preventivas definirán los requerimientos para:

a) identificar las potenciales no conformidades y sus causas,
b) determinar e implementar las acciones preventivas necesarias,
c) registrar los resultados de las acciones realizadas,
d) revisar las acciones preventivas realizadas,
e) identificar los cambios en los riesgos y garantizar que se tienen en cuenta.

La prioridad de las acciones preventivas estará determinada por los resultados de la evaluación de riesgos.

NOTA: Las acciones para prevenir las no conformidades generalmente representan un menor coste que las acciones correctivas.

Control de los Registros

Se establecerán y mantendrán los registros para proporcionar evidencia del cumplimiento de los requerimientos y la eficiente operatividad del SGSI. Estos deberán estar sometidos a control. El SGSI tendrá en cuenta cualquier cambio relevante en los requerimientos legales. Los registros estarán fácilmente accesibles y serán fácilmente comprensibles. Los controles necesarios para la identificación, almacenamiento, protección, recuperación, tiempo de conservación y eliminación de los controles deberán estar documentados. El proceso de gestión determinará las necesidades de estos registros.

Éstos deberán registrar el rendimiento de los procesos y todas las incidencias en materia de seguridad relativas al SGSI.

2. DESARROLLO

2.1 BASES TEORICAS Y METODOLOGICAS DE LA TESIS

En la actualidad cualquier organización debe reconocer que el buen funcionamiento de los sistemas de información es crítico en el desarrollo de sus actividades y, al mismo tiempo, que dichos sistemas se encuentran en situación de riesgo tanto por la propia vulnerabilidad de los sistemas como por una insuficiente implantación de políticas y normas de seguridad. Estas vulnerabilidades pueden producir perdidas de activos de la organización o perdida de la continuidad del negocio cuyo alcance hay que conocer para poder decidir el nivel de riesgo que se está dispuesto a asumir.

Las empresas son conscientes de la gran importancia que tiene para el desarrollo de sus actividades proteger de forma adecuada la información que poseen y especialmente aquella que les sirve para realizar correctamente su actividad de negocio.

El poder gestionar bien la seguridad de la información que manejan no sólo permitirá garantizar, de cara a la propia organización, que sus recursos están protegidos- asegurando la confidencialidad, integridad y disponibilidad de los mismos- sino que de cara a los posibles clientes les aportará un grado de confianza superior al que puedan ofrecer sus competidores, convirtiéndose en un factor más de distinción en el competitivo mercado en el que comercia la empresa.

Debido a la necesidad de securizar la información que poseen las organizaciones era precisa la existencia de alguna normativa o estándar que englobase todos los aspectos a tener en consideración por parte de las organizaciones para protegerse eficientemente frente a todos los probables incidentes que pudiesen afectarla, ante esta disyuntiva apareció el BS 7799, o estándar para la gestión de la seguridad de la información, un estándar desarrollado por el British Standard Institute en 1999 en el que se engloban todos los aspectos relacionados con la gestión de la seguridad de la información dentro de la organización.

La primera pregunta que debe plantearse es: ¿Qué se entiende por información? Y es que a la hora de hablar de información es necesario tener claro a que se esta refiriendo a todo aquel sistema, proceso, dato o elemento que posea la organización y que intervenga en las actividades de negocio de la misma, en otras palabras, información es desde las bases de datos con las que trabaja la organización, hasta los posibles servidores en los

que se almacenan dichas bases de datos, así como las impresoras o carpetas en las que se almacenan los documentos, y por supuesto las personas. Con esto se quiere reflejar al hablar de información nos estamos refiriendo a cualquier elemento que pueda intervenir en el desarrollo de las actividades de negocio de una organización.

Evolución

Si se echa una rápida mirada hacia atrás en el tiempo se vera que a lo largo de la historia el tema de la seguridad dentro de las organizaciones ha ido evolucionando. En un principio se consideraba que los incidentes de seguridad eran cosa de películas o que en "nuestra organización nunca pasarían" y que no era necesario aplicar medidas de seguridad para intentar protegerse ante ellos, posteriormente se conocía de su existencia, pero se pensaba y se señalaba directamente al departamento de informática de la organización como si fuesen los únicos responsables de los mismos y en la actualidad la gran mayoría de las organizaciones ya son conscientes de que no sólo es un tema que afecta al departamento de informática o de sistemas sino que atañe a toda la organización en general y por ello todos tienen que implicarse a la hora de mantener de forma segura los sistemas de información que poseen.

Este paulatino cambio se debe en gran parte a la rápida evolución de las nuevas tecnologías y más concretamente a la rápida expansión de Internet, se ha pasado de trabajar en organizaciones que tenían un campo de actuación bastante restringido o por lo menos bastante controlado a tener que desenvolverse en una globalidad prácticamente absoluta, esto ha facilitado la expansión de las organizaciones dándoles la posibilidad de darse a conocer de forma rápida y llegando a potenciales nuevos clientes a los que anteriormente era imposible acceder, pero también ha fomentado la aparición de nuevos intrusos o de los potenciales peligros que pueden afectar a estas organizaciones. Y es por ello que las empresas se han ido mentalizando de la necesidad de securizar sus propias instalaciones tanto a nivel físico como a nivel lógico para intentar impedir que se vean afectados los sistemas de información que poseen o por lo menos conseguir minimizar los impactos en el caso de que sufran un incidente.

2.1.1 ESTRUCTURA DE LA NORMA:

2.1.2 Dominios de control y objetivos.

La norma ISO-17799 establece 11 dominios de control que cubren por completo la Gestión de la Seguridad de la Información:

1. Política de seguridad.
2. Aspectos organizativos para la seguridad.
3. Clasificación y control de activos.
4. Seguridad ligada al personal.
5. Seguridad física y del entorno.
6. Gestión de comunicaciones y operaciones.
7. Control de accesos.
8. Desarrollo y mantenimiento de sistemas.
9. Incidentes de la Seguridad de la Información
10. Gestión de continuidad del negocio.
11. Conformidad con la legislación.

De estos 11 dominios se derivan 39 objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 133 controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo).

A continuación se comentan los detalles de cada dominio de control:

1. Política de seguridad

- Su objetivo principal es dirigir y dar soporte a la gestión de la seguridad de la información.
- La alta dirección debe definir una política que refleje las líneas directrices de la organización en materia de seguridad, aprobarla y publicitarla de la forma adecuada a todo el personal implicado en la seguridad de la información.
- La política se constituye en la base de todo el sistema de seguridad de la información.
- La alta dirección debe apoyar visiblemente la seguridad de la información en la compañía.

2. Organización de la seguridad

- Gestionan la seguridad de la información dentro de la organización.
- Mantienen la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización que son accedidos por terceros.

- Mantienen también la seguridad de la información cuando la responsabilidad de su tratamiento se ha externalizado a otra organización.
- Debe diseñarse una estructura organizativa dentro de la compañía que defina las responsabilidades que en materia de seguridad tiene cada usuario o área de trabajo relacionada con los sistemas de información de cualquier forma.
- Dicha estructura debe poseer un enfoque multidisciplinar: los problemas de seguridad no son exclusivamente técnicos.

3. Clasificación y control de activos

- Mantener una protección adecuada sobre los activos de la organización. Asegurar un nivel de protección adecuado a los activos de información.
- Debe definirse una clasificación de los activos relacionados con los sistemas de información, manteniendo un inventario actualizado que registre estos datos, y proporcionando a cada activo el nivel de protección adecuado a su criticidad en la organización.

4. Seguridad ligada al personal

- Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios.
- Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo.
- Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.
- Las implicaciones del factor humano en la seguridad de la información son muy elevadas.
- Todo el personal, tanto interno como externo a la organización, debe conocer tanto las líneas generales de la política de seguridad corporativa como las implicaciones de su trabajo en el mantenimiento de la seguridad global.
- Debe haber diferentes relaciones con los sistemas de información: operador, administrador, guardia de seguridad, personal de servicios, etc, y procesos de notificación de incidencias claros, ágiles y conocidos por todos.

5. Seguridad física y del entorno

- Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización.
- Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización.
- Prevenir las exposiciones a riesgo o robos de información y de recursos de tratamiento de información.
- Las áreas de trabajo de la organización y sus activos deben ser clasificadas y protegidas en función de su criticidad, siempre de una forma adecuada y frente a cualquier riesgo factible de índole física (robo, inundación, incendio...).

6. Comunicaciones y gestión de explotación

- Asegurar la operación correcta y segura de los recursos de tratamiento de información.
- Minimizar el riesgo de fallos en los sistemas. Proteger la integridad del software y de la información.
- Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.
- Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.
- Evitar daños a los activos e interrupciones de actividades de la organización.
- Prevenir la pérdida, modificación o mal uso de la información intercambiada entre organizaciones.
- Se debe garantizar la seguridad de las comunicaciones y de la operación de los sistemas críticos para el negocio.

7. Control de acceso al sistema

- Controlar los accesos a la información, evitar accesos no autorizados a los sistemas de información, evitar el acceso de usuarios no autorizados, proteger los servicios en red.
- Evitar accesos no autorizados a ordenadores, el acceso no autorizado a la información contenida en los sistemas.
- Detectar actividades no autorizadas. Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y tele-trabajo.

- Se deben establecer los controles de acceso adecuados para proteger los sistemas de información críticos para el negocio, a diferentes niveles: sistema operativo, aplicaciones, redes, etc.

8. Desarrollo y mantenimiento

- Asegurar que la seguridad está incluida dentro de los sistemas de información.
- Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.
- Proteger la confidencialidad, autenticidad e integridad de la información. Asegurar que los proyectos de Tecnología de la Información y las actividades complementarias son llevadas a cabo de una forma segura.
- Mantener la seguridad del software y la información de la aplicación del sistema.
- Debe contemplarse la seguridad de la información en todas las etapas del ciclo de vida del software en una organización: especificación de requisitos, desarrollo, explotación, mantenimiento...

9. Plan de continuidad

- Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente grandes fallos o desastres.
- Todas las situaciones que puedan provocar la interrupción de las actividades del negocio deben ser prevenidas y contrarrestadas mediante los planes de contingencia adecuados.
- Los planes de contingencia deben ser probados y revisados periódicamente.
- Se deben definir equipos de recuperación ante contingencias, en los que se identifiquen claramente las funciones y responsabilidades de cada miembro en caso de desastre.

10. Conformidad

- Evitar el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad.
- Garantizar la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma.
- Maximizar la efectividad y minimizar la interferencia de o desde el proceso de auditoría de sistemas. Se debe definir un plan de auditoría interna y ser ejecutado convenientemente, para garantizar la detección de desviaciones con respecto a la política de seguridad de la información.

Niveles de seguridad:

- Lógica: Confidencialidad, integridad y disponibilidad del software y datos de un SGI.
- Organizativa: Relativa a la prevención, detección y corrección de riesgos.
- Física: Protección de elementos físicos de las instalaciones: servidores, PCs...
- Legal: Cumplimiento de la legislación vigente.

2.2. Por qué es necesaria la seguridad de la información?

La información y los procesos, sistemas y redes que le brindan apoyo constituyen importantes recursos de la empresa. La confidencialidad, integridad y disponibilidad de la información pueden ser esenciales para mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial.

Las organizaciones y sus redes y sistemas de información, se enfrentan en forma creciente con amenazas relativas a la seguridad, de diversos orígenes, incluyendo el fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio o inundación. Daños tales como los ataques mediante virus informáticos, "hacking" y denegación de servicio se han vuelto más comunes, ambiciosos y crecientemente sofisticados.

La dependencia de las organizaciones respecto de los sistemas y servicios de información denota que ellas son más vulnerables a las amenazas concernientes a seguridad. La interconexión de las redes públicas y privadas y el uso compartido de los recursos de información incrementa la dificultad de lograr el control de los accesos. La tendencia hacia el procesamiento distribuido ha debilitado la eficacia del control técnico centralizado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados. La identificación de los controles que deben implementarse requieren una cuidadosa planificación y atención a todos los detalles. La administración de la seguridad de la información, exige, como mínimo, la participación de todos los empleados de la organización. También puede requerir la participación de proveedores, clientes y accionistas. Asimismo, puede requerirse el asesoramiento experto de organizaciones externas. Los controles de seguridad de la información resultan considerablemente más económicos y eficaces si se incorporan en la etapa de especificación de requerimientos y diseños.

2.3 Preparación para el desarrollo del SGSI

En la UTEG se considera para la implementación de la norma ISO 17799 la siguiente relación entre las unidades operativas:

Dominios ISO 17799	Dirección y gestión	Finanzas y Contabilidad	Recursos Humanos	TI / SIG y comunicación	Secretaria General	Auditoria	Edificios
Política de Seguridad	X	X	X	X	X		
Seguridad de Organización	X	X	X	X		X	X
Clasificación y control de activos		X		X	X	X	
Seguridad del personal		X	X	X	X	X	X
Seguridad física y ambiental		X	X	X			X
Gestión de comunicación y operaciones		X	X	X			X
Control de accesos		X		X		X	
Desarrollo y mantenimiento de sistemas				X		X	
Gestión de Incidentes de la Seguridad de la Información	X	X	X	X	X	X	x
Administración de la continuidad del negocio	X	X	X	X	X	X	X
Cumplimiento			X	X	X	X	

2.3.1 Definición del SGSI

Una vez que se ha creado el comité de dirección se debe definir el alcance del entorno en materia de seguridad de la información para poder centrarse en lo esencial. El perímetro de seguridad puede cubrir los departamentos de la UTEG seleccionados o a toda la UTEG. Se debe tener en cuenta que el SGSI debe someterse a un control interno. Si la UTEG no controla el SGSI, será imposible gestionarlo eficientemente.

2.3.2 Identificación y detalle del SGSI:

Meta / Objetivo	Adopción de la norma
Alcance	Matriculación, registro de notas, pago a proveedores y profesores, controles y asignaciones de accesos, registro de notas, validación, aprobación, homologación, representación / defender UTEG, cumplimiento de las reglas (marco regulatorio), legalización de títulos, proveedores, manejo de personal, roles de pago, mantenimiento, mercadeo, control de pago a profesores, gestión interna administrativa
Límites / Limitaciones	Gestión de la información en (dirección administrativa, dirección jurídica, dirección financiera, dirección de TI)
Interfaces	Sistema Financiero, SRI, Mac Security: seguridad física, Satnet: acceso a internet, Palosanto: proveedor de tecnología, Free zone: tecnología, CONEA: ente acreditador de la calidad, CONESUP: ente regulador de la operación terceros: casero
Dependencias	CONEA: ente acreditador de la calidad; CONESUP: ente regulador de la operación
Exclusiones	Decanatos
Justificación de éstas exclusiones	El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones la visión es desarrollarla desde las otras dependencias hacia los decanatos (dirección académicas)
Contexto Estratégico	Crecimiento, diversificación, desarrollo académico, calidad de servicio, desarrollo de los recursos humanos, desarrollo de campus (Vía a la Costa), acreditación ante el CONEA
Contexto Organizativo	Formar profesionales con mentalidad proactiva, que confirmen los valores e ideales de nacionalidad, justicia social, democracia, paz, solidaridad y defensa de los derechos humanos. ; estudiar, analizar y comparar la realidad regional, del país y del mundo, identificando los problemas para encontrar soluciones desde una perspectiva científica y humana. ; promover la interacción entre la universidad y el sector externo, a través de la asistencia y el apoyo a las iniciativas estudiantiles, empresariales y culturales.

2.4 Detalle del SGSI por dependencia organizacional

2.4.1 Gestión Administrativa.-

Alcance.-

- Contactar proveedores, pago a proveedores
- Manejo de personal, servicios prestados
- Roles de pago
- Evaluar necesidades internas, mantenimiento
- Publicidad y marketing
- Prestamos, anticipo de sueldos
- Mantener control de pago a profesores
- Gestionar transportación
- Gestión Interna Administrativa

Limites-Limitaciones.-

- Roles se generan manualmente
- Gestión de Información manual
- Tecnología: Se acredita con tarjeta de Internet
- (Tarjeta virtual)

Interfaces.-

- Banco Bolivariano, Banco del Pacifico
- Mac Security
- Free Zone: Soporte Técnico
- Distribuidor Juan Eljuri
- Constructora Valero

Dependencias.-

- Conesup

Exclusiones y Justificaciones de estas.-

- Incremento de sueldos
- Se requiere de la autorización del rector
- Publicidad, multitrabajo

Contexto Estratégico.-

- Rediseñar la Planeación Estratégica
- Manuales de Funciones
- Cámara de Industria, Turismo

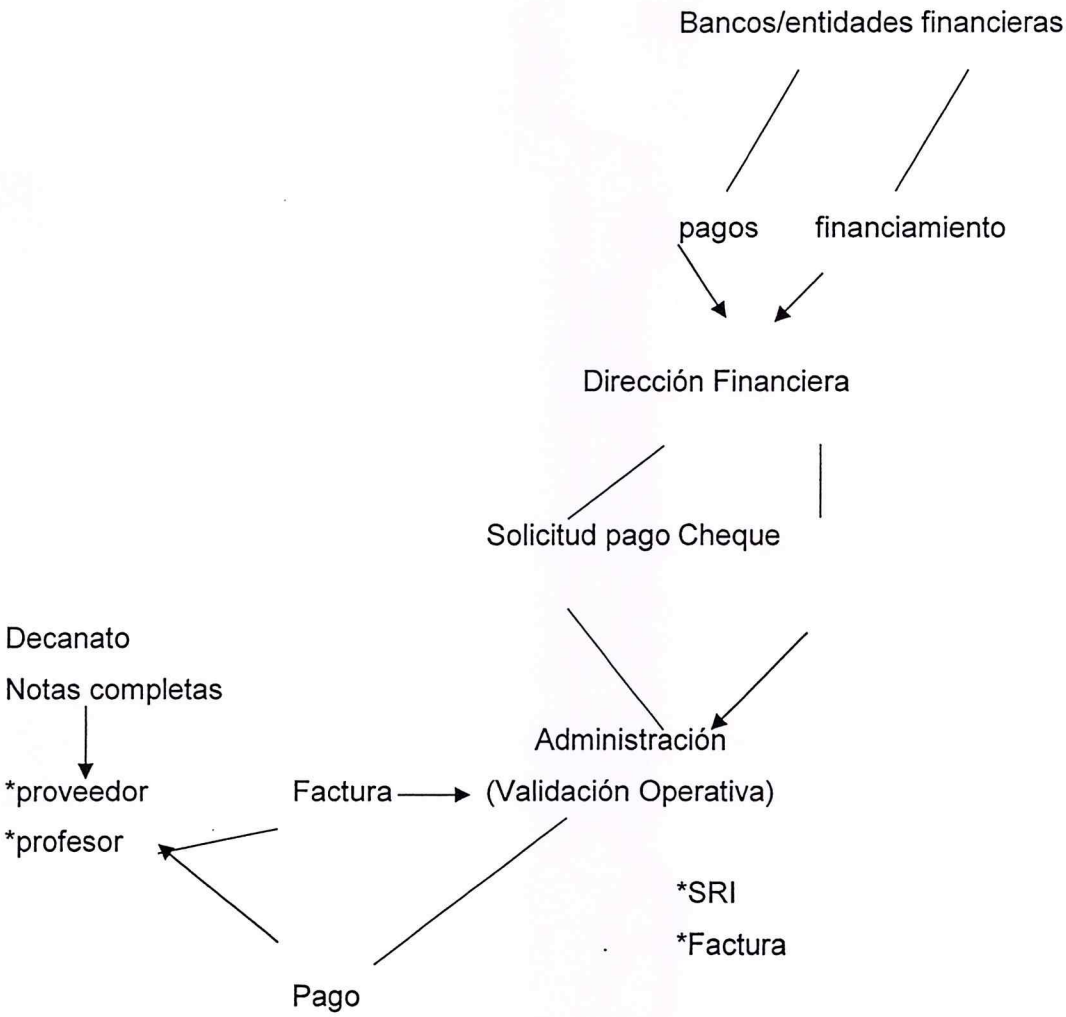
Contexto Organizativo.-

- Servidores SIGA
- Nuevas obligaciones a empleados que no estaban contempladas
- Infraestructura limitada
- Información critica susceptible

Diagrama de relaciones

Pago a Proveedores y Profesores

Procesos financieros



2.4.2 JURIDICO – LEGAL

Alcance.- Registro de Notas, Validación, Aprobación, Homologación, Representación / Defender UTEG, Cumplimiento de las Reglas, Legalizar títulos

Limites / Limitaciones.-

Cumplir con todas las áreas involucradas. A nivel de Tecnología, se cuenta con toda la documentación escrita y archivada. Registro de convenios. No cuentan con un inventario de datos críticos.

Interfaces.-

- Relación con Constructora Valero. (aun no cuentan con permiso de construcción)
- CONEA – CONESUP.
- Bancos (pagos). Bolivariano – Pacifico.
- Mac Security.
- Colegios Economistas, Ing.Industriales, Univ. La Habana, MBA Uruguay, Tec. Monterrey, *becas.

Dependencias.- CONEA – CONESUP

Contexto Estratégico: Ley de Universidades y Escuelas Politécnicas

Contexto Organizativo.-

ANTECEDENTES LEGALES E HISTÓRICOS

La Universidad Tecnológica Empresarial de Guayaquil UTEG fue creada, por iniciativa de la Cámara de Comercio de Guayaquil (CCG), mediante ley 2000 - 50 aprobada por el H. Congreso Nacional, sancionada por el Presidente Constitucional de la República, Dr. Gustavo Noboa Bejarano, y publicada en el Registro Oficial el 31 de enero del 2000, con la finalidad de ofrecer estudios en carreras superiores del tercer nivel. La idea y los esfuerzos para lograrlo fueron impulsados por el señor Joaquín Zevallos Macchiavello presidente de la Cámara de Comercio de Guayaquil. Su primera Rectora fue la doctora Genoveva Zavala de Mayer y su actual Rector es el abogado Marcelo Santos Vera.

La CCG había iniciado su actividad educativa en 1984 con el Instituto de Desarrollo Profesional (IDEPRO), financiado la AID. El éxito alcanzado ha permitido que dicha institución continúe hasta la fecha con seminarios y cursos de capacitación dictados a un promedio de cuatro mil personas al año.

El 6 de marzo de 1995 se fundó el Instituto Tecnológico de Comercio (INTESCO) con la finalidad de formar técnicos titulados en administración, capaces de incorporarse al siglo XXI según las exigencias de nueva economía globalizada.

Importante puntal de crecimiento del INTESCO fue el convenio con la Cámara de Comercio de la ciudad de Sherbrooke, Québec, Canadá, por medio del cual se ofrecía adiestramiento técnico a los profesores de la institución, al mismo tiempo que permitía establecer contactos comerciales entre empresas canadienses y ecuatorianas.

MISIÓN, VISIÓN, OBJETIVOS Y PROPÓSITOS INSTITUCIONALES

MISIÓN

La Universidad Tecnológica Empresarial de Guayaquil UTEG es una universidad privada, abierta a todas las corrientes de pensamiento, cuya función social es la formación de profesionales, la investigación científica y la innovación tecnológica, a partir de un modelo de gestión universitaria que potencia el aprendizaje por problemas, la realización de proyectos de creación y una constante vinculación entre la teoría y la práctica, sustentando valores éticos y morales, con un fuerte compromiso hacia la comunidad, la realidad del entorno, la defensa de los derechos humanos, la democracia y la paz.

VISIÓN

La Universidad Tecnológica Empresarial de Guayaquil UTEG, tiene como objetivo ser la universidad líder en la formación profesional de los empresarios del globalizado mundo de hoy, a base del ejercicio simultáneo de la docencia, la investigación y la práctica laboral en escenarios reales, contribuyendo al desarrollo socioeconómico del país, presente y futuro.

OBJETIVOS: Crecimiento, Diversificación, Desarrollo Académico, Calidad de servicio, Desarrollo de los recursos humanos.

PROPÓSITOS INSTITUCIONALES

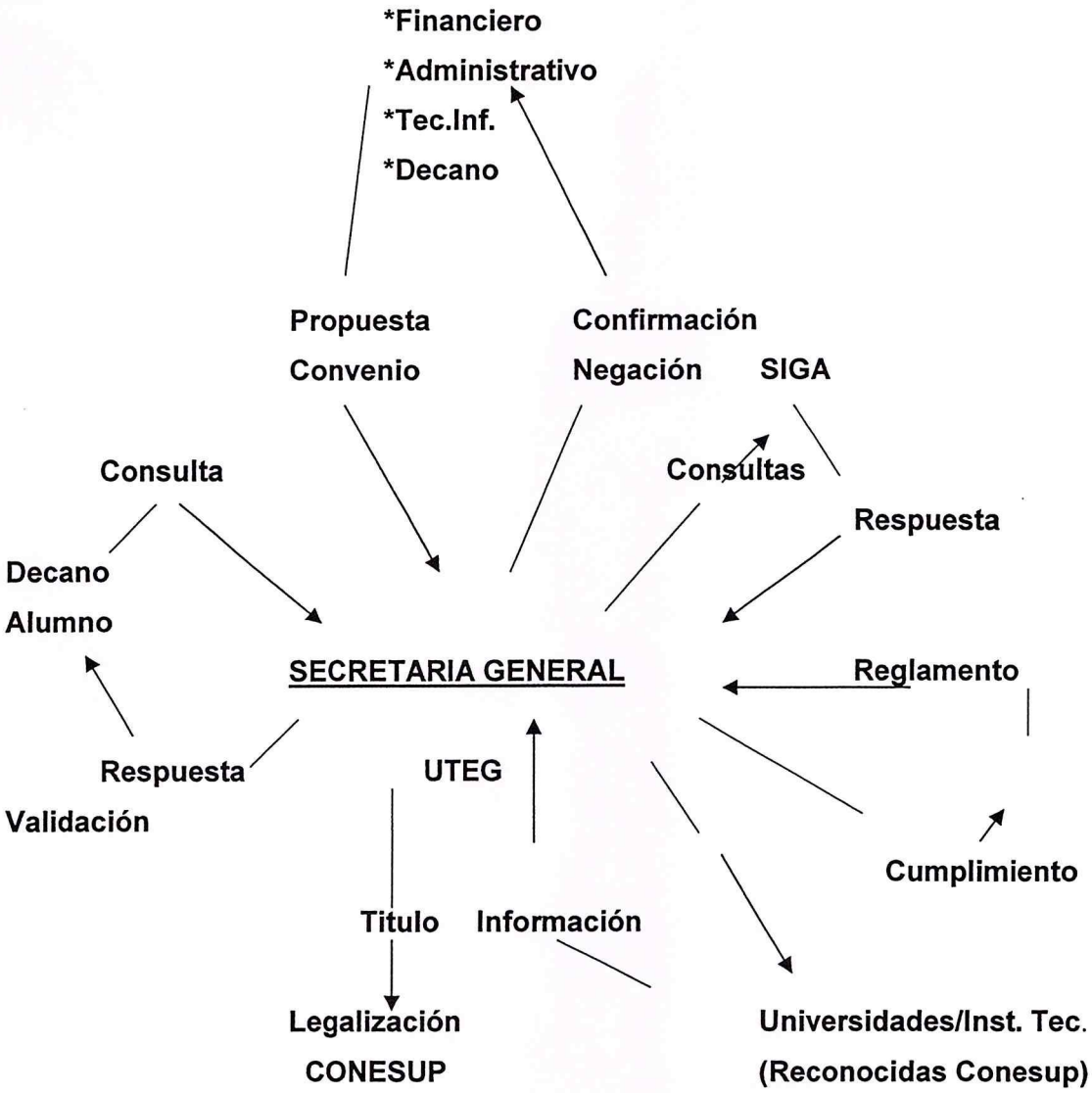
Formar profesionales con mentalidad proactiva, que confirmen los valores e ideales de nacionalidad, justicia social, democracia, paz, solidaridad y defensa de los derechos humanos.

Estudiar, analizar y comparar la realidad regional, del país y del mundo, identificando los problemas para encontrar soluciones desde una perspectiva científica y humana.

Promover la interacción entre la universidad y el sector externo, a través de la asistencia y el apoyo a las iniciativas estudiantiles, empresariales y culturales.

Mapeo de Procesos

Dirección



2.4.3 Tecnologías de la Información (Sistemas)

Alcance.- Tecnología de la Información. (Las actividades serán las siguientes)

1. Matriculación.
2. Registro de Notas
3. Controles y asignaciones de accesos
4. Servicios de Sistemas de Información

Limites / Limitaciones.- Administración de Redes, servidores, accesos a la Web (correo electrónico), Sistema de Gestión Académica, PCW, usuarios – passwords.

Interfaces.-

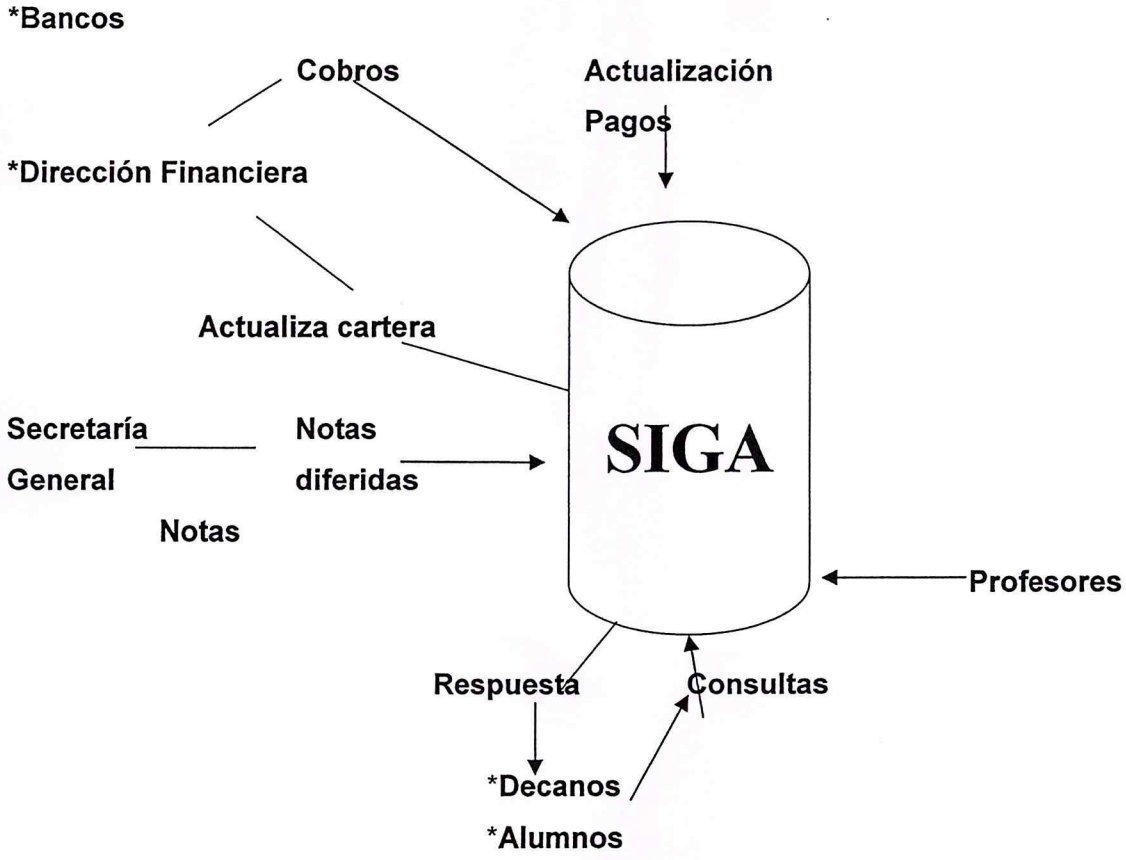
- Pagos en efectivo se realizan en bancos
- (Banco Bolivariano).
- La Compañía que provee de seguridad a la UTEG (Mac Security).
- Servidor en Miami.
- Proveedores locales de equipos de computación.

Dependencias.- En este punto el Ing. Mosquera nos indico que la UTEG es una institución académica autofinanciada, sin fines de lucro; y sin una junta de accionistas conformada: además de la Ley de Universidades y Escuelas Politécnicas

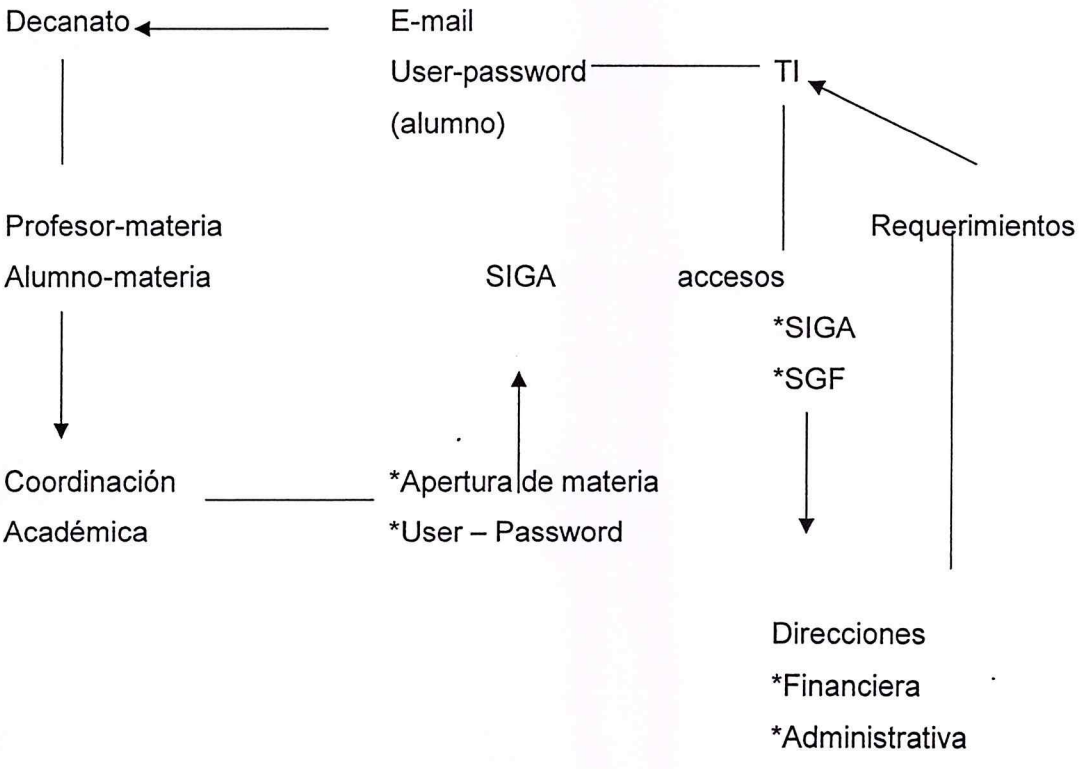
Exclusiones y Justificación de estas.- A validar con el Director Financiero, si solamente la UTEG debe regirse por la Ley de Universidades y Escuelas Politécnicas

Diagrama de relaciones

- Matriculación
- Registro de Notas



Asignación y Controles de Accesos



2.4.4 Finanzas / Contabilidad SGSI

Meta/objetivo: Adopción de la norma

Alcance

1. Administración de cartera/aranceles: Cobro y administración de la cartera a estudiantes, seguimiento de cuentas vencidas, etc.
2. Control y pago a proveedores: Revisión de facturas, revisión vs presupuesto, emisión de pagos (docencia, bienes y servicios generales)
3. Contabilidad: Desarrollo y emisión de estados financieros

Limitaciones

1. Servicio de recaudación externo (bancos): Control pormenorizado al volumen de estudiantes
2. Recepción oportuna de facturas (docentes)
3. Programa del sistema contable no óptimo

Interfaces

1. Relaciones de cobro de las empresas emisoras de tarjetas de crédito (quincenalmente), revisión de los reportes diarios de recaudación de los bancos, control sobre los créditos directos otorgados por la universidad
2. Control de fondos financieros en bancos, supervisión del reporte distributivo de horas de docencia, revisión del presupuesto
3. Relaciones con el SRI, alimentación de información de otros departamentos (RRHH, facultades, etc.)

Dependencias

- Internas: Consejo Universitario
- Externas: SRI, CONESEP, obligaciones financieras bancarias.

2.5 Recopilación de la Documentación Existente

Revisión de la documentación existente para evaluar el alcance de las medidas existentes

Documento	NO existe	Existencia	
		documentada	No documentada
1. Documentos de la política de seguridad	X		
2. Normas y procedimiento de las políticas (administrativos o técnicos)	X		
3. Informes de evaluación de riesgos	X		
4. Planes de tratamiento de riesgos	X		
5. Documentos que indiquen la existencia de controles de seguridad y su gestión	X		
6. Manuales de control interno (finanzas y contabilidad)		X	
7. Plan de continuidad del negocio	X		

2.6 Evaluación del riesgo

¿Por qué es necesaria una evaluación del Riesgo?

Independientemente del tipo o tamaño del negocio (multinacional o PYME), todas las organizaciones son vulnerables a la amenazas que ponen en peligro la confidencialidad, integridad y disponibilidad de la información importante. Cuanto antes se adopten las medidas correctivas, la seguridad representará un menor coste y será más efectiva. Para poder realizar una identificación y selección de controles más sencillas que permitan una mejor gestión de los recursos humanos y financieros, se deben conocer la fuente y naturaleza de las amenazas.

2.6.1 Cumplimiento de los controles de la ISO 17799: Diagnóstico Preliminar

El diagnóstico preliminar puede usarse para conocer el estado de la seguridad del entorno, en relación con los controles, procesos y procedimientos requeridos por la norma ISO 17799. Además, el análisis de las preguntas contribuye a incrementar el conocimiento de la norma y su código de prácticas.

2.7 Autodiagnóstico del SGSI

Resumen de Respuestas : aplicado al Ing. Xavier Mosquera (Decano de la FTI y Director de Sistemas), **ver anexo_01_autodiagnostico_del_sgsi**

- Es inexistente un documento que describa un elemental Sistema de Gestión de la Información (SGSI) lo cual implica que no se han establecidos activos de información, riesgos y sus correspondientes métricas con miras a una mitigación.
- Hay iniciativas aisladas (no formales y/o institucionalizadas) que tratan de establecer algún tipo de política y/o procedimiento encaminado a la seguridad de accesos.

2.7.1 Identificación y Evaluación de Activos

Datos a proteger

La primera fase del proceso de evaluación del riesgo es la identificación de los datos sensibles y/o críticos. La UTEG debe realizar un inventario de toda la información necesaria para el funcionamiento adecuado del negocio, de las estrategias de marketing, etc. La información puede tener diferentes grados de importancia y debe tratarse de acuerdo a estos (confidencial, sólo para uso interno, público, etc.)

Lista de activos ordenada por el valor de los criterios: Confidencialidad

Activo con valor de: (1) Bajo

Lista de Activos		
Nombre	**Descripción**	**Valor - USD ($)**
acta de notas	acta de notas por cada materia	
certificados	certificados de homologaciones, notas, asistencias, etc.	
conectividad	conectividad lan-wan	
documentos de egreso	documentos de egreso	
documentos de ingreso	documentos de ingreso	
mallas	mallas en sistema	
matricula	boleta de inscripción facturada en siga y dada de alta en acade	

Activo con valor de: (2) Medio

Lista de Activos		
Nombre	**Descripción**	**Valor - USD ($)**
desarrollo/definición de software	Desarrollo/definición de software de acuerdo a las necesidades de la UTEG	
helpdesk	helpdesk para usuarios	
historial	historial académico del estudiante	
homologación	acta de homologaciones internas y externas	
inscripción	boleta de inscripción	
mantenimiento	mantenimiento de hardware y software	
materias	rediseño de materias en formato presencial a formato "hibrido"	
pc's	pc's de uso individual de cada propietario	1000
pcw	plataforma de cursos web	4000

Activo con valor de: (3) Alto

Lista de Activos		
Nombre	**Descripción**	**Valor - USD ($)**
acade	sistema de gestión académica	4000
auditoria	auditoria externa	
cartera	cartera de cobro	
estados financieros	desarrollo de estados financieros	
safi	sistema de gestión administrativa-contable-financiera	3000
server linux	servidor donde funciona acade	3000
server safi	servidor donde funciona safi	2000

Identificación y Evaluación de activos

Puesto que la información es un activo intangible, se debe gestionar, procesar, almacenar, imprimir, eliminar y transmitir a través de medios tangibles. Por lo tanto, se deben identificar los activos intangibles de la UTEG e identificar su valor como una función de los criterios de confidencialidad, integridad, disponibilidad y requerimientos legales). Por ejemplo, una información financiera almacenada en un disco duro puede tener un alto valor confidencial, medio de integridad y medio de disponibilidad.

Selección de Categorías de Activos

Estándar	Categorías
COBIT	Aplicaciones
COBIT	Datos
COBIT	Personal
COBIT	Servicios
COBIT	Tecnología
ISO	Documento electrónico
ISO	Documento en papel
ISO	Equipamiento
ISO	Equipamiento de protección del edificio
ISO	Equipo de protección informático
ISO	Hardware
ISO	Infraestructura
ISO	Instalaciones
ISO	Medios de soporte
ISO	Mobiliario y equipamiento
ISO	Recurso externo
ISO	Recurso interno
ISO	Servicio externo
ISO	Servicio interno
ISO	Software comercial

ISO	Software desarrollado internamente
ISO	Soporte informático
ISO	Telecomunicaciones

2.7.2 Lista de Activos de Cada Proceso

SGSI UTEG

Proceso : impartición de clases (Pública)

Lista de Activos :

Nombre	Descripción	Categoría	Identificador	Ubicación	Propietario	Valor - USD ($)
acade	sistema de gestión académica	Aplicaciones	acade	centro de computo, server Miami	Xavier Mosquera	4000
pcw	plataforma de cursos web	Aplicaciones	pcw	centro de computo, server Miami	Xavier Mosquera	4000
matricula	boleta de inscripción facturada en siga y dada de alta en acade	Datos	matricula	acade, siga	Decano	
titulo	legalización de títulos	Datos	titulo	acade, siga	Guido Coppiano	
ups	ups centro de computo	Equipo de protección informático	ups	centro de computo	Xavier Mosquera	500
helpdesk	helpdesk para usuarios	Medios de soporte	helpdesk	sistemas	Xavier Mosquera	
conectividad	conectividad lan-wan	Servicios	conectividad		Xavier Mosquera	
desarrollo de software	desarrollo de software de acuerdo a las necesidades de la UTEG	Servicios	desarrollo software		Xavier Mosquera	
mantenimiento	mantenimiento de hardware y software	Servicios	mantenimiento h&s	sistemas	Xavier Mosquera	
materias	rediseño de	Servicios	materias on line		Xavier	

	materias en formato presencial a formato "hibrido"				Mosquera	
pc's	pc's de uso individual de cada propietario	Tecnología	pc			1000
server linux	servidor donde funciona acade	Tecnología	server linux		Xavier Mosquera	3000

Proceso : matriculación (Sólo para uso interno)

Lista de Activos :

Nombre	Descripción	Categoría	Identificador	Ubicación	Propietario	Valor - USD ($)
acade	sistema de gestión académica	Aplicaciones	acade	centro de computo, server Miami	Xavier Mosquera	4000
pcw	plataforma de cursos web	Aplicaciones	pcw	centro de computo, server Miami	Xavier Mosquera	4000
safi	sistema de gestión administrativa-contable-financiera	Aplicaciones	siga	centro de computo	Cristobal Naranjo	3000
historial	historial académico del estudiante	Datos	historial	acade	Guido Coppiano	
inscripción	boleta de inscripción	Datos	inscripción	acade, siga	Decano	
matricula	boleta de inscripción facturada en siga y dada de alta en acade	Datos	matricula	acade, siga	Decano	
titulo	legalización de títulos	Datos	titulo	acade, siga	Guido Coppiano	
cartera	cartera de cobro	Documento electrónico			Cristobal Naranjo	
certificados	certificados de homologaciones,	Documento en papel	certificados	secretaria académica	Guido Coppiano	

	notas, asistencias, etc.					
documentos de egreso	documentos de egreso	Documento en papel	documentos de egreso	documentos de egreso	Cristobal Naranjo	
ups	ups centro de computo	Equipo de protección informático	ups	centro de computo	Xavier Mosquera	500
helpdesk	helpdesk para usuarios	Medios de soporte	helpdesk	sistemas	Xavier Mosquera	
palo santo	proveedor de soluciones en software (lamp)	Recurso externo	palo santo	palo santo	Xavier Mosquera	
conectividad	conectividad lan-wan	Servicios	conectividad		Xavier Mosquera	
estados financieros	desarrollo de estados financieros	Servicios	estados financieros	contabilidad	Cristobal Naranjo	
pc's	pc's de uso individual de cada propietario	Tecnología	pc			1000
server linux	servidor donde funciona acade	Tecnología	server linux		Xavier Mosquera	3000
server safi	servidor donde funciona safi	Tecnología	alter	centro de computo	Xavier Mosquera	35000

Proceso : cobranza (Privada)

Lista de Activos :

Nombre	Descripción	Categoría	Identificador	Ubicación	Propietario	Valor - USD ($)
acade	sistema de gestión académica	Aplicaciones	acade	centro de computo, server Miami	Xavier Mosquera	4000
safi	sistema de gestión administrativa-contable-financiera	Aplicaciones	siga	centro de computo	Cristobal Naranjo	3000
matricula	boleta de inscripción facturada en siga y dada de alta en	Datos	matricula	acade, siga	Decano .	

	acade					
titulo	legalización de títulos	Datos	titulo	acade, siga	Guido Coppiano	
cartera	cartera de cobro	Documento electrónico			Cristobal Naranjo	
documentos de ingreso	documentos de ingreso	Documento en papel	documentos de ingreso	contabilidad	Cristobal Naranjo	
ups	ups centro de computo	Equipo de protección informático	ups	centro de computo	Xavier Mosquera	500
helpdesk	helpdesk para usuarios	Medios de soporte	helpdesk	sistemas	Xavier Mosquera	
auditoria	auditoria externa	Recurso externo	auditoria	contabilidad	Cristobal Naranjo	
safi	desarrolladores de safi	Recurso externo	desarrollo safi	desarrollo safi	Xavier Mosquera	
conectividad	conectividad lan-wan	Servicios	conectividad		Xavier Mosquera	
desarrollo de software	desarrollo de software de acuerdo a las necesidades de la UTEG	Servicios	desarrollo software		Xavier Mosquera	
estados financieros	desarrollo de estados financieros	Servicios	estados financieros	contabilidad	Cristobal Naranjo	
pc's	pc's de uso individual de cada propietario	Tecnología	pc			1000
server linux	servidor donde funciona acade	Tecnología	server linux		Xavier Mosquera	3000
server safi	servidor donde funciona safi	Tecnología	alter	centro de computo	Xavier Mosquera	35000

Proceso : alta en sistemas de información (Sólo para uso interno)

Lista de Activos :

Nombre	Descripción	Categoría	Identificador	Ubicación	Propietario	Valor - USD ($)
acade	sistema de gestión académica	Aplicaciones	acade	centro de computo, server Miami	Xavier Mosquera	4000
pcw	plataforma de cursos web	Aplicaciones	pcw	centro de computo, server Miami	Xavier Mosquera	4000
acta de notas	acta de notas por cada materia	Datos	acta	acade	Decano	
inscripción	boleta de inscripción	Datos	inscripción	acade, siga	Decano	
mallas	mallas en sistema	Datos	mallas	acade	Guido Coppiano	
matricula	boleta de inscripción facturada en siga y dada de alta en acade	Datos	matricula	acade, siga	Decano	
titulo	legalización de títulos	Datos	titulo	acade, siga	Guido Coppiano	
ups	ups centro de computo	Equipo de protección informático	ups	centro de computo	Xavier Mosquera	500
helpdesk	helpdesk para usuarios	Medios de soporte	helpdesk	sistemas	Xavier Mosquera	
palo santo	proveedor de soluciones en software (lamp)	Recurso externo	palo santo	palo santo	Xavier Mosquera	
conectividad	conectividad lan-wan	Servicios	conectividad		Xavier Mosquera	
desarrollo de software	desarrollo de software de acuerdo a las necesidades de la	Servicios	desarrollo software		Xavier Mosquera	

	UTEG					
pc's	pc's de uso individual de cada propietario	Tecnología	pc			1000
server linux	servidor donde funciona acade	Tecnología	server linux		Xavier Mosquera	3000
satnet	proveedor de enlace a Internet	Telecomunicaciones	satnet	sistemas	Xavier Mosquera	

Proceso : facturación (Privada)

Lista de Activos :

Nombre	Descripción	Categoría	Identificador	Ubicación	Propietario	Valor - USD ($)
acade	sistema de gestión académica	Aplicaciones	acade	centro de computo, server Miami	Xavier Mosquera	4000
safi	sistema de gestión administrativa-contable-financiera	Aplicaciones	siga	centro de computo	Cristobal Naranjo	3000
matricula	boleta de inscripción facturada en siga y dada de alta en acade	Datos	matricula	acade, siga	Decano	
titulo	legalización de títulos	Datos	titulo	acade, siga	Guido Coppiano	
cartera	cartera de cobro	Documento electrónico			Cristobal Naranjo	
documentos de egreso	documentos de egreso	Documento en papel	documentos de egreso	documentos de egreso	Cristobal Naranjo	
documentos de ingreso	documentos de ingreso	Documento en papel	documentos de ingreso	contabilidad	Cristobal Naranjo	
ups	ups centro de computo	Equipo de protección informático	ups	centro de computo	Xavier Mosquera	500

helpdesk	helpdesk para usuarios	Medios de soporte	helpdesk	sistemas	Xavier Mosquera	
auditoria	auditoria externa	Recurso externo	auditoria	contabilidad	Cristobal Naranjo	
palo santo	proveedor de soluciones en software (lamp)	Recurso externo	palo santo	palo santo	Xavier Mosquera	
safi	desarrolladores de safi	Recurso externo	desarrollo safi	desarrollo safi	Xavier Mosquera	
conectividad	conectividad lan-wan	Servicios	conectividad		Xavier Mosquera	
desarrollo de software	desarrollo de software de acuerdo a las necesidades de la UTEG	Servicios	desarrollo software		Xavier Mosquera	
estados financieros	desarrollo de estados financieros	Servicios	estados financieros	contabilidad	Cristobal Naranjo	
pc's	pc's de uso individual de cada propietario	Tecnología	pc			1000
server linux	servidor donde funciona acade	Tecnología	server linux		Xavier Mosquera	3000
server safi	servidor donde funciona safi	Tecnología	alter	centro de computo	Xavier Mosquera	35000

Proceso : legalización de títulos (Pública)

Lista de Activos :

Nombre	Descripción	Categoría	Identificador	Ubicación	Propietario	Valor - USD ($)
acade	sistema de gestión académica	Aplicaciones	acade	centro de computo, server Miami	Xavier Mosquera	4000
acta de notas	acta de notas por cada materia	Datos	acta	acade	Decano	
matricula	boleta de	Datos	matricula	acade, siga	Decano	

	inscripción facturada en siga y dada de alta en acade					
titulo	legalización de títulos	Datos	titulo	acade, siga	Guido Coppiano	
cartera	cartera de cobro	Documento electrónico			Cristobal Naranjo	
certificados	certificados de homologaciones, notas, asistencias, etc.	Documento en papel	certificados	secretaria académica	Guido Coppiano	
titulo	titulo de carrera	Documento en papel	titulo	secretaria académica	Guido Coppiano	
palo santo	proveedor de soluciones en software (lamp)	Recurso externo	palo santo	palo santo	Xavier Mosquera	
conectividad	conectividad lan-wan	Servicios	conectividad		Xavier Mosquera	
desarrollo de software	desarrollo de software de acuerdo a las necesidades de la UTEG	Servicios	desarrollo software		Xavier Mosquera	
pc's	pc's de uso individual de cada propietario	Tecnología	pc			1000
server linux	servidor donde funciona acade	Tecnología	server linux		Xavier Mosquera	3000
server safi	servidor donde funciona safi	Tecnología	alter	centro de computo	Xavier Mosquera	35000

2.8 Diagnóstico de Cumplimiento del SGSI (133 preguntas)

Ver: anexo_02_cuestionario_estandar_iso_133_preguntas

Completar el cuestionario ayudará a determinar la aproximación llevada a cabo por la Dirección, quien permite el desarrollo, control, revisión, mantenimiento y mejora del entorno de gestión adecuado. Éste también verifica la capacidad para gestionar la

documentación necesaria para la certificación y para cumplir con los requerimientos de seguridad inherentes a este proceso.

2.8.1 Resumen del Cuestionario (ponderado de 1 a 100)

Cumplimiento del Cuestionario: 33%

Alcance :

Términos y definiciones :

Estructura de este estándar :

Evaluación y tratamiento del riesgo :

Política de Seguridad : 0

Política de seguridad de la información : 0

Organización de la seguridad de la información : 8

Organización interna : 0

Partes externas : 17

Gestión de activos : 38

Responsabilidad de los activos : 50

Clasificación de la información : 25

Seguridad de los recursos humanos : 39

Previo al empleo : 33

Durante el empleo : 0

Finalización o cambio de empleo : 83

Seguridad física y ambiental : 67

Áreas seguras : 42

Seguridad del equipamiento : 92

Gestión de las comunicaciones y las operaciones : 59

Responsabilidad y procedimientos operacionales : 50

Gestión de servicios provistos por terceras partes : 83

Planificación y aceptación del sistema : 50

Protección contra código móvil y malicioso : 0

Salvaguarda (Back-up) : 50

Gestión de seguridad en la red : 50

Gestión de soportes : 67

Intercambio de información : 75

Servicios de comercio electrónico : 100

Monitorización : 67

Control de acceso : 43

Requerimientos de negocio para control de acceso : 50

Gestión de accesos de usuario : 50

Responsabilidades de usuario : 33

Control de accesos a redes : 58

Control de acceso al sistema operativo : 33

Control de acceso a la información y las aplicaciones : 75

Informática móvil y teletrabajo : 0

Adquisición, desarrollo y mantenimiento de los sistemas de información : 59

Requerimientos de seguridad de los sistemas de información : 100

Procesamiento correcto en las aplicaciones : 63

Controles criptográficos : 50

Seguridad de los ficheros del sistema : 50

Seguridad en el desarrollo y soporte de procesos : 90

Gestión de vulnerabilidades técnicas : 0

Gestión de incidentes de seguridad de la información : 25

Informes de los eventos de seguridad de la información y vulnerabilidades: 50

Gestión de incidentes y mejoras de seguridad de la información : 0

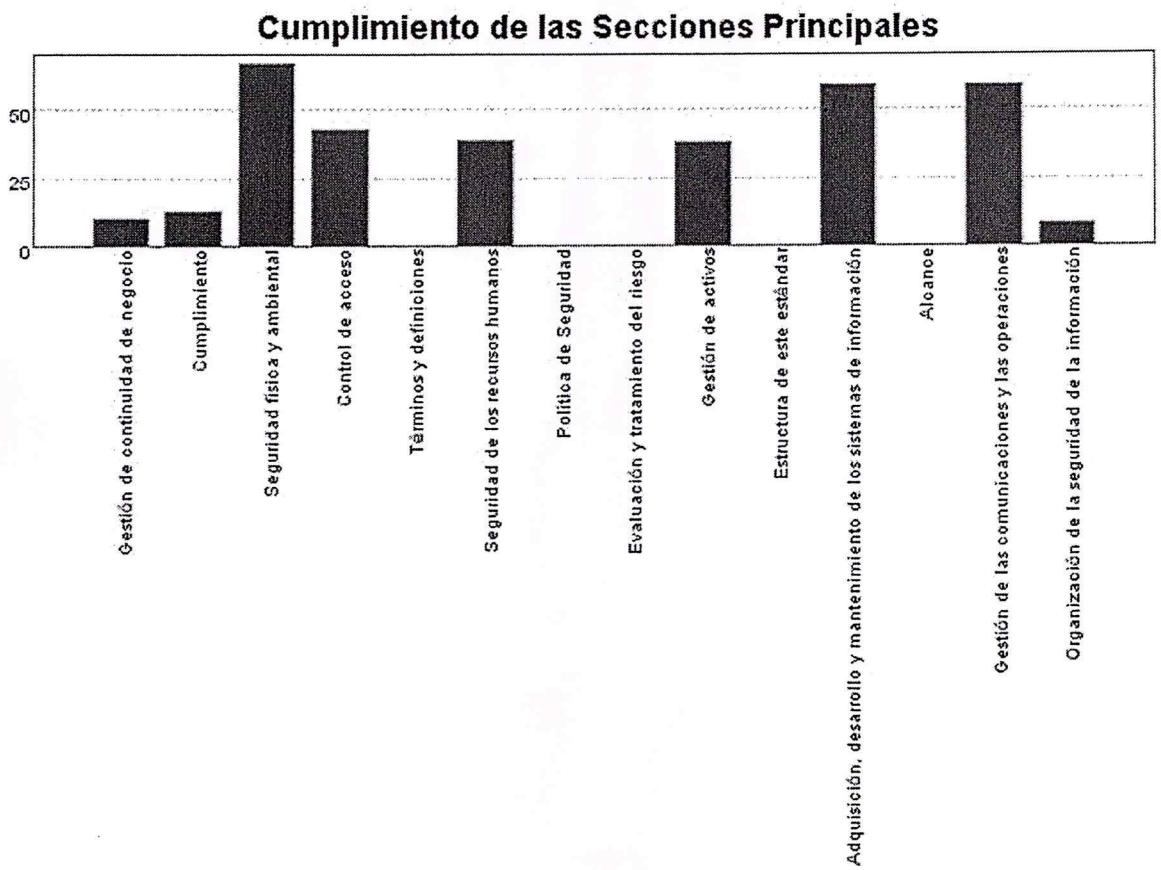
Gestión de continuidad de negocio : 10

Gestión de los aspectos de seguridad de la continuidad de negocio : 10

Cumplimiento : Cumplimiento de los requerimientos legales : 13

Cumplimiento con las políticas y estándares de seguridad y cumplimiento técnico : 0

Consideraciones de auditoría de sistemas de información : 0


Cumplimiento de las Secciones Principales
50
25
0
Gestión de continuidad de negocio
Cumplimiento
Seguridad física y ambiental
Control de acceso
Términos y definiciones
Seguridad de los recursos humanos
Política de Seguridad
Evaluación y tratamiento del riesgo
Gestión de activos
Estructura de este estándar
Adquisición, desarrollo y mantenimiento de los sistemas de información
Alcance
Gestión de las comunicaciones y las operaciones
Organización de la seguridad de la información

2.9 Declaración de Aplicabilidad

Ver:anexo_03_declaracion_de_aplicabilidad

La declaración de aplicabilidad debe realizarse antes de la auditoría. Este documento proporciona la justificación para la aplicabilidad o no aplicabilidad de cada control de la norma ISO 17799 para el SGSI considerado. Éste además incluye, cuando sea aplicable, el estado de implementación de cada control.

En resumen, los objetivos, controles seleccionados y los motivos para la selección están explicados en él, así como las razones para la exclusión de todas las medidas indicadas en la norma ISO 17799.

2.9.1 Secciones donde se verificara la aplicabilidad

Ver: anexo_03_declaracion_de_aplicabilidad

Planificación y Organización

1.1 - Define un Plan Estratégico de Tecnologías de la Información
1.2 - Define la Arquitectura de la Información
1.3 - Determina la Dirección Tecnológica
1.4 - Define la Organización TI y las Relaciones
1.5 - Gestiona la Inversión en TI
1.6 - Comunica los objetivos de la Dirección
1.7 - Gestiona los Recursos Humanos
1.8 - Asegura el Cumplimiento de Requerimientos Externos
1.9 - Evaluación de Riesgos
1.10 - Gestiona Proyectos
1.11 - Gestiona Calidad

Adquisición e Implantación

2.2 - Adquiere y Mantiene Software de Aplicación
2.3 - Adquiere y Mantiene Infraestructuras Tecnológicas
2.4 - Desarrolla y Mantiene Procedimientos
2.5 - Instala y Acredita Sistemas
2.6 - Gestiona Cambios

Distribución y Soporte

3.1 - Define y Gestiona Niveles de Servicio

3.2 - Gestiona Servicios de Terceras Partes

3.3 - Gestiona el Rendimiento y la Capacidad

3.4 - Asegura la Continuidad del Servicio

3.5 - Asegura la Seguridad de los sistemas

3.6 - Identifica y Asigna Costes

3.7 - Educa y Forma a Usuarios

3.8 - Asiste y Aconseja a Usuarios

3.9 - Gestiona la Configuración

3.10 - Gestiona Problemas e Incidentes

3.11 - Gestiona Datos

3.12 - Gestiona Facilidades

3.13 - Gestiona Operaciones

Monitorización

4.1 - Monitoriza los Procesos

4.2 - Evalúa la Adecuación del Control Interno

4.3 - Obtener un seguro independiente

4.4 - Provee Auditoría Independiente

Política de Seguridad

5.1 - Política de seguridad de la Información

Organización de la seguridad de la información

6.1 - Organización interna

6.2 - Partes Externas

Gestión de activos

7.1 - Responsabilidad de los activos

7.2 - Clasificación de la información

Seguridad de los recursos humanos

8.1 - Previo al empleo

8.2 - Durante el empleo

8.3 - Terminación o cambio de empleo

Seguridad física y ambiental

9.1 - Áreas seguras

9.2 - Equipamiento de seguridad

Gestión de operaciones y comunicaciones

10.1 - Procedimientos y responsabilidades operativas

10.2 - Gestión de la provisión de servicios de terceras partes

10.3 - Planificación y aceptación del sistema

10.4 - Protección contra código móvil y malicioso

10.5 - Copia de seguridad

10.6 - Gestión de seguridad de la red

10.7 - Manejo de soportes

10.8 - Intercambio de información

10.9 - Servicios de comercio electrónico

10.10 - Monitorización

Control de accesos

11.1 - Requerimientos de negocio para control de accesos

11.2 - Gestión de acceso de usuarios

11.3 - Responsabilidades de usuario

11.4 - Control de acceso a la red

11.5 - Control de acceso al sistema operativo

11.6 - Control de acceso a la información y a las aplicaciones

11.7 - Informática móvil y teletrabajo

Adquisición, desarrollo y mantenimiento de sistemas de información

12.1 - Requerimientos de seguridad de los sistemas de información

12.2 - Correcto procesamiento de las aplicaciones

12.3 - Controles criptográficos

12.4 - Seguridad de los ficheros del sistema

12.5 - Seguridad en los procesos de soporte y desarrollo

12.6 - Gestión de vulnerabilidades técnicas

Gestión de incidentes de seguridad de la información

13.1 - Informes de eventos y debilidades de seguridad de la información

13.2 - Gestión de incidentes y mejoras de la seguridad de la información

Gestión de continuidad de negocio

14.1 - Aspectos de seguridad de la información de la gestión de la continuidad del

Cumplimiento

15.1 - Cumplimiento de los requerimientos legales

15.2 - Cumplimiento con las políticas, estándares y aspectos técnicos de la seguridad

15.3 - Consideraciones de la auditoría de sistemas de información

2.10 PRESENTACION DE LOS RESULTADOS DE LA TESIS

Esta sección pretende ofrecer, a la UTEG, en detalle en función de los controles de seguridad recomendados (por la norma) los activos y sus vulnerabilidades

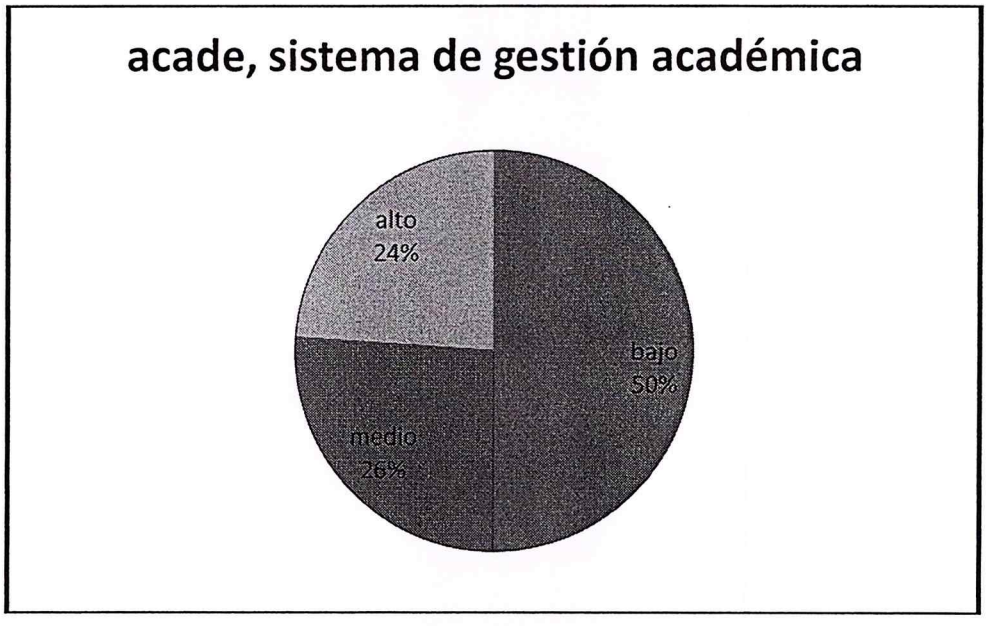
Ver: anexo_04_activos

Activo : acade

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
sistema de gestión académica	Aplicaciones	acade	centro de computo, server Miami	Xavier Mosquera	4000 $

Vulnerabilidad	Nivel
1. Interfaz de usuario excesivamente complicada	(1) Bajo
2. Uso inadecuado del software o hardware	(1) Bajo
3. Formación en materia de seguridad insuficiente	(1) Bajo
4. Ausencia de copias de respaldo	(1) Bajo
5. Ausencia de mecanismos de identificación y autenticación	(1) Bajo
6. Ausencia de mecanismos de monitorización	(1) Bajo
7. Pruebas del software insuficientes o inexistentes	(1) Bajo
8. Descarga y/o uso de software sin control	(1) Bajo
9. Asignación inadecuada de permisos de acceso	(1) Bajo
10. Transferencia de contraseñas en claro	(1) Bajo
11. Ausencia de personal	(1) Bajo
12. Temperaturas extremas	(1) Bajo
13. Gestión inadecuada de la red	(1) Bajo
14. Controles de acceso físico a las instalaciones inadecuados o inexistentes	(1) Bajo
15. Servicio de mantenimiento inadecuado	(1) Bajo
16. Falta de cuidado en la eliminación	(1) Bajo
17. Ausencia de protección física del edificio, puertas y ventanas	(1) Bajo
18. Ubicación en áreas susceptibles de inundarse	(1) Bajo
19. Especificaciones a los desarrolladores poco claras o incompletas	(1) Bajo
20. Copias sin control	(1) Bajo
21. Líneas de comunicación sin protección	(1) Bajo
22. Tablas de contraseñas sin protección	(1) Bajo
23. Trabajo de personal externo sin supervisar	(1) Bajo
24. Vulnerabilidades conocidas del software	(1) Bajo
25. Mantenimiento inadecuado de los medios de almacenamiento	(2) Medio
26. Ausencia de concienciación en materia de seguridad	(2) Medio
27. Gestión inadecuada de contraseñas	(2) Medio
28. Ausencia de control de cambios	(2) Medio
29. Almacenamiento sin protección	(2) Medio
30. Líneas de llamada	(2) Medio

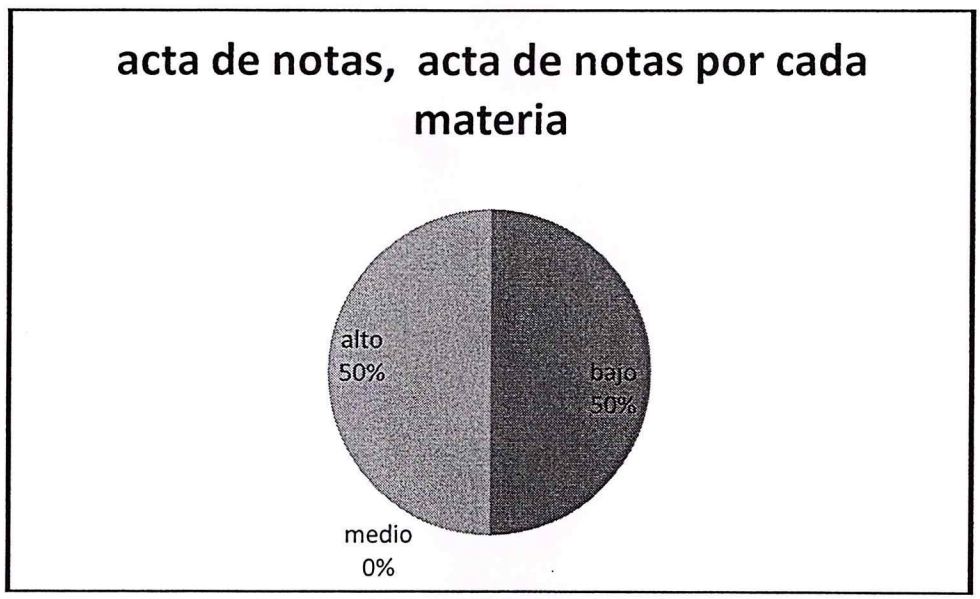
31. Eliminación o reutilización de medios de almacenamiento sin haberlos borrado adecuadamente	(2) Medio
32. Procedimientos de contratación inadecuados	(2) Medio
33. Ausencia de registros y pruebas de envío y recepción de mensajes	(2) Medio
34. Un único punto de fallo	(2) Medio
35. Conexiones a redes públicas sin protección	(2) Medio
36. Tráfico de información sensible sin protección	(2) Medio
37. Ausencia de pistas de auditoría	(3) Alto
38. No realizar "logout" al dejar el puesto de trabajo	(3) Alto
39. Ausencia de documentación	(3) Alto
40. Ausencia de identificación y autenticación del emisor receptor	(3) Alto
41. Ausencia de procedimientos de sustitución periódica	(3) Alto
42. Ausencia de políticas relativas al uso correcto de las infraestructuras de comunicaciones	(3) Alto
43. Conexiones de cables inadecuadas	(3) Alto
44. Sensibilidad a la radiación electromagnética	(3) Alto
45. Sensibilidad a la humedad, polvo, etc.	(3) Alto
46. Sensibilidad a las variaciones de temperaturas	(3) Alto
47. Sensibilidad a las variaciones de voltaje	(3) Alto



Activo : acta de notas

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
acta de notas por cada materia	Datos	acta	Acade	Decano	-

Vulnerabilidad	Nivel
1. Gestión inadecuada de la red aplicable	(0) No
2. Controles de acceso físico a las instalaciones	(1) Bajo
3. inadecuados o inexistentes	
4. Ausencia de pistas de auditoría	(3) Alto



Activo : auditoria

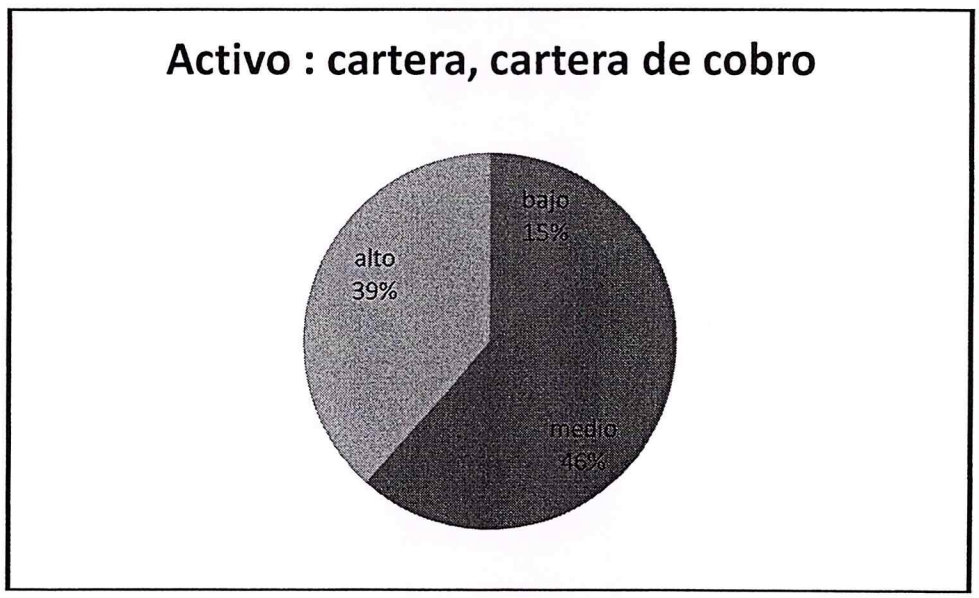
Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
auditoria externa	Recurso externo	auditoria	contabilidad	Cristobal Naranjo	-

Vulnerabilidad	Nivel
1. Ausencia de personal aplicable	(0) No
2. Procedimientos de contratación inadecuados aplicable	(0) No
3. Trabajo de personal externo sin supervisar aplicable	(0) No
4. Uso inadecuado del software o hardware	(1) Bajo
5. Ausencia de concienciación en materia de seguridad	(1) Bajo
6. Formación en materia de seguridad insuficiente	(2) Medio

Activo : cartera

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
cartera de cobro	Documento electrónico			Cristobal Naranjo	-

Vulnerabilidad	Nivel
1. Sensibilidad a la radiación electromagnética	(0) No aplicable
2. Transferencia de contraseñas en claro	(0) No aplicable
3. Ausencia de mecanismos de monitorización	(1) Bajo
4. Gestión inadecuada de contraseñas	(1) Bajo
5. Mantenimiento inadecuado de los medios de almacenamiento	(2) Medio
6. Ausencia de copias de respaldo	(2) Medio
7. Ausencia de mecanismos de identificación y autenticación	(2) Medio
8. Ausencia de identificación y autenticación del emisor o receptor	(2) Medio
9. Ausencia de concienciación en materia de seguridad	(2) Medio
10. Copias sin control	(2) Medio
11. Formación en materia de seguridad insuficiente	(3) Alto
12. Ausencia de pistas de auditoría	(3) Alto
13. Falta de cuidado en la eliminación	(3) Alto
14. Ausencia de políticas relativas al uso correcto de las infraestructuras de comunicaciones	(3) Alto
15. Ausencia de registros y pruebas de envío y	(3) Alto
16. recepción de mensajes	



Activo : certificados

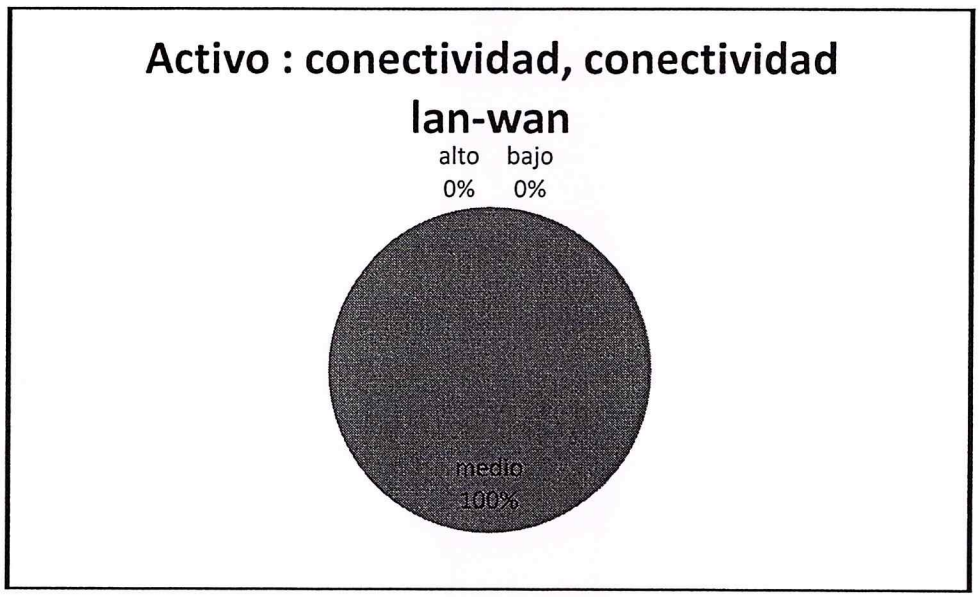
Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
certificados de homologaciones, notas, asistencias, etc.	Documento en papel	certificados	secretaria académica	Guido Coppiano	-

Vulnerabilidad	Nivel
1. Trabajo de personal externo sin supervisar aplicable	(0) No
2. Temperaturas extremas	(1) Bajo
3. Controles de acceso físico a las instalaciones inadecuados o inexistentes	(1) Bajo
4. Formación en materia de seguridad insuficiente	(1) Bajo
5. Ausencia de documentación	(1) Bajo
6. Ausencia de protección física del edificio, puertas y ventanas	(1) Bajo
7. Sensibilidad a la humedad, polvo, etc.	(1) Bajo
8. Sensibilidad a las variaciones de temperaturas	(1) Bajo
9. Ausencia de concienciación en materia de seguridad	(2) Medio
10. Almacenamiento sin protección	(2) Medio
11. Ubicación en áreas susceptibles de inundarse	(3) Alto

Activo : conectividad

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
conectividad lan-wan	Servicios	conectividad		Xavier Mosquera	-

Vulnerabilidad	Nivel
1. Eliminación o reutilización de medios de almacenamiento sin haberlos borrado adecuadamente	(0) No aplicable
2. Ausencia de copias de respaldo	(0) No aplicable
3. Ausencia de personal	(2) Medio
4. Interfaz de usuario excesivamente complicada	(2) Medio
5. Líneas de llamada	(2) Medio



Activo : desarrollo de software

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
desarrollo de software de acuerdo a las necesidades de la UTEG	Servicios	desarrollador acade		Xavier Mosquera	-

Vulnerabilidad	Nivel
1. Eliminación o reutilización de medios de almacenamiento sin haberlos borrado adecuadamente	(0) No aplicable
2. Interfaz de usuario excesivamente complicada	(1) Bajo
3. Líneas de llamada	(2) Medio
4. Ausencia de copias de respaldo	(2) Medio
5. Ausencia de personal	(3) Alto

Activo : documentos de egreso

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
documentos de egreso	Documento en papel	documentos de egreso	Documentos de egreso	Cristobal Naranjo	-

Vulnerabilidad	Nivel
1. Trabajo de personal externo sin supervisar	(0) No aplicable
2. Temperaturas extremas	(1) Bajo
3. Formación en materia de seguridad insuficiente	(1) Bajo
4. Ausencia de documentación	(1) Bajo
5. Ausencia de protección física del edificio, puertas y ventanas	(1) Bajo
6. Sensibilidad a las variaciones de temperaturas	(1) Bajo
7. Controles de acceso físico a las instalaciones inadecuados o inexistentes	(2) Medio
8. Ausencia de concienciación en materia de seguridad	(2) Medio
9. Almacenamiento sin protección	(2) Medio
10. Ubicación en áreas susceptibles de inundarse	(3) Alto
11. Sensibilidad a la humedad, polvo, etc.	(3) Alto

Activo : documentos de ingreso

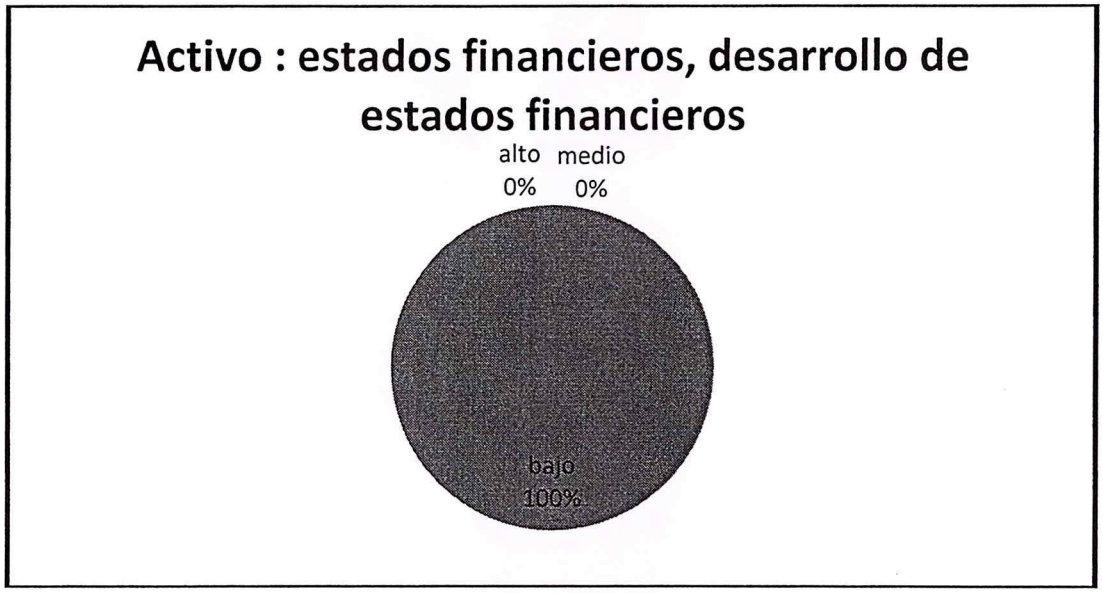
Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
documentos de ingreso	Documento en papel	documentos de ingreso	contabilidad	Cristobal Naranjo	-

Vulnerabilidad	Nivel
1. Trabajo de personal externo sin supervisar	(0) No aplicable
2. Temperaturas extremas	(1) Bajo
3. Formación en materia de seguridad insuficiente	(1) Bajo
4. Ausencia de documentación	(1) Bajo
5. Ausencia de protección física del edificio, puertas y ventanas	(1) Bajo
6. Sensibilidad a las variaciones de temperaturas	(1) Bajo
7. Controles de acceso físico a las instalaciones inadecuados o inexistentes	(2) Medio
8. Ausencia de concienciación en materia de seguridad	(2) Medio
9. Almacenamiento sin protección	(2) Medio
10. Ubicación en áreas susceptibles de inundarse	(3) Alto
11. Sensibilidad a la humedad, polvo, etc.	(3) Alto

Activo : estados financieros

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
desarrollo de estados financieros	Servicios	estados financieros	contabilidad	Cristobal Naranjo	-

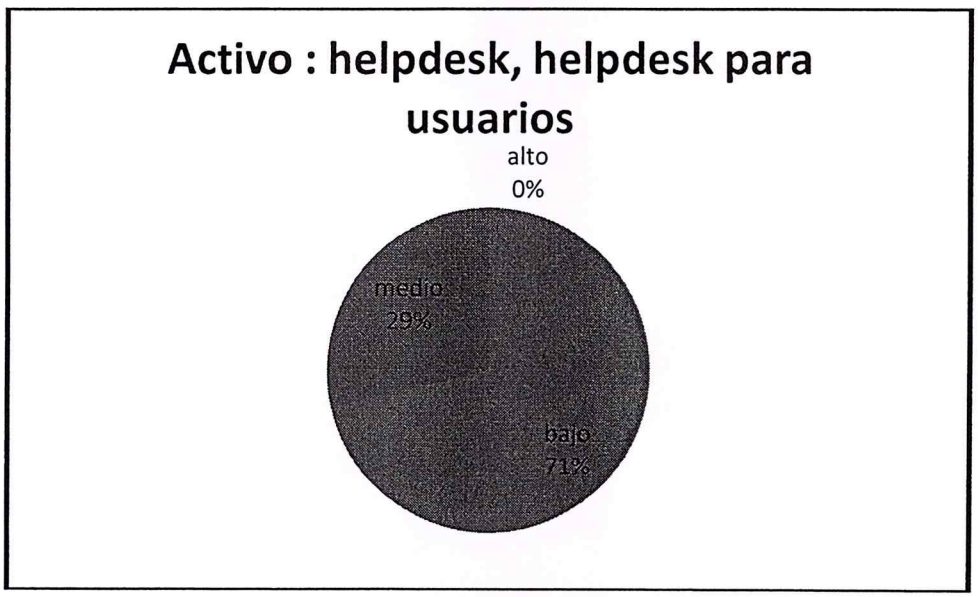
Vulnerabilidad	Nivel
1. Ausencia de personal	(0) No aplicable
2. Líneas de llamada	(0) No aplicable
3. Ausencia de copias de respaldo	(0) No aplicable
4. Interfaz de usuario excesivamente complicada	(1) Bajo
5. Eliminación o reutilización de medios de almacenamiento sin haberlos borrado adecuadamente	(1) Bajo



Activo : helpdesk

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
helpdesk para usuarios	Medios de soporte	helpdesk	sistemas	Xavier Mosquera	-

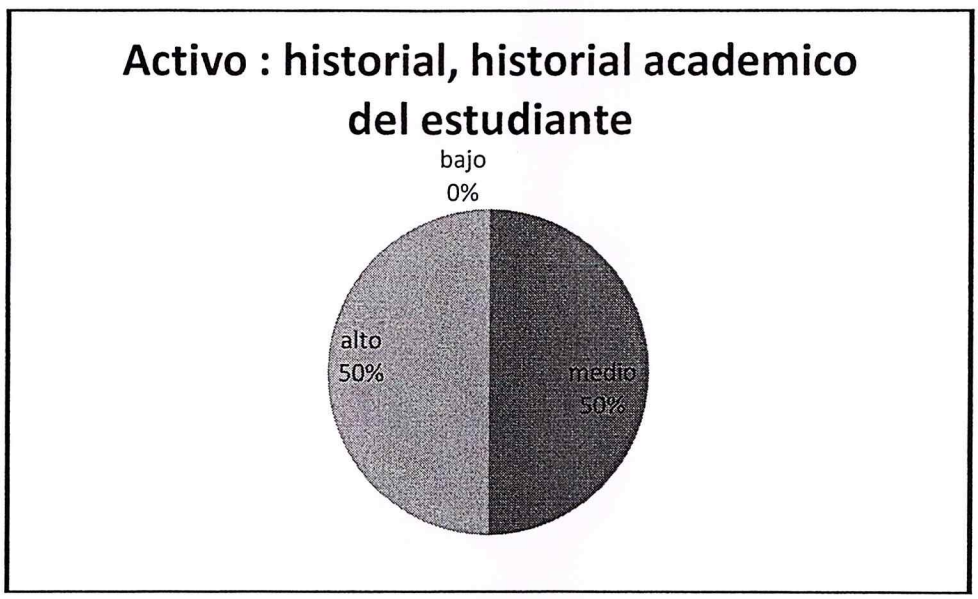
Vulnerabilidad	Nivel
1. Ausencia de políticas relativas al uso correcto de aplicable las infraestructuras de comunicaciones	(0) No
2. Ausencia de copias de respaldo	(1) Bajo
3. Falta de cuidado en la eliminación	(1) Bajo
4. Ausencia de mecanismos de identificación y autenticación	(1) Bajo
5. Ausencia de identificación y autenticación del emisor o receptor	(1) Bajo
6. Ausencia de registros y pruebas de envío y recepción de mensajes	(1) Bajo
7. Ausencia de concienciación en materia de seguridad	(1) Bajo
8. Gestión inadecuada de contraseñas	(1) Bajo
9. Sensibilidad a la radiación electromagnética	(1) Bajo
10. Transferencia de contraseñas en claro	(1) Bajo
11. Copias sin control	(1) Bajo
12. Formación en materia de seguridad insuficiente	(2) Medio
13. Mantenimiento inadecuado de los medios de almacenamiento	(2) Medio
14. Ausencia de pistas de auditoría	(2) Medio
15. Ausencia de mecanismos de monitorización	(2) Medio



Activo : historial

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
historial académico del estudiante	Datos	historial	Acade	Guido Coppiano	-

Vulnerabilidad	Nivel
1. Gestión inadecuada de la red	(0) No aplicable
2. Controles de acceso físico a las instalaciones inadecuados o inexistentes	(2) Medio
3. Ausencia de pistas de auditoría	(3) Alto



Activo : homologación

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
acta de homologaciones internas y externas	Datos	homologación	Acade	Guido Coppiano	-

Vulnerabilidad	Nivel
1. Gestión inadecuada de la red	(0) No aplicable
2. Controles de acceso físico a las instalaciones inadecuados o inexistentes	(2) Medio
3. Ausencia de pistas de auditoría	(3) Alto

Activo : inscripción

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
boleta de inscripción	Datos	inscripción	acade, siga	Decano	-

Vulnerabilidad	Nivel
1. Gestión inadecuada de la red	(0) No aplicable
2. Controles de acceso físico a las instalaciones inadecuados o inexistentes	(0) No aplicable
3. Ausencia de pistas de auditoría	(3) Alto

Activo : mallas

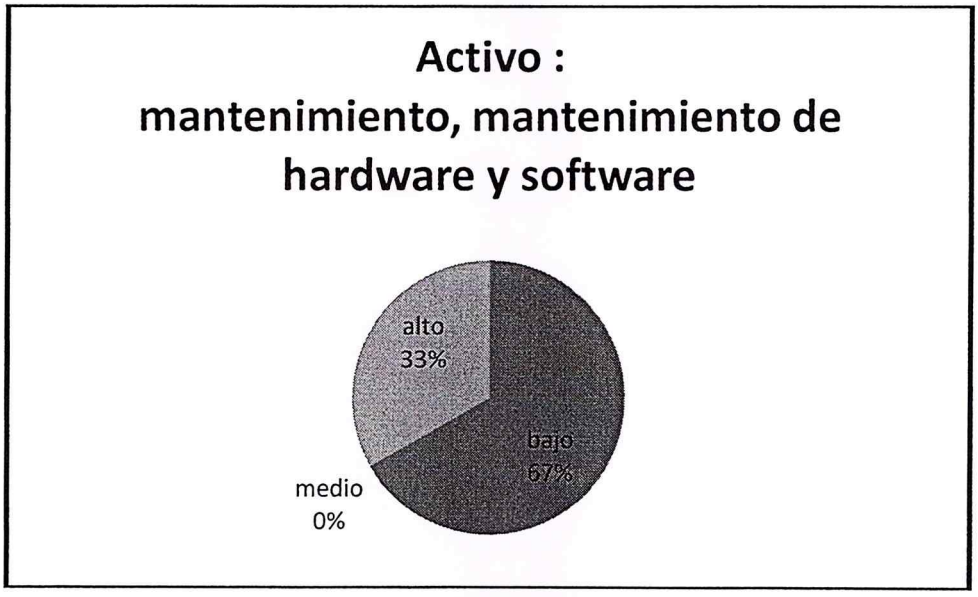
Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
mallas en sistema	Datos	mallas	acade	Guido Coppiano	-

Vulnerabilidad	Nivel
4. Gestión inadecuada de la red	(0) No aplicable
5. Controles de acceso físico a las instalaciones	(2) Medio
6. inadecuados o inexistentes	
7. Ausencia de pistas de auditoría	(2) Medio

Activo : mantenimiento

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
mantenimiento de hardware y software	Servicios	mantenimiento h&s	Sistemas	Xavier Mosquera	-

Vulnerabilidad	Nivel
1. Eliminación o reutilización de medios de almacenamiento sin haberlos borrado adecuadamente	(0) No aplicable
2. Ausencia de copias de respaldo	(0) No aplicable
3. Ausencia de personal	(1) Bajo
4. Interfaz de usuario excesivamente complicada	(1) Bajo
5. Líneas de llamada	(3) Alto



Activo : materias

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
rediseño de materias en formato presencial a formato "hibrido"	Servicios	materias on line		Xavier Mosquera	-

Vulnerabilidad	Nivel
1. Eliminación o reutilización de medios de	(0) No aplicable
2. almacenamiento sin haberlos borrado adecuadamente	
3. Ausencia de personal	(2) Medio
4. Interfaz de usuario excesivamente complicada	(2) Medio
5. Líneas de llamada	(2) Medio
6. Ausencia de copias de respaldo	(2) Medio

Activo : matricula

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
boleta de inscripción facturada en siga y dada de alta en acade	Datos	matricula	acade, siga	Decano	-

Vulnerabilidad	Nivel
1. Gestión inadecuada de la red	(0) No aplicable
2. Controles de acceso físico a las instalaciones inadecuados o inexistentes	(0) No aplicable
3. Ausencia de pistas de auditoría	(2) Medio

Activo : pc's

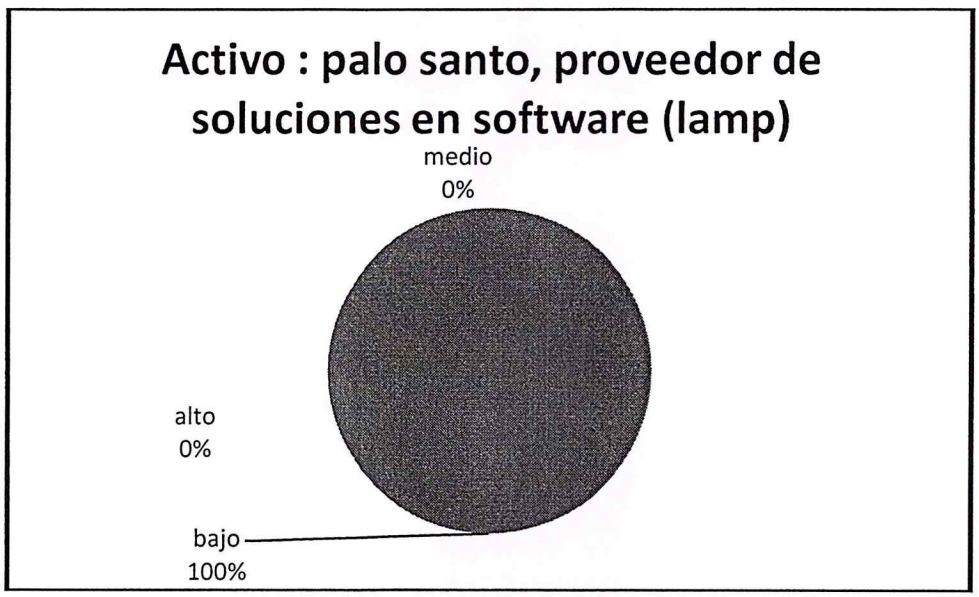
Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
pc's de uso individual de cada propietario	Tecnología	Pc			1000 $

Vulnerabilidad	Nivel
1. Procedimientos de contratación inadecuados	(0) No aplicable
2. Formación en materia de seguridad insuficiente	(0) No aplicable
3. Uso inadecuado del software o hardware	(1) Bajo

Activo : palo santo

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
proveedor de soluciones en software (lamp)	Recurso externo	palo santo	palo santo	Xavier Mosquera	-

Vulnerabilidad	Nivel
1. Ausencia de personal	(0) No aplicable
2. Procedimientos de contratación inadecuados	(0) No aplicable
3. Uso inadecuado del software o hardware	(1) Bajo
4. Formación en materia de seguridad insuficiente	(1) Bajo
5. Ausencia de concienciación en materia de seguridad	(1) Bajo
6. Trabajo de personal externo sin supervisar	(1) Bajo

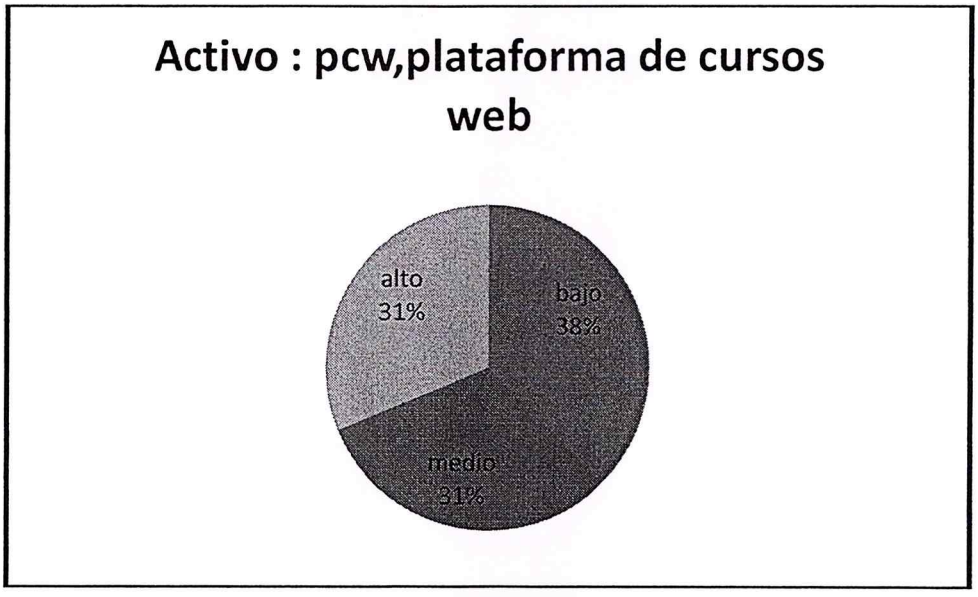


Activo : pcw

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
plataforma de cursos web	Aplicaciones	pcw	centro de computo, server Miami	Xavier Mosquera	4000 $

Vulnerabilidad	Nivel
1. Ausencia de personal	(1) Bajo
2. Eliminación o reutilización de medios de	(1) Bajo
3. almacenamiento sin haberlos borrado adecuadamente	
4. Controles de acceso físico a las instalaciones inadecuados o inexistentes	(1) Bajo
5. Servicio de mantenimiento inadecuado	(1) Bajo
6. Uso inadecuado del software o hardware	(1) Bajo
7. Falta de cuidado en la eliminación	(1) Bajo
8. Ausencia de protección física del edificio , puertas y ventanas	(1) Bajo
9. Ubicación en áreas susceptibles de inundarse	(1) Bajo
10. Conexiones de cables inadecuadas	(1) Bajo
11. Gestión inadecuada de contraseñas	(1) Bajo
12. Transferencia de contraseñas en claro	(1) Bajo
13. Especificaciones a los desarrolladores poco claras o incompletas	(1) Bajo
14. Copias sin control	(1) Bajo
15. Descarga y/o uso de software sin control	(1) Bajo
16. Líneas de comunicación sin protección	(1) Bajo
17. Tráfico de información sensible sin protección	(1) Bajo
18. Trabajo de personal externo sin supervisar	(1) Bajo
19. Asignación inadecuada de permisos de acceso	(1) Bajo
20. Interfaz de usuario excesivamente complicada	(2) Medio
21. Líneas de llamada	(2) Medio
22. Gestión inadecuada de la red	(2) Medio
23. Procedimientos de contratación inadecuados	(2) Medio
24. Mantenimiento inadecuado de los medios de almacenamiento	(2) Medio
25. Ausencia de copias de respaldo	(2) Medio
26. Ausencia de control de cambios	(2) Medio
27. Ausencia de control de cambios de la configuración	(2) Medio
28. Ausencia de procedimientos de sustitución periódica	(2) Medio
29. Ausencia de concienciación en materia de seguridad	(2) Medio
30. Pruebas del software insuficientes o inexistentes	(2) Medio
31. Un único punto de fallo	(2) Medio
32. Conexiones a redes públicas sin protección	(2) Medio
33. Almacenamiento sin protección	(2) Medio
34. Vulnerabilidades conocidas del software	(2) Medio
35. Temperaturas extremas	(3) Alto
36. Formación en materia de seguridad insuficiente	(3) Alto
37. Ausencia de pistas de auditoría	(3) Alto

38. Ausencia de documentación (3) Alto
39. Ausencia de mecanismos de identificación y autenticación (3) Alto
40. Ausencia de identificación y autenticación (3) Alto
41. del emisor o receptor
42. Ausencia de mecanismos de monitorización (3) Alto
43. Ausencia de políticas relativas al uso correcto de las infraestructuras de comunicaciones (3) Alto
44. Ausencia de registros y pruebas de envío y recepción de mensajes (3) Alto
45. No realizar "logout" al dejar el puesto de trabajo (3) Alto
46. Sensibilidad a la radiación electromagnética (3) Alto
47. Sensibilidad a la humedad, polvo, etc. (3) Alto
48. Sensibilidad a las variaciones de temperaturas (3) Alto
49. Sensibilidad a las variaciones de voltaje (3) Alto
50. Tablas de contraseñas sin protección (3) Alto



Activo : safi

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
sistema de gestión administrativa-contable-financiera	Aplicaciones	siga	centro de computo	Cristobal Naranjo	3000 $

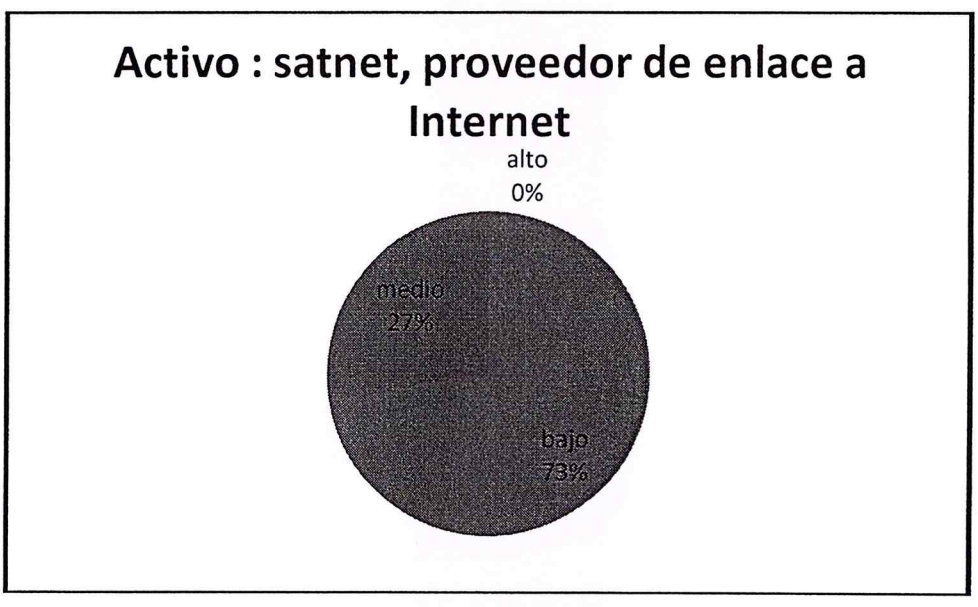
	Vulnerabilidad	Nivel
1.	Ausencia de personal	(1) Bajo
2.	Interfaz de usuario excesivamente complicada	(1) Bajo
3.	Líneas de llamada	(1) Bajo
4.	Eliminación o reutilización de medios de almacenamiento sin haberlos borrado adecuadamente	(1) Bajo
5.	Gestión inadecuada de la red	(1) Bajo
6.	Controles de acceso físico a las instalaciones inadecuados o inexistentes	(1) Bajo
7.	Procedimientos de contratación inadecuados	(1) Bajo
8.	Servicio de mantenimiento inadecuado	(1) Bajo
9.	Ausencia de copias de respaldo	(1) Bajo
10.	Falta de cuidado en la eliminación	(1) Bajo
11.	Ausencia de protección física del edificio , puertas y ventanas	(1) Bajo
12.	Ubicación en áreas susceptibles de inundarse	(1) Bajo
13.	Pruebas del software insuficientes o inexistentes	(1) Bajo
14.	Gestión inadecuada de contraseñas	(1) Bajo
15.	Transferencia de contraseñas en claro	(1) Bajo
16.	Especificaciones a los desarrolladores poco claras o incompletas	(1) Bajo
17.	Copias sin control	(1) Bajo
18.	Descarga y/o uso de software sin control	(1) Bajo
19.	Líneas de comunicación sin protección	(1) Bajo
20.	Tablas de contraseñas sin protección	(1) Bajo
21.	Tráfico de información sensible sin protección	(1) Bajo
22.	Trabajo de personal externo sin supervisar	(1) Bajo
23.	Asignación inadecuada de permisos de acceso	(1) Bajo
24.	Uso inadecuado del software o hardware	(2) Medio
25.	Formación en materia de seguridad insuficiente	(2) Medio
26.	Mantenimiento inadecuado de los medios de almacenamiento	(2) Medio
27.	Ausencia de documentación	(2) Medio
28.	Ausencia de control de cambios	(2) Medio
29.	Ausencia de control de cambios de la configuración	(2) Medio
30.	Ausencia de mecanismos de identificación y autenticación	(2) Medio
31.	Ausencia de identificación y autenticación del emisor o receptor	(2) Medio
32.	Ausencia de procedimientos de sustitución periódica	(2) Medio

33. Ausencia de políticas relativas al uso correcto de las infraestructuras de comunicaciones	(2) Medio
34. Ausencia de registros y pruebas de envío y recepción de mensajes	(2) Medio
35. Ausencia de concienciación en materia de	(2) Medio
36. seguridad	
37. Conexiones de cables inadecuadas	(2) Medio
38. Conexiones a redes públicas sin protección	(2) Medio
39. Almacenamiento sin protección	(2) Medio
40. Vulnerabilidades conocidas del software	(2) Medio
41. Temperaturas extremas	(3) Alto
42. Ausencia de pistas de auditoría	(3) Alto
43. Ausencia de mecanismos de monitorización	(3) Alto
44. No realizar "logout" al dejar el puesto de trabajo	(3) Alto
45. Sensibilidad a la radiación electromagnética	(3) Alto
46. Un único punto de fallo	(3) Alto
47. Sensibilidad a la humedad, polvo, etc.	(3) Alto
48. Sensibilidad a las variaciones de temperaturas	(3) Alto
49. Sensibilidad a las variaciones de voltaje	(3) Alto

Activo : satnet

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
proveedor de enlace a Internet	Telecomunicaciones	satnet	sistemas	Xavier Mosquera	-

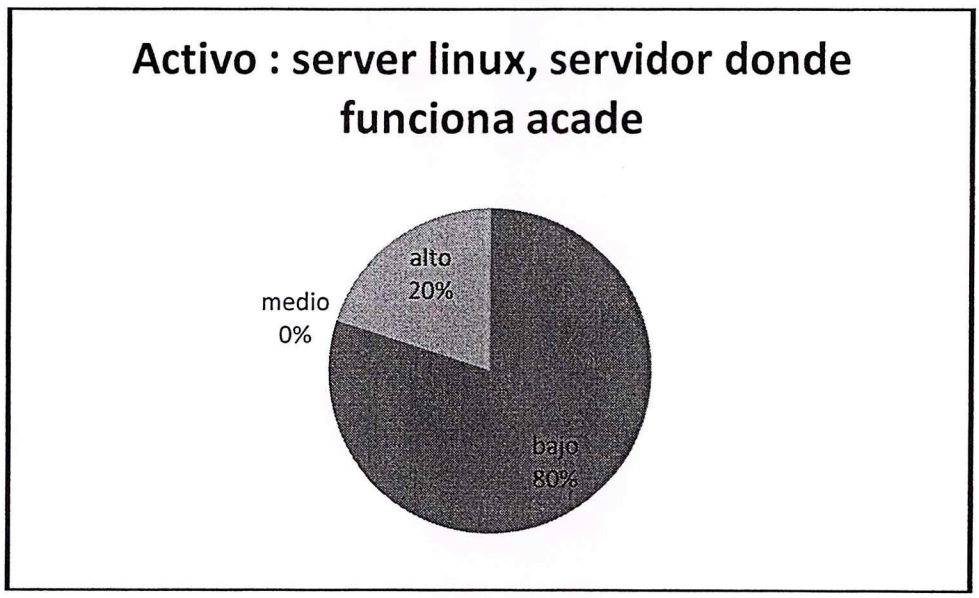
	Vulnerabilidad	Nivel
1.	Temperaturas extremas	(0) No aplicable
2.	Servicio de mantenimiento inadecuado	(0) No aplicable
3.	Ausencia de protección física del edificio, puertas y ventanas	(0) No aplicable
4.	Sensibilidad a la radiación electromagnética	(0) No aplicable
5.	Sensibilidad a la humedad, polvo, etc.	(0) No aplicable
6.	Sensibilidad a las variaciones de temperaturas	(0) No aplicable
7.	Sensibilidad a las variaciones de voltaje	(0) No aplicable
8.	Gestión inadecuada de la red	(1) Bajo
9.	Controles de acceso físico a las instalaciones inadecuados o inexistentes	(1) Bajo
10.	Formación en materia de seguridad insuficiente	(1) Bajo
11.	Ausencia de políticas relativas al uso correcto de las infraestructuras de comunicaciones	(1) Bajo
12.	Conexiones de cables inadecuadas	(1) Bajo
13.	Gestión inadecuada de contraseñas	(1) Bajo
14.	Conexiones a redes públicas sin protección	(1) Bajo
15.	Asignación inadecuada de permisos de acceso	(1) Bajo
16.	Líneas de llamada	(2) Medio
17.	Ausencia de mecanismos de monitorización	(2) Medio
18.	Ausencia de concienciación en materia de seguridad	(2) Medio



Activo : server linux

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
servidor donde funciona acade	Tecnología	server linux		Xavier Mosquera	3000 $

	Vulnerabilidad	Nivel
1.	Formación en materia de seguridad insuficiente	(0) No aplicable
2.	Procedimientos de contratación inadecuados	(1) Bajo
3.	Servicio de mantenimiento inadecuado	(1) Bajo
4.	Uso inadecuado del software o hardware	(1) Bajo
5.	Mantenimiento inadecuado de los medios de almacenamiento	(1) Bajo
6.	Ausencia de pistas de auditoría	(3) Alto



Activo : server safi

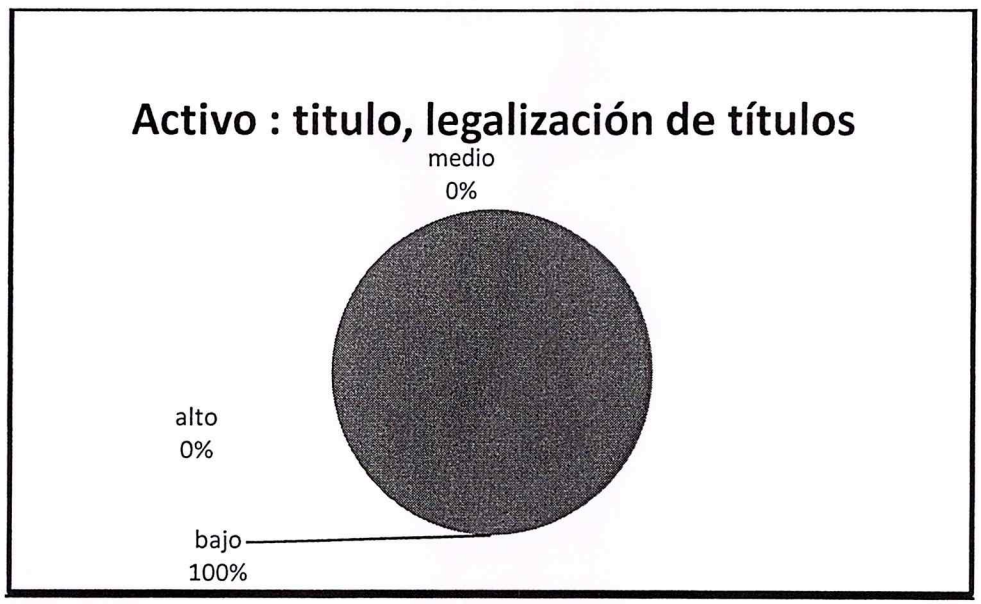
Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
servidor donde funciona safi	Tecnología	alter	centro de computo	Xavier Mosquera	35000 $

	Vulnerabilidad	Nivel
1.	Procedimientos de contratación inadecuados	(1) Bajo
2.	Servicio de mantenimiento inadecuado	(1) Bajo
3.	Uso inadecuado del software o hardware	(1) Bajo
4.	Formación en materia de seguridad insuficiente	(2) Medio
5.	Mantenimiento inadecuado de los medios	(2) Medio
6.	de almacenamiento	
7.	Ausencia de pistas de auditoría	(3) Alto

Activo : titulo

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
legalización de títulos	Datos	titulo	acade, siga	Guido Coppiano	-

Vulnerabilidad	Nivel
1. Gestión inadecuada de la red	(0) No aplicable
2. Controles de acceso físico a las instalaciones inadecuados o inexistentes	(0) No aplicable
3. Ausencia de pistas de auditoría	(1) Bajo



Activo : titulo

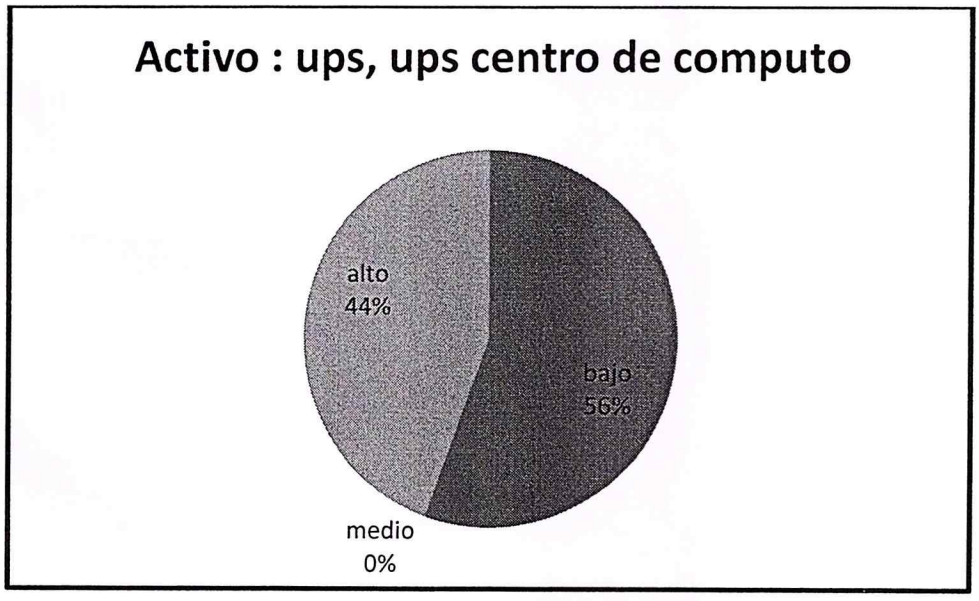
Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
titulo de carrera	Documento en papel	titulo	Secretaria académica	Guido Coppiano	-

	Vulnerabilidad	Nivel
1.	Formación en materia de seguridad insuficiente	(0) No aplicable
2.	Trabajo de personal externo sin supervisar	(0) No aplicable
3.	Temperaturas extremas	(1) Bajo
4.	Controles de acceso físico a las instalaciones inadecuados o inexistentes	(1) Bajo
5.	Ausencia de documentación	(1) Bajo
6.	Ausencia de protección física del edificio, puertas y ventanas	(1) Bajo
7.	Ausencia de concienciación en materia de seguridad	(1) Bajo
8.	Sensibilidad a la humedad, polvo, etc.	(1) Bajo
9.	Sensibilidad a las variaciones de temperaturas	(1) Bajo
10.	Almacenamiento sin protección	(1) Bajo
11.	Ubicación en áreas susceptibles de inundarse	(3) Alto

Activo : ups

Descripción	Categoría	Identificador	Ubicación	Propietario	Valor
ups centro de computo	Equipo de protección informático	ups	centro de computo	Xavier Mosquera	500 $

	Vulnerabilidad	Nivel
1.	Controles de acceso físico a las instalaciones inadecuados o inexistentes	(1) Bajo
2.	Ausencia de procedimientos de sustitución periódica	(1) Bajo
3.	Ausencia de concienciación en materia de seguridad	(1) Bajo
4.	Ubicación en áreas susceptibles de inundarse	(1) Bajo
5.	Trabajo de personal externo sin supervisar	(1) Bajo
6.	Temperaturas extremas	(3) Alto
7.	Sensibilidad a la humedad, polvo, etc.	(3) Alto
8.	Sensibilidad a las variaciones de temperaturas	(3) Alto
9.	Sensibilidad a las variaciones de voltaje	(3) Alto



3. CONCLUSIONES

1.- Política de Seguridad

i) Se debe contar con un documento de políticas de seguridad de la información el cual cubra el alcance definido por el SGSI.

ii) Deben contar con una estructura de cálculo de riesgo claramente definida, así como también con una clara definición y tratamiento del riesgo.

iii) Debe existir una precisa identificación del riesgo, con el fin de mitigarlo a términos aceptables.

iv) Debe existir un proceso establecido para preparar una declaración de aplicabilidad (SOA).

v) Establecer un proceso de diseño de SGSI, con su definición, alcance y metodología de revisión periódica del mismo.

vi) Establecer procedimientos de monitorización de controles, con el fin de detectar errores, identificar violaciones en la seguridad y ejecutar actividades delegadas o implementadas por la tecnología para preservar la continuidad del negocio.

vii) Realizar auditorias internas del SGSI a intervalos debidamente planificados.

2.- Organización de la Seguridad

i) Coordinar las actividades de la seguridad de la información con los representantes de cada una de los directivos de las diferentes áreas (identificadas en el SGSI) de la organización.

ii) Definir de manera clara y concisa las respectivas responsabilidades de la seguridad de la información en la organización (principalmente en términos de dueños de datos, impacto en el SGSI y activos de información).

iii) Institucionalmente ejecutar el Plan de Gestión del tratamiento de la información (SGSI).

iv) Establecer métricas de confidencialidad y no-divulgación en función de las necesidades reales de protección (activos) de la información de la organización y proceder a una revisión periódica de la misma.

v) Establecer una debida asignación de responsabilidades para la seguridad de la información (asociada a la estructura del SGSI).

vi) Mantener un contacto apropiado con grupos de interés en la seguridad o asociaciones de este tipo, básicamente para efectos de actualización y replica de mejores practicas en organizaciones similares.

vii) Mejorar el conocimiento de las mejores prácticas de la seguridad de la información, es decir, un completo entrenamiento y capacitación a todo el personal (asociado a un plan de carrera profesional y sobre todo a los objetivos plasmados en el Plan Estratégico de la organización).

viii) Establecer una revisión independiente y periódica del SGSI

ix) Establecer una identificación y tratamiento de todos los requisitos de la seguridad de la información, antes de darle acceso a los clientes (internos-externos) de la misma.

3.- Gestión de Activos

i) Identificar todos los activos, sus responsables, así como también elaborar y mantener un inventario de los más importantes.

ii) Debe clasificarse la información en base a su valor, su criticidad, sensibilidad y requerimientos legales vigentes.

4.- Seguridad del Personal

i) Debe definirse y documentar los roles y responsabilidades de acuerdo con las políticas de seguridad de la información de la organización.

ii) Verificación de antecedentes de todos los candidatos previo al empleo.

iii) El personal a contratar deben aceptar y firmar un contrato con los términos y condiciones de su empleo.

iv) Definir claramente la responsabilidad de la gerencia con respecto al cumplimiento de las normas de seguridad a cumplir por el personal.

v) Proceso disciplinario para los usuarios que incumplan la seguridad.

vi) Devolución de los activos que tengan en su posesión el personal al momento de la terminación del contrato laboral.

vii) Retiro de los derechos de acceso al momento del término del contrato laboral.

5.- Seguridad Física y del Entorno

i. Diseñar y aplicar un sistema de protección física contra daños causados por incendios, inundaciones, terremotos, explosiones, ataques provocados por personas y/o otras formas de desastre natural o artificial.

ii. Diseñar e implantar un sistema de seguridad física para las oficinas, salas y resto de instalaciones.

iii. Proteger el equipamiento informático ante los posibles fallos de alimentación eléctrica y otras perturbaciones causadas por los fallos en las utilidades de soporte.

iv. Aplicar la seguridad adecuada al respaldo off-site (fuera de las áreas pertenecientes a la organización), considerando los riesgos implicados al encontrarse fuera de las premisas de la organización.

6.- Gestión de Comunicaciones y Operaciones

i. Deben estar documentados los procedimientos operativos, mantenidos y puestos a disposición de todos los usuarios que los necesiten.

ii. Establecer los deberes y áreas de responsabilidad para reducir las oportunidades de modificación, uso erróneo, no autorizado, modificaciones no intencionadas o uso indebido, de los activos de la organización.

iii. Separar las instalaciones de desarrollo, producción y pruebas para reducir los riesgos de accesos o cambios en los sistemas operativos no autorizados.

iv. Se deben monitorizar y revisar de forma regular los servicios, informes y registros proporcionados por terceras partes, y se deben llevar a cabo auditorias de forma regular y planificada.

v. Monitorizar y afinar el uso de recursos y realizar proyecciones de futuros requisitos de capacidad para asegurar el rendimiento del sistema.

vi. Implementar controles de detección, recuperación y prevención, así como procedimientos de alerta a los usuarios que les proteja contra código malicioso.

vii. Desarrollar simulacros con las copias de seguridad respectivas (back-ups).

viii. Identificar las características de seguridad, los niveles de servicio, y los requerimientos de gestión de todos los servicios de red, incluidos en los pactos con los diferentes proveedores de servicios de red, bien sean internos o externos.

ix. Establecer procedimientos en la gestión y el almacenamiento de la información, de forma que se proteja de la divulgación no autorizada o de un uso inapropiado.

x. Proteger la documentación del sistema contra accesos no autorizados.

xi. Establecer acuerdos para el intercambio de información y software entre la organización y otras externas.

xii. Proteger debidamente la información soportada por la mensajería electrónica de actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizada.

xiii. Grabados los registros de auditoria, las actividades de los usuarios, las excepciones, los eventos de seguridad de la información durante un periodo de tiempo acordado para poder usarlo en investigaciones futuras y monitorizar el control de acceso.

xiv. Registrar la actividades del administrador(es) y del operador(es) del sistema.

7.- Control de Acceso

i. Establecer y documentar una política de control de accesos que sea revisada basándose en los requisitos de seguridad y del negocio.

ii. Se debe restringir y controlar la asignación de privilegios; así como las contraseñas deben realizarse conforme a un proceso formal de gestión.

iii. Los derechos de acceso de los usuarios deben revisarse a intervalos regulares.

iv. Deben usarse métodos de autentificación adecuados para controlar el acceso remoto de usuarios.

v. Deben controlarse física y lógicamente los accesos a los puertos de diagnostico y configuración.

vi. El acceso a los sistemas operativos, debe ser controlado por un procedimiento de acceso seguro.

vii. Deben tener todos los usuarios un identificador único para su uso personal y seleccionarse una técnica de autentificación adecuada para exigir la identidad del usuario.

viii. Establecer una política formal que proteja contra el riesgo del uso de la informática móvil y de todas las facilidades de las comunicaciones.

8.- Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

i) Deben implantarse procedimientos de control adecuados a la instalación de software sobre sistemas operacionales.

ii) Debe obtenerse regularmente información respecto a las vulnerabilidades técnicas de los sistemas de información que están en uso.

iii) Se deben evaluar las amenazas a dichas vulnerabilidades y tomarse las medidas oportunas para gestionar el riesgo asociado.

9.- Gestión de Incidentes de Seguridad de la Información

I. La UTEG posterior a un plan de mitigación de riesgo (a partir de un inventario de activos y vulnerabilidades) deberá desarrollar su definición de Incidente de Seguridad y posteriormente sus respectivas contramedidas.

10.- Gestión de Continuidad del Negocio

i. Se debe desarrollar un proceso para dotar de continuidad al negocio que tiene en cuenta los requerimientos de seguridad necesarios para el mismo, y mantenerlo adecuadamente.

ii. Deben desarrollarse e implantarse planes para mantener o recuperar las operaciones de forma que se asegure la disponibilidad de la información al nivel de los tiempos de recuperación requeridos ante una interrupción o fallo de los procesos críticos del negocio.

iii. Mantener un solo marco de planes de continuidad del negocio que asegure que todos los planes son consistentes, que aseguren el cumplimiento de los requerimientos de seguridad de la información e identifiquen las prioridades para probarlos y mantenerlos.

11.- Cumplimiento

i. Deben ser definidos, actualizados y guardados todos los requerimientos necesarios para cada sistema de información de los tipos: legales, contractuales, regulatorios y estatutarios.

ii. Verificar los sistemas de información en el cumplimiento de la implementación de estándares de seguridad.

3.1 Política General de la Seguridad de la Información en la Organización

Para preservar la confidencialidad, disponibilidad e integridad, es decir, la salvaguarda de los activos de información de la organización en términos generales, será imprescindible el compromiso y apoyo manifiesto por parte de los directivos, implementando una política general de seguridad de la información, basada en una distribución de guías sobre políticas y estándares de seguridad dirigida a todo el personal, desde operadores hasta la alta gerencia, como también una capacitación y entrenamientos adecuados, estableciendo así una comunicación eficaz de los temas de seguridad, mejorando el conocimiento y concienciación, a fin de lograr un completo y claro entendimiento de seguridad, evaluación y tratamiento del riesgo; y en la manera de cómo estos podrían afectar o impactar las actividades comerciales, operativas y legales de la empresa.

4.Bibliografía

Norma Técnica ISO 17799:2005