ESCUELA POLITECNICA DEL EJÉRCITO

DPTO. DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMATICA

"EVALUACIÓN TÉCNICA DE LA SEGURIDAD INFORMÁTICA DEL DATA CENTER DE LA ESCUELA POLITÉCNICA DEL EJÉRCITO"

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS E INFORMÁTICA

POR:

RICARDO NAPOLEÓN GUAGALANGO VEGA

PATRICIO ESTEBAN MOSCOSO MONTALVO

SANGOLQUÍ, AGOSTO de 2011

CERTIFICACION

Certifico que el presente trabajo fue realizado en su totalidad por los Srs. Patricio Esteban Moscoso Montalvo y Ricardo Napoleón Guagalango Vega como requerimiento parcial a la obtención del título de INGENIEROS EN SISTEMAS

Julio del 2011

_____

Ing. Walter Fuertes D.,PhD.

DEDICATORIA

Este trabajo está dedicado especialmente a mis padres Rosita Vega y Luis Guagalango, a mis hermanas Marilyn y Patricia Guagalango y a mi abuelita Herminia Vega, ya que gracias su esfuerzo y sacrificio diario me ayudaron a nunca rendirme en los momentos difíciles, puesto que con todo su amor y cariño supieron darme fuerzas para mantenerme constante en conseguir mis metas. Fueron mi principal fuente de inspiración en mi vida profesional y personal e inculcarme todos los valores desde mi infancia para ser una persona de bien, por depositar en mi toda su confianza y apoyo, por aconsejarme diariamente para de esta manera disfrutar de esta nueva etapa en mi vida.

RICARDO NAPOLEON GUAGALANGO VEGA

DEDICATORIA

Dedico este trabajo primeramente a Dios que me acompaña siempre, cuida mis pasos, y es la razón de mi ser. A mis padres Alfonsito y Marcita, quienes me apoyaron en todo momento con su esfuerzo y cariño en todas las etapas de mi vida, inculcándome los valores cristianos que llevo siempre en mi formación personal y profesional. Para toda mi linda familia y amigos que estuvieron muy pendientes de este logro, animándome para alcanzar mis metas y objetivos.

PATRICIO ESTEBAN MOSCOSO MONTALVO

AGRADECIMIENTO

En primer lugar agradezco a Dios que es quien me ha dado lo más importante que es la vida y me ha sabido dar aliento en los peores momentos.

Agradezco a mis padres ROSITA VEGA Y LUIS GUAGALANGO, a mis hermanas MARILYN Y PATRICIA GUAGALANGO y a mi abuelita HERMINIA VEGA, ya que ellos fueron quienes me apoyaron moralmente, económicamente, y sobre todo me brindaron todo su amor.

A mis hermanos y familiares que me supieron dar consejos muy valiosos en los momentos más difíciles, lo cual me sirvió para salir adelante.
A mi amigo y colaborador de este trabajo PATRICIO MOSCOSO, por quien pongo las manos al fuego ya que es una persona súper comprometida con su trabajo.

Al Ingeniero WALTER FUERTES, al Ingeniero ROMEL ALDÁS y al Ingeniero SANTIAGO SALVADOR, quienes con su apoyo supieron guiarnos para la culminación de este trabajo.

A la universidad donde fui formado y a mis maestros que fueron más que docentes, por impartir el conocimiento durante todo el tiempo que duro mi carrera
A todas las personas que son parte de este éxito.

RICARDO NAPOLEON GUAGALANGO VEGA

AGRADECIMIENTO

Doy gracias a Dios por su misericordia, que me ha permitido culminar mis estudios universitarios, por la salud, la vida y la hermosa familia que me ha dado. A mis padres ALFONSITO y MARCITA que son un regalo de Dios para mi, quienes han estado conmigo en los momentos más difíciles y sin su apoyo no podría haber logrado este importante objetivo.

A mi hermana MARCIA SOLEDAD que me apoyo siempre en oración y es un ejemplo de vida. A mis hermanos CARLOS M. e IVAN M. a quienes los quiero mucho.

A mi compañero de Tesis RICARDO GUAGALANGO que ha demostrado ser, esforzado, colaborador durante el desarrollo de toda la Tesis, y desde siempre un gran profesional.

A mis amigos que me acompañaron y motivaron durante mi Carrera en la Universidad en especial a CRISTINA H, JUAN CARLOS M y LORENA J.

A los profesores que me guiaron e impartieron sus enseñanzas para desempeñar los trabajos con responsabilidad, conocimiento y valores éticos.

A nuestros Directores de Tesis, y docentes que permitieron el inicio y finalización de este Proyecto.

A todos ellos que Dios les bendiga grandemente.

PATRICIO ESTEBAN MOSCOSO MONTALVO

Tabla de Contenidos

Capítulo V

Conclusiones y Recomendaciones

LISTADO DE TABLAS

LISTADO DE FIGURAS

LISTADO DE ANEXOS

RESUMEN

Con el desarrollo acelerado del Internet, hoy en día existen amenazas y vulnerabilidades que atentan contra la seguridad informática de las universidades, entre ellas el Data Center de la Escuela Politécnica del Ejército.

El presente proyecto se enfoca en el uso de los controles de la Norma ISO 27000, dedicada a especificar requerimientos necesarios para: establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.

En este contexto, existe una metodología formal de Análisis y Gestión de Riesgos denominada MAGERIT, que permite recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos. Para llevarlo a cabo es necesario complementar con un software denominado PILAR, que permite el análisis de riesgos en Seguridad Informática, de acuerdo a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad y disponga de salvaguardas, normas y procedimientos de seguridad para obtener el riesgo residual en el proceso de tratamiento. Los resultados obtenidos muestran una mejora a nivel de seguridad informática aplicando las salvaguardas, y se reduce el riesgo de la situación actual.

Los resultados han permitido técnicamente obtener un informe ejecutivo, definir los lineamientos para el plan de seguridad informático, cara a certificarse en la Norma ISO 27001.

CAPITULO I

INTRODUCCIÓN

1.1. Generalidades

Las técnicas de evaluación permiten revisar controles y procedimientos Informáticos para los Sistemas de Información en las organizaciones y determinar falencias actuales y sugerir soluciones amparadas en los estándares ISO 27001 e ISO 27002 en el área de Seguridad Informática.

La investigación de campo permitirá más adelante establecer las recomendaciones respectivas que podrán ser implantadas en controles como: accesos para los equipos informáticos (usuarios y claves), uso de software malicioso (virus, spyware, troyanos), uso del correo electrónico, y la información que tienen las bases de datos en los servidores que pueda ser modificada por terceros.

Las normas ISO 27001 e ISO 27002**;** se cimenta en pilares como: Integridad, confidencialidad y disponibilidad de la información.

Esta norma también propone métodos de control para lograr su objetivo, reconociendo que la Institución tiene su forma particular en el manejo de sus datos, programas etc.

Dada la importancia de un diagnóstico previo para la aplicación de recomendaciones basadas en la norma, se propone el siguiente perfil para el desarrollo de una Tesis de Grado.

1.2. Antecedentes

La Escuela Politécnica del Ejército (ESPE) es un organismo de Derecho Público, cuya finalidad esencial es formar profesionales e investigadores de excelencia y líderes en la gestión del conocimiento y de la tecnología en el Sistema Nacional de Educación Superior, sus sistemas y centros de información necesariamente deben reflejar veracidad y eficiencia en sus resultados, por lo que, sus sistemas y centros informáticos al someterse a una

evaluación técnica objetiva, reflejarían las fortalezas y debilidades en los procesos que estos conllevan, para medir su eficacia, logrando así asegurar la continuidad del servicio, identificar debilidades y contrarrestarlas.

Es de nuestro conocimiento que La ESPE recibe cada año a cientos estudiantes que ingresan a las diferentes carreras, y que para mantener políticas y controles de acceso a la información, es necesario establecer las condiciones adecuadas para elaborar en el futuro un Plan de Seguridades Informático. Por tanto se deberá realizar una Evaluación Técnica de la Seguridad Informática y mediante ese resultado obtener las Recomendaciones que servirían a la Institución, pues la ESPE no está libre de tener riesgos y amenazas para su información, por el gran crecimiento de hackers, y programas maliciosos como (malware, virus, troyanos, etc), que afectan a los datos en la Unidad de Sistemas de Información del Data Center.

Cabe señalar que: la veracidad, integridad, y actualidad de la Información, en el procesamiento de datos, son importantes para la ESPE y especialmente para la unidad de sistemas de información del Data Center.

Es de prioridad para el Data Center de la Institución, el proteger la información mediante políticas y controles de Seguridad Informática, de las amenazas constantes que afectan a los sistemas en todo el mundo por los problemas mencionados anteriormente.

1.3. Justificación

La ESPE se beneficiaría de este Proyecto, que será elaborado en el desarrollo del Proyecto de Grado, porque en los resultados se encontrarían las debilidades en el sistema informático, y mediante las Recomendaciones basadas en los estándares ISO 27001 e ISO 27002, se podría hacer rectificaciones posteriores en las políticas de seguridad así como en los controles existentes que sean críticos y ocasionen problemas en sus Sistemas.

Es necesario realizar la Evaluación o Diagnóstico de la Seguridad Informática

en el Data Center, porque aparte de verificar las falencias, se podrían aplicar controles y políticas en base a las recomendaciones obtenidas para minimizar en el futuro que ocurran estos problemas, y como una forma de prevención para el tratamiento adecuado de Datos y el cuidado de la información.

1.4. Objetivos

1.4.1. Objetivo General

Realizar una Evaluación Técnica Informática en la Unidad de Sistemas de Información del Data Center de la Escuela Politécnica del Ejército en Sangolquí, considerando como referencia los estándares ISO 27001 e ISO 27002.

1.4.2. Objetivos Específicos

- Realizar el marco teórico partiendo de conceptos principales de Auditoria y Seguridad Informática en los estándares ISO 27001, 27002.
- Elaborar la matriz de riesgo informático de las seguridades del Data Center.
- Elaborar el plan de investigación de campo.
- Elaborar y aplicar los instrumentos de investigación de campo.
- Procesar los datos obtenidos en la investigación.
- Realizar un análisis confrontativo con las normas ISO 27001 y 27002.
- Elaborar los informes ejecutivo y detallado.

1.5. Alcance

Este trabajo cubre las seguridades de las instalaciones en la Unidad de Sistemas de Información del Data Center de la ESPE, sede Sangolquí, contempla las normas internacionales ISO 27001 y 27002, no contempla el Plan de Seguridad Informática.

El diagnostico, evaluación y diseño de recomendaciones comprende los siguientes aspectos:

- Política de seguridad
- Aspectos organizativos de la seguridad de la información
- Gestión de activos
- Seguridad ligada a los recursos humanos
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Gestión de incidentes de seguridad en la seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento

Los resultados de este proyecto, servirán para que los usuarios de la Unidad de Sistemas de Información del Data Center de la ESCUELA POLITECNICA DEL EJÉRCITO, se encuentre en capacidad de aplicar medidas en lo que a seguridad se refiere para que la información se mantenga disponible y sea confiable y oportuna.

CAPITULO II

FUNDAMENTACION TEORICA

2.1. Conceptos Principales de Auditoria y Seguridad Informática

Auditoria Informática, es el proceso realizado por expertos, que consiste en recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo de la empresa.

Auditar consiste en estudiar los mecanismos de control que están implantados en una empresa u organización determinando si los mismos son adecuados y cumplen objetivos y estrategias.

Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

Seguridad Informática, es el área de la informática que tiene como objetivo proteger la infraestructura computacional incluyendo la información contenida.

Actualmente existen estándares, protocolos, métodos, reglas y leyes que permiten minimizar riesgos a la infraestructura o a la información. La Seguridad informática abarca software, bases de datos, metadatos, archivos y todo lo que la organización valore como activo y signifique un riesgo; es decir en cuanto al tipo de información que se conoce como privilegiada o confidencial.

Seguridad de la Información: Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistema tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad y Integridad de la misma.[1]

[1] **Fuente:** Libro Informática; Glosario de Términos y Siglas, Antonio Baquero, Luis Joyanes, Mc.Grow Hill

Activo: Cualquier cosa que tenga valor para la organización.[2]

Amenaza: Una amenaza es cualquier cosa que puede suceder y que, cuando ocurre, tiene consecuencias negativas sobre el valor de nuestros activos.

Impacto: Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza.

Riesgo: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

Riesgo Residual: Riesgo remante que existe después de que se hayan tomado las medidas de seguridad.

Salvaguarda: Protección referente a las amenazas para los activos.

Análisis de riesgos: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.

Gestión de riesgos: Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.[3]

Disponibilidad: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Integridad: La propiedad de salvaguardar la exactitud e integridad de los activos.[4]

Confidencialidad: La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados. [5]

Autenticidad: Comprobación de que la fuente de datos recibidos es la alegada.

Trazabilidad: Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. [6]

---

[2] **Fuente:** Norma ISO/IEC 13335-1:2004

[3] **Fuente:** Libro de MAGERIT 2 (Método) – Ministerio de Administraciones Publicas de España

[4] **Fuente:** Biblioteca PILAR

[5] **Fuente:** Norma ISO/IEC 13335-1:2004

Seguridad de Información: Preservación de la confidencialidad, integridad y disponibilidad de la información; además también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad. [7]

Evento de seguridad de la Información: Una ocurrencia identificada del estado de un sistema, servicio o red indicando una posible violación de la política de seguridad de la información o falla en las salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad.[8]

Incidente de Seguridad de la Información: Un solo o una sola serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer las operaciones comerciales y amenazan la seguridad de la información. [9]

2.2 Análisis y Gestión de Riesgos

Los activos están expuestos a amenazas que pueden degradar al activo, produciendo un impacto. Por ende es necesario deducir el riesgo al que está expuesto el sistema.

Entonces se dispone de salvaguardas, que o bien reducen la frecuencia de ocurrencia, o bien reducen o limitan el impacto. Dependiendo del grado de implantación de estas salvaguardas, el sistema pasa a una nueva estimación de riesgo que se denomina riesgo residual.

---

[6] **Fuente:** biblioteca PILAR
[7] **Fuente:** Norma ISO/IEC 17799-1:2005

[8] **Fuente:** Norma ISO/IEC 13335-1:2004

[9] **Fuente:** Norma ISO/IEC TR 18044:2004

Para el análisis y la gestión de riesgos del Data Center al área de sistema de información utilizaremos la metodología MAGERIT versión 2.[10]

Sistema de Gestión de Seguridad de la Información SGSI: Esa parte del sistema gerencial general, basada en un enfoque de riesgo comercial; para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Nota: el sistema gerencial incluye la estructura organizacional, políticas, actividades de planeación, responsabilidades, prácticas, procedimientos, procesos y recursos.

Impacto acumulado: Los activos dependen unos de otros, mientras que la materialización de las amenazas en los activos inferiores causa un daño directo sobre éstos y un daño indirecto sobre los activos superiores.

Riesgo Acumulado: El riesgo acumulado es la valoración del daño para la organización, evaluado en los activos inferiores.

Riesgo Residual: El riesgo remanente después del tratamiento del riesgo. [11]

Análisis de riesgo: Uso sistemático de la información para identificar fuentes y para estimar el riesgo.

Valuación del Riesgo: Proceso general de análisis del riesgo y evaluación del riesgo.

Evaluación del Riesgo: Proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo.

Gestión del Riesgo: Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

Tratamiento del Riesgo: Proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo.

[10] **Fuente:** Libro de MAGERIT 2 (Método) – Ministerio de Administraciones Publicas de España

[11] **Fuente**: Biblioteca PILAR

Enunciado de Aplicabilidad: Enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización.[12]

2.3. MAGERIT versión 2.0

MAGERIT 2, es la metodología formal para el análisis y gestión de riesgos que soportan los sistemas de información elaborada por el Consejo Superior de Administración Electrónica de España. MAGERIT persigue los siguientes objetivos:

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos. (ver Fig. 2.3.1).
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

La Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones públicas, MAGERIT, es un método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.[13]

2.3.1. Proceso de la Metodología MAGERIT

[12] **Fuente**: Norma ISO/IEC Guía 73:2002

[13] **Fuente:** Libro de MAGERIT 2 – Publicación del Ministerio de Administraciones Publicas de España

Figura 2.3.1 Proceso MAGERIT

2.3.2 Identificación de Activos

Es en donde se identifican los activos de la organización. El activo esencial es la información que maneja el sistema; o sea los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes para su manejo en PILAR:

- **Los servicios** que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- **Las aplicaciones informáticas** *(software)* que permiten manejar los datos.
- **Los equipos informáticos** *(hardware)* y que permiten hospedar datos, aplicaciones y servicios.
- **Los soportes de información** que son dispositivos de almacenamiento de datos.
- **El equipamiento auxiliar** que complementa el material informático.
- **Las redes de comunicaciones** que permiten intercambiar datos.
- **Las instalaciones** que acogen equipos informáticos y de comunicaciones.

- **Las personas** que explotan u operan todos los elementos anteriormente citados.

2.3.3. Clases de Activos

No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes. PILAR contiene una tabla de clases de activos, que abarca todos los aspectos concernientes a los recursos de procesamiento de la información. Se debe asociar cada activo a una o varias clases de las propuestas en la herramienta.

2.3.4. Valoración de Activos

La valoración de un activo (ver Tabla 2.3.4.), se la hace de acuerdo a sus dimensiones (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad). A cada una de estas dimensiones se le da un valor de acuerdo a la siguiente tabla:

Tabla 2.3.4. Criterio de Valoración de Activos

Valor		Criterio
10	Muy alto	Daño muy grave a la organización
7 – 9	Alto	Daño grave a la organización
4 – 6	Medio	Daño importante a la organización
1 – 3	Bajo	Daño menor a la organización
0	Despreciable	Irrelevante a efectos prácticos

Para obtener el valor, PILAR dispone de una serie de criterios de valoración; este valor varía según la afectación que sufra activo, y que el usuario podrá escoger con la finalidad de obtener un valor preciso.

2.3.5. Identificación de Amenazas

PILAR presenta un catálogo de posibles amenazas incluidas en su biblioteca, que se asocian al activo de acuerdo a la clase seleccionada para el mismo.

2.3.6. Valoración de Amenazas

Una vez determinado que una amenaza puede perjudicar a un activo, PILAR estima cuán vulnerable es el activo, en dos sentidos (ver Tabla 2.4.6):

Degradación: cuán perjudicado resultaría el activo
Frecuencia: cada cuánto se materializa la amenaza

Tabla 2.3.6. Criterio de Valoración de Amenazas

FRECUENCIA	**DEGRADACION**
0,1 una vez cada 10 años	De 0% a 100% para los cinco pilares
1 todos los años	
10 todos los meses	
100 todos los días	

2.3.7. Impacto y Riesgo

El impacto es un indicador de qué puede suceder cuando ocurren las amenazas.

El riesgo es un indicador de lo que probablemente suceda por causa de las amenazas.

En PILAR, se miden los impactos y los riesgos como sigue (ver Tabla 2.3.7):

Tabla 2.3.7. Impacto y Riesgo

	cualitativo
impacto	nivel de valor
riesgo	nivel de criticidad

El impacto acumulado se calcula tomando en cuenta la siguiente fórmula:

Impacto acumulado = valor acumulado * degradación

Para calcular el riesgo acumulado que utilizamos el impacto acumulado y la probabilidad:

Riesgo acumulado = impacto acumulado * probabilidad

Análisis mediante tablas:

Para la Nomenclatura Utilizada (ver Tabla 2.3.7.1):

Tabla 2.3.7.1. Nomenclatura de la Estimación del Impacto y Riesgo

Estimación del Impacto

impacto		*degradación*		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

MB: muy bajo

B: bajo

M: medio

A: alto

MA: muy alto

Estimación del Riesgo

riesgo		*frecuencia*			
		PF	FN	F	MF
impacto	MA	A	MA	MA	MA
	A	M	A	MA	MA
	M	B	M	A	MA
	B	MB	B	M	A
	MB	MB	MB	B	M

MF: muy frecuente (a diario)

F: Frecuente (mensual)

FN: Frecuencia normal (anual)

PF: poco frecuente (cada varios años)

Aquellos activos que reciban una calificación de impacto muy alto (MA) deberían ser objeto de atención inmediata.	Aquellos activos que reciban una calificación de riesgo muy alto (MA) deberían ser objeto de atención inmediata. Los que reciban una calificación de riesgo alto, deberían ser objeto de planificación inmediata de salvaguardas.

El impacto y el riesgo se mitigan por medio de salvaguardas, viéndose reducidos a valores residuales.

2.3.8. Identificación y Valoración de Salvaguardas

PILAR en su biblioteca de trabajo contiene una colección de salvaguardas que están de acuerdo con los estándares internaciones de seguridad de la información. Se presenta una relación de salvaguardas adecuadas para cada tipo de activos.

La valoración de las salvaguardas depende de cuantas etapas existan en el proyecto. Por defecto existe la etapa actual y la objetivo. En cada etapa se realizara la evaluación del nivel de madurez de cada salvaguarda de acuerdo al progreso en ella con los siguientes criterios:

- **Eficacia de las Salvaguardas.**

Todos los modelos requieren una evaluación de la eficacia de las salvaguardas que se despliegan para proteger un activo de una amenaza.

Paquete de salvaguardas: Se define como el conjunto de salvaguardas acumuladas sobre un activo. Las diferentes Salvaguardas se pueden acumular de manera concurrente.

Eficacia de una Salvaguarda: Cada salvaguarda se valora según su eficacia reduciendo el riesgo del activo que protege. La eficacia de un paquete de salvaguardas es un número real entre 0,0 y 1,0:

- si una salvaguarda es idónea (100% eficaz), se dice que e = 1
- si una salvaguarda es insuficiente, se dice que e < 1
- si una salvaguarda no sirve, se dice que e= 0
- si una salvaguarda no tiene sentido en este contexto, se dice que e = na

2.4. Herramienta PILAR.

Pilar es un software que utiliza la metodología MAGERIT de análisis y gestión de riesgos.

Además tiene una biblioteca estándar de propósito general, y permite evaluar con puntaje la seguridad respecto:

Normas ISO 27000, Criterios de Seguridad, Normalización y Conservación del Consejo Superior de Informática, entre otras.

Con la utilización de esta herramienta se pretende:

Analizar los riesgos de acuerdo a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

También dispone de salvaguardas, normas y procedimientos de seguridad para el análisis del riesgo residual en el proceso de tratamiento.

Para un análisis de riesgos adecuado, es necesario tener conocimiento sobre el entorno Pilar en cuanto a:
Identificar los Activos, dependencias, valoración de activos, identificación amenazas, valoración de amenazas, identificación y valoración de salvaguardas.

2.5. Normas ISO

ISO es una organización no gubernamental que forma un puente entre los sectores públicos y privados y nació con el objetivo de "facilitar la coordinación internacional y la unificación de los estándares industriales."

La ISO ha reservado la serie ISO/IEC 27000 para una gama de normas de gestión de la seguridad de la información de manera similar a lo realizado con las normas de gestión de la calidad, la serie ISO 9000.

2.5.1. Norma ISO 27000

La serie ISO 27000 es una serie de estándares publicados por la Organización Internacional para la Estandarización y la Comisión Electrotécnica Internacional que contiene las normas para la Seguridad de la Información, utilizada por cualquier tipo de organización, pública o privada, grande o pequeña.

Las distintas normas que componen la serie ISO 27000; indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001.

2.5.2. Familias de la Norma ISO 27000

Iso 27001: Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información

Iso 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

Iso 27003: guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases.

Iso 27004: Sistema de Gestión de Seguridad de Información y de los controles relacionados

Iso 27005: Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

2.5.2.1. Norma ISO 27001

La Norma ISO 27001, siendo la principal norma en requisitos de la serie, está dedicada a especificar los requerimientos necesarios para: establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información.

Esta norma se basa en la gestión de riesgos y en el mejoramiento de los procesos, además para ser implantada el tiempo necesario es de 6 meses a 1 año.

La ISO 27001 contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma a la cual se certifican por auditores externos los SGSI de las organizaciones.

Seguridad de la Información

La seguridad de la información consiste en procesos y controles diseñados para proteger información de su divulgación no autorizada, transferencia, modificación o destrucción, a los efectos de:

- asegurar la continuidad del negocio;
- minimizar posibles daños al negocio;
- maximizar oportunidades de negocios.

La información debe ser protegida adecuadamente ya que viene a ser un activo muy importante en cualquier empresa.

La información puede estar:

- Impresa o escrita en papel
- Almacenada electrónicamente
- Transmitida por correo o medios electrónicos
- Mostrada en videos
- Hablada en conversación.

Pilares de Seguridad de la Información

Confidencialidad: Solo personas autorizadas tienen acceso a la información

Integridad: La información y sus métodos de proceso son exactos y completos

Disponibilidad: Los usuarios autorizados tienen acceso a la información y a sus activos asociados requeridos.

Enfoque del Proceso

Este estándar Internacional promueve la adopción de un enfoque del proceso para establecer implementar, operar, monitorear, revisar, mantener y mejorar el Sistema de Gestión de Seguridad Informática SGSI de una organización.

La Norma ISO 27001 adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA), el cual se puede aplicar a todos los procesos SGSI.

Modelo PDCA (ver Fig. y Tabla 2.5.2.1.), utilizado para establecer, implementar, monitorear y mejorar el SGSI

Ciclo de adaptación de la Norma

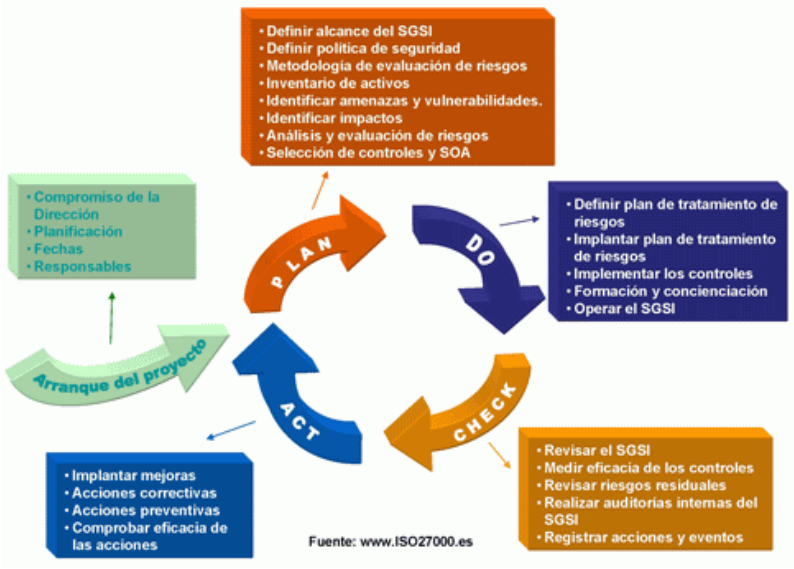


Figura 2.5.2.1. Ciclo de Adaptación de la Norma

Tabla 2.5.2.1. Ciclo de Adaptación de la Norma

Planear (Establecer el SGSI)	Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
Hacer (Implementar y operar el SGSI)	Implementar y operar la política controles, procesos y procedimientos SGSI
Chequear (monitorear y revisar el SGSI)	Evaluar y, donde sea aplicable medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión
Actuar (mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas basadas en los resultados de la auditoria interna SGSI y la revisión gerencial u otra información relevante continua del SGSI.

2.5.2.2. Estándar Internacional ISO/IEC 27002

Antes llamada ISO/IEC 17799, es una guía de buenas prácticas en la gestión de la seguridad de la información. Esta contiene los dominios, objetivos de control y controles para el proceso de diseño e implantación de sistemas de seguridad de la información.

ISO/IEC 27002 está conformada de 11 dominios, 39 objetivos de control en donde constan los 133 controles recomendados para la seguridad de la información. Los dominios son los siguientes:

- **Política de seguridad:** proporciona a la gerencia la dirección y soporte para la seguridad de la información.
- **Aspectos organizativos de la seguridad de la información: L**a organización interna, tiene como objetivo manejar la seguridad de la información y mantener la seguridad de la información y los medios de procesamiento de información de la organización.
- **Gestión de activos: A**signa responsabilidades por cada uno de los activos de la organización.
- **Seguridad física y ambiental: S**e refiere a un perímetro de seguridad física, seguridad del cableado, mantenimiento y control de temperatura de los equipos, etc.
- **Gestión de comunicaciones y operaciones: A**segura la operación correcta y segura de los medios de procesamiento de la información.
- **Control de acceso:** Consiste en tener registro y autenticación de usuarios, gestión de privilegios, y contraseñas, etc.
- **Gestión de incidentes de seguridad en la seguridad de la información:** Recomienda trabajar con reportes de los eventos y debilidades de la seguridad de la información.
- **Gestión de la continuidad del negocio:** Desarrollo de planes para la continuidad del negocio para asegurar la reanudación oportuna de las operaciones esenciales en caso de alguna falencia.
- **Cumplimiento:** Prioriza el cumplimiento de requisitos legales para evitar violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

Esta Norma nos da a conocer el estándar en el tema de Seguridad de la Información, el mismo que tiene en su base tres pilares (ver Fig. 2.5.2.2.) que son: Confidencialidad, integridad, y disponibilidad, sin embargo no toma en cuenta el criterio de autenticidad, el mismo que podría considerarse como un cuarto pilar para fortalecer el concepto de Seguridad.

Alcance

Figura 2.5.2.2. Pilares de Seguridad

Objetivos de control y controles de la Norma ISO/IEC 27002

Todas estas fases de la metodología serán realizadas con base en las normas ISO 27001 e ISO 27002, tratadas anteriormente en este documento, las cuales son estándares para la seguridad de la información en donde se establecen los dominios, objetivos de control y controles necesarios para el desarrollo de un sistema de seguridad internacionalmente aceptado.

Los dominios, objetivos de control y controles (ver Tabla 2.5.2.2.), están resumidos a continuación:

Tabla 2.5.2.2. Objetivos de Control y Controles de la Norma ISO/IEC 27002

Objetivos de Control y Controles

Edición 2005		Objetivos	Controles
5	Política de Seguridad	1	2
6	Aspectos organizativos para la seguridad	2	11
7	Gestión de los activos	2	5
8	Seguridad de los Recursos Humanos	3	9
9	Seguridad física y del entorno	2	13
10	Gestión de comunicaciones y operaciones	10	32
11	Control de accesos	7	25
12	Adquisición, Desarrollo y mantenimiento de sistemas	6	16
13	Gestión de incidentes de seguridad de la información.	2	5
14	Gestión de continuidad del negocio	1	5
15	Conformidad	3	10
Totales		39	133

CAPITULO III

Diagnóstico de la situación actual del Data Center basado en los controles de la Norma ISO 27004 y Aplicación de la Metodología MAGERIT

3.1 Situación Actual del Data Center

El informe fue elaborado en base a la información provista por UTICS y las observaciones tomadas durante las visitas realizadas al la institución durante los meses de Noviembre 2010 y Enero 2011.

3.1.1 Introducción:

Este informe de la situación actual de la Seguridad informática del Data Center de la ESPE contiene según los resultados de las encuestas el estado de los S.I.

3.1.2 Metodología

En el Presente diagnostico se obtuvieron resultados de las Encuestas y Cuestionarios elaborados a partir de las preguntas de la Norma ISO 27004 y documentado en las fechas establecidas en el Plan de Investigación.

A continuación presentamos las respuestas obtenidas en forma General de las encuestas en cuanto a Seguridad de la Información abarcando las respuestas de los 11 dominios que indica la Norma ISO 27001 y 27002.

En los resultados siguientes se incluye la gráfica correspondiente a cada pregunta.

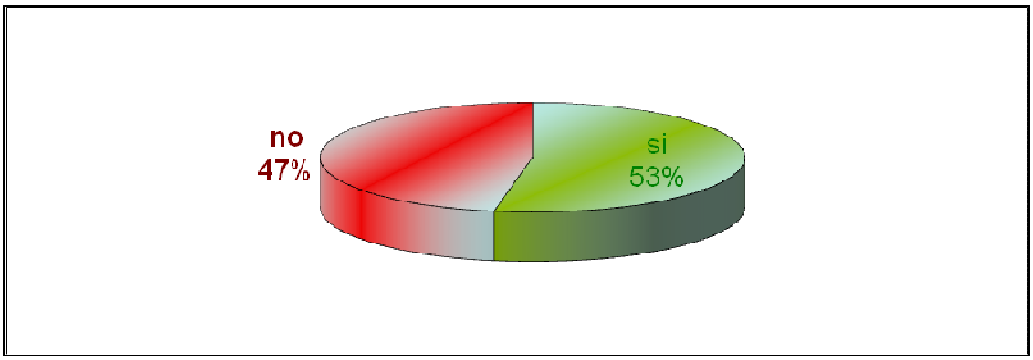


Figura 3.1. Resultado de la encuesta a UTIC'S

Si cumple con la Norma ISO 27004: en 53%, No cumple en un 47%

3.1.3 Políticas de Seguridad

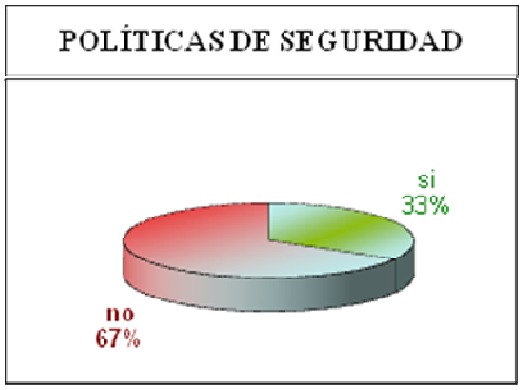
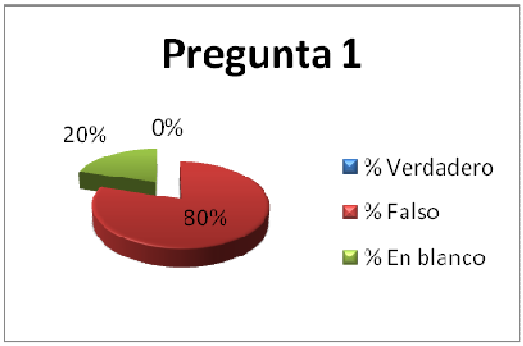


Figura 3.1.3 Resultado del Dominio: Políticas de Seguridad

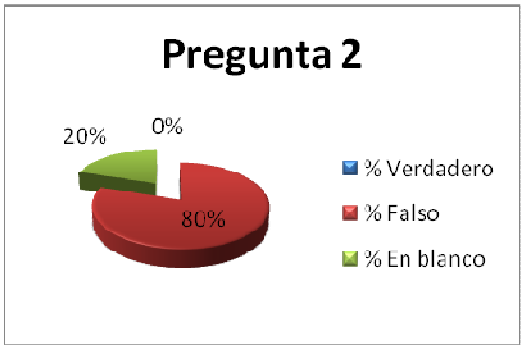
3.1.3.1. Existen documento(s) de políticas de seguridad de S.I.?

Si Hay	
No hay	X



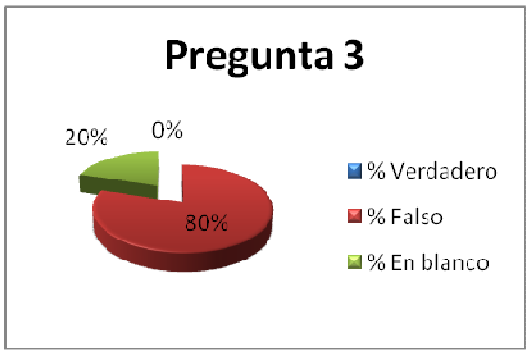
3.1.3.2. Existe normativa relativa a la seguridad de S.I.

Si Hay	
No hay	x



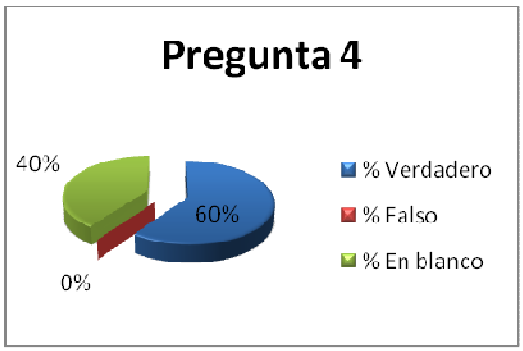
3.1.3.3. Existen procedimientos relativos a la seguridad de S.I.

Si Hay	
No hay	x



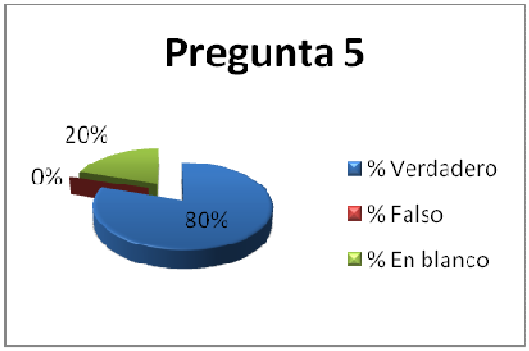
3.1.3.4. Existe un responsable de las políticas, normas y procedimientos

Si Hay	x
No hay	



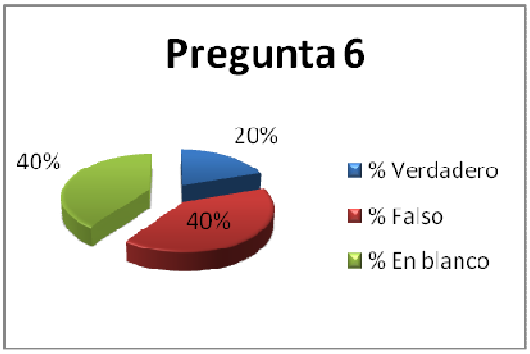
3.1.3.5. Existen mecanismos para la comunicación a los usuarios de las normas

Si Hay	X
No hay	



3.1.3.6. Existen controles regulares para verificar la efectividad de las políticas

Si	
No	X

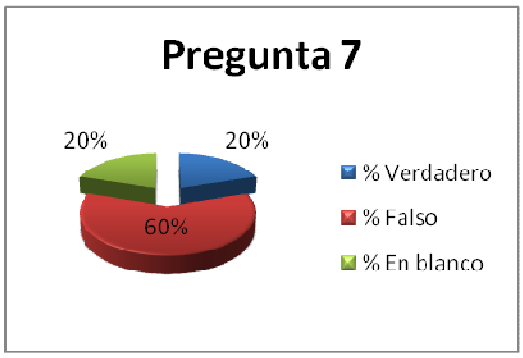


3.1.4 Organización de la Seguridad

Figura 3.1.4 Resultado del Dominio: Organización de la Seguridad

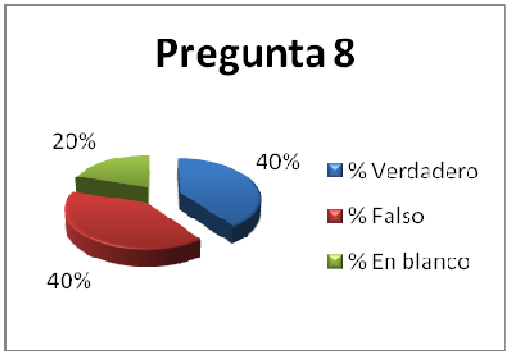
3.1.4.1. Existen roles y responsabilidades definidos para las personas implicadas en la seguridad.

Si Hay [ ]
No hay [X]



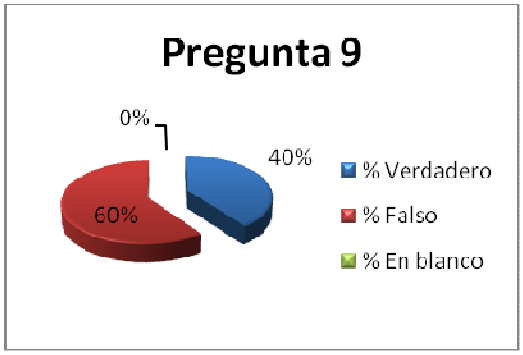
3.1.4.2. Existe un responsable encargado de evaluar la adquisición y cambios de S.I.

Si Hay [ ]
No hay [X]



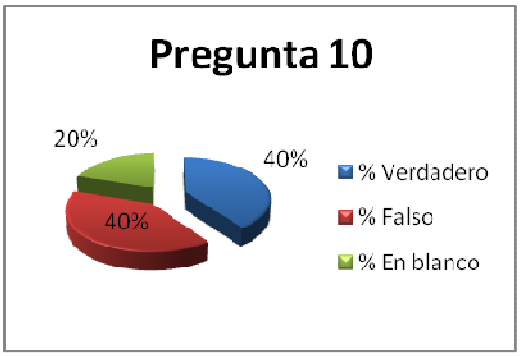
3.1.4.3. La Dirección y las áreas de la Organización de UTIC'S participa en temas de seguridad.

Si Hay [ ]
No hay [X]



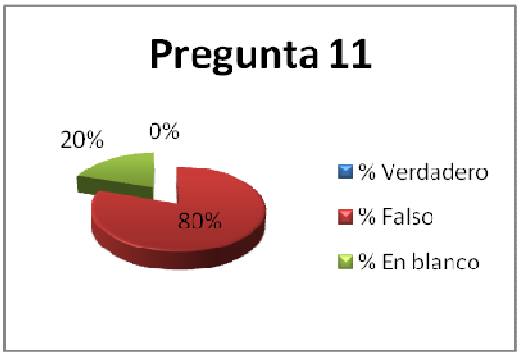
3.1.4.4 Existen condiciones contractuales de seguridad con terceros y Outsourcing.

Si Hay	
No hay	x



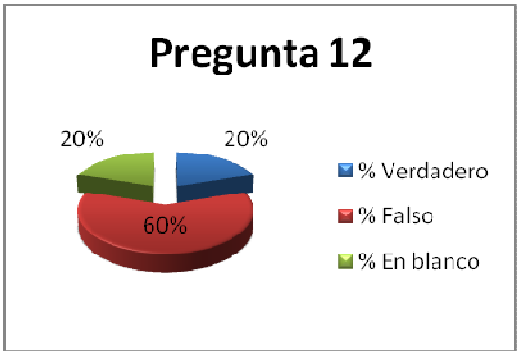
3.1.4.5. Existen criterios de seguridad en el manejo de terceras partes:

Si Hay	
No hay	x



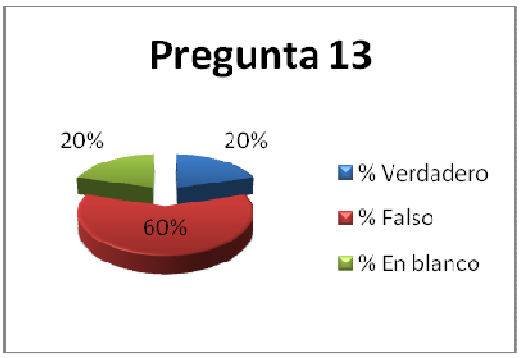
3.1.4.6. Existen programas de formación en seguridad para los empleados, clientes y terceros

Si Hay [ ]
No hay [x]



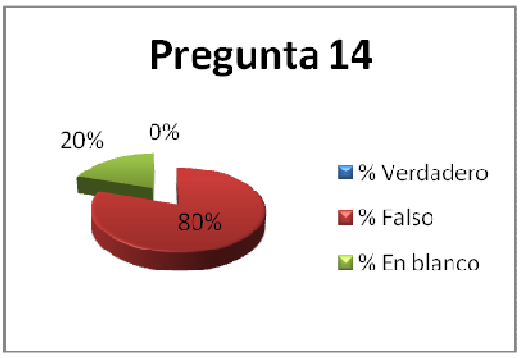
3.1.4.7 . Existe un acuerdo de confidencialidad de la información a la que se accede.

Si Hay [ ]
No hay [X]



3.1.4.8. Se revisa la organización de la seguridad periódicamente por una empresa externa

Si Hay [ ]
No hay [x]



3.1.5 Gestión de Activos

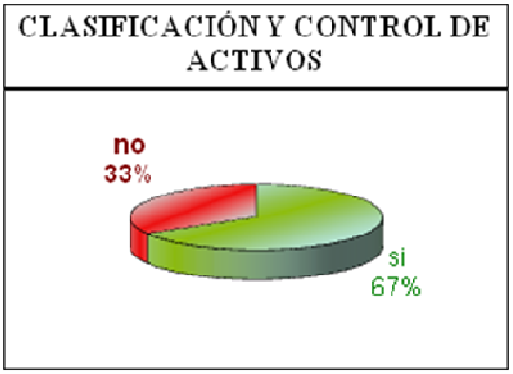
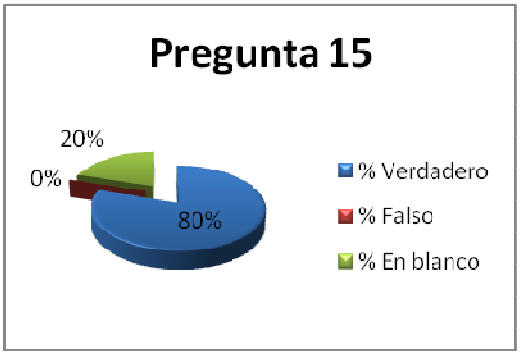


Figura 3.1.5 Resultado del Dominio: Gestión de Activos

3.1.5.1. Existe un inventario de activos actualizado

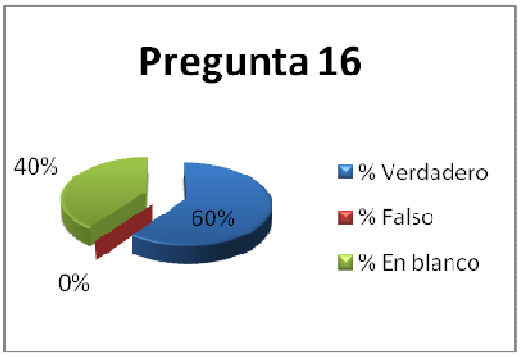
Control: Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes.

Si Hay	X
No hay	



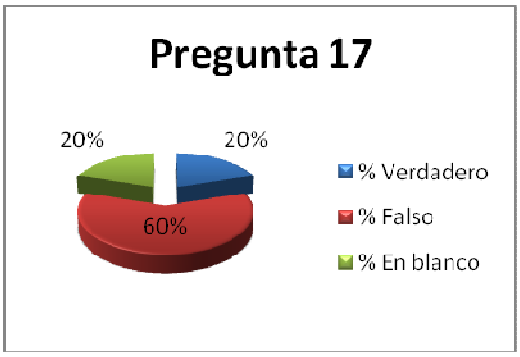
3.1.5.2. El Inventario contiene activos de datos, software, equipos y servicios

Si Hay	X
No hay	



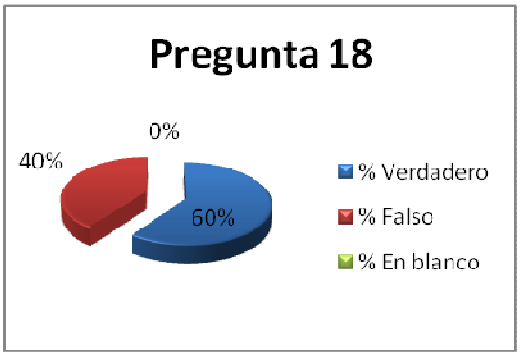
3.1.5.3 Se dispone de una clasificación de la información según la criticidad de la misma.

Si Hay [ ]
No hay [x]



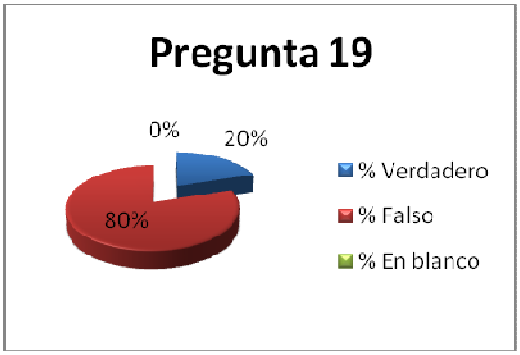
3.1.5.4 Existe un responsable de los activos

Si Hay [x]
No hay [ ]



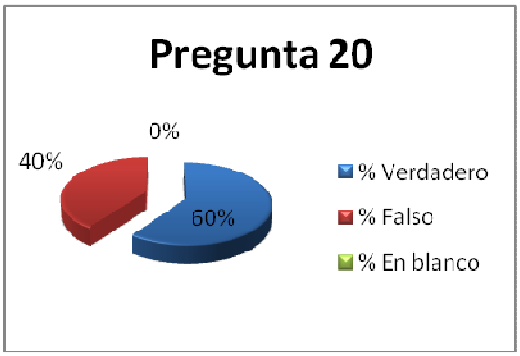
3.1.5.5. Existen procedimientos para clasificar la información.

Si Hay	
No hay	x



3.1.5.6 Existen procedimientos de etiquetado de la información

Si Hay	x
No hay	



3.1.6 Seguridad Ligada a los Recursos Humanos

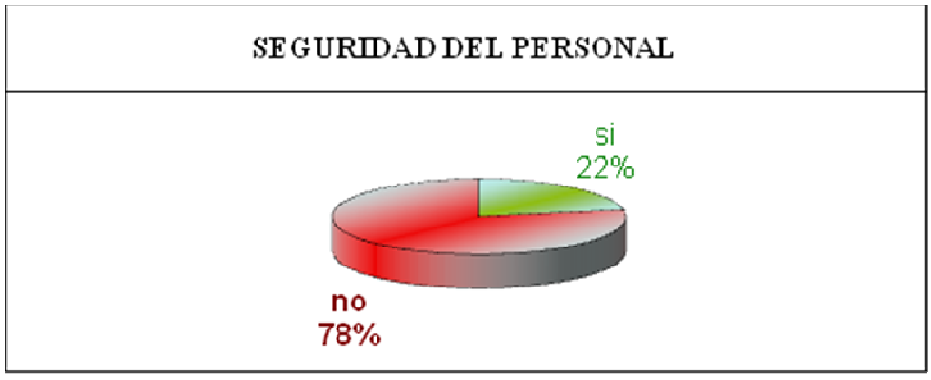
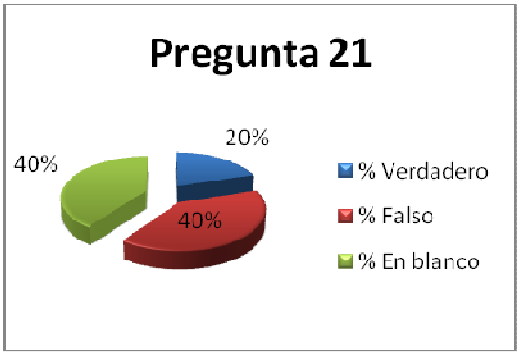


Figura 3.1.6 Resultado del Dominio: Seguridad Ligada a los Recursos Humanos

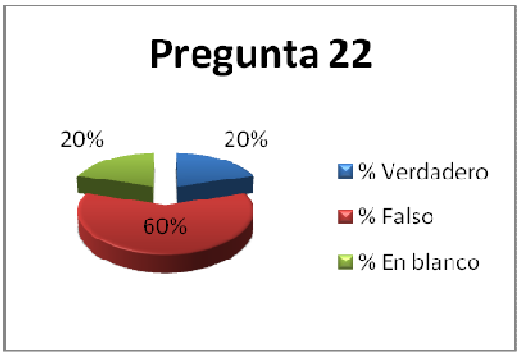
3.1.6.1. Se tienen definidas responsabilidades y roles de seguridad.

Si Hay	
No hay	x



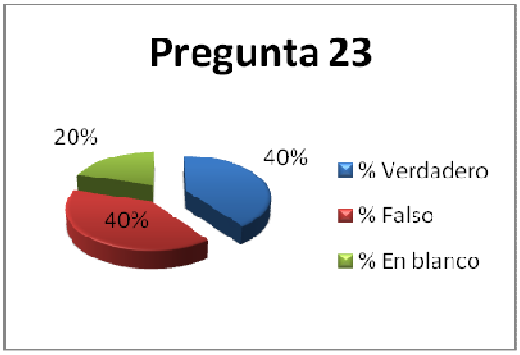
3.1.6.2. Se tiene en cuenta la seguridad en la selección y baja del personal

Si Hay	
No hay	x



3.1.6.3. Se plasman las condiciones de confidencialidad y responsabilidades en los contratos.

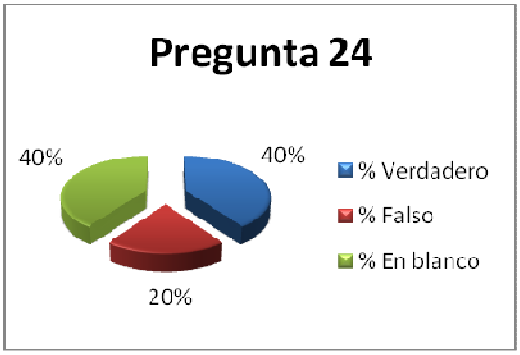
Si Hay	
No hay	x



3.1.6.4. Se imparte la formación adecuada de seguridad y tratamiento de activos.

Se proporciona a todos los empleados, contratistas y usuarios de tercera parte, un nivel adecuado de concienciación, educación y formación en los procedimientos de seguridad así como en el uso correcto de los recursos de tratamiento de la información, para minimizar los posibles riesgos de seguridad.

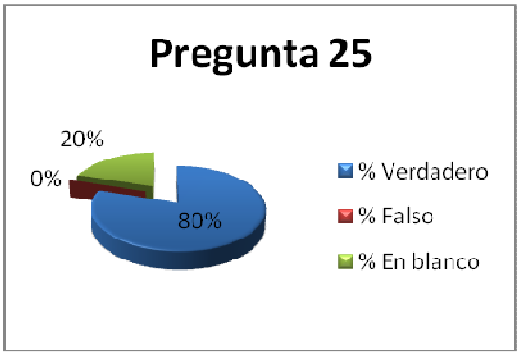
Si Hay	
No hay	x



3.1.6.5. Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad:

Incidentes de Seguridad Informática como por ejemplo:
Accesos no autorizados, códigos maliciosos, denegación del servicio, escaneos, pruebas o intentos de obtención de información de la red o de un servidor en particular, mal uso de los recursos tecnológicos.
UTIC'S posee algún procedimiento para contrarrestar estos posibles incidentes:

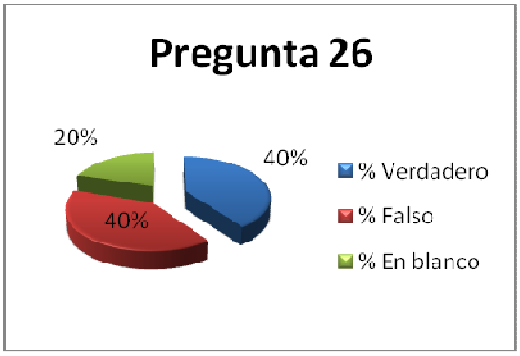
Si Hay [X]
No hay [ ]



3.1.6.6. Se recogen los datos de los incidentes de forma detallada

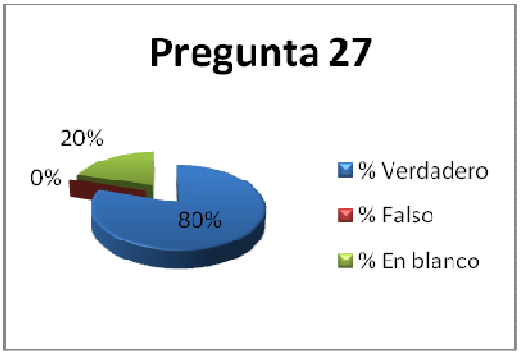
Control: Recolección ordenada de incidentes

Si [ ]
No [X]



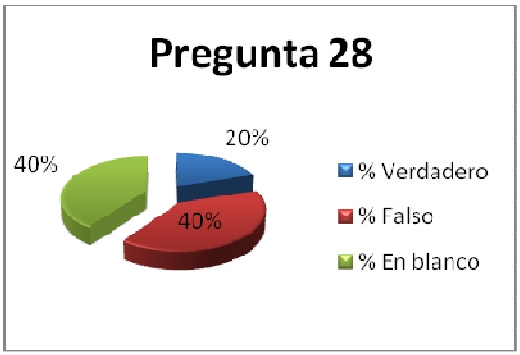
3.1.6.7. Informan los usuarios de las vulnerabilidades observadas o sospechadas:

Si Hay [X]
No hay [ ]



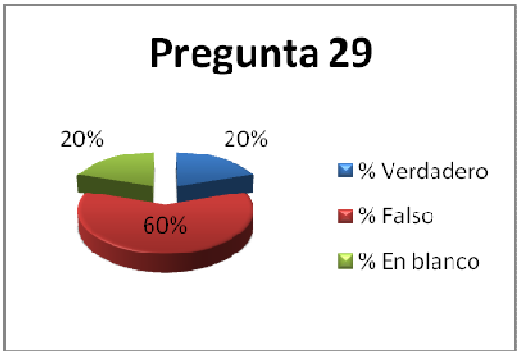
3.1.6.8. Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades.

Si Hay	
No hay	x



3.1.6.9. Existe un proceso disciplinario de la seguridad de la información:

Si Hay	
No hay	x



3.1.7 Seguridad Física y del Ambiente

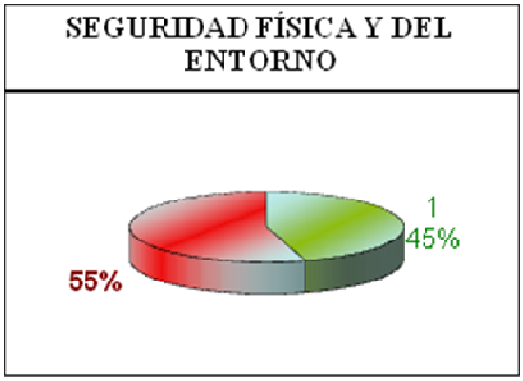
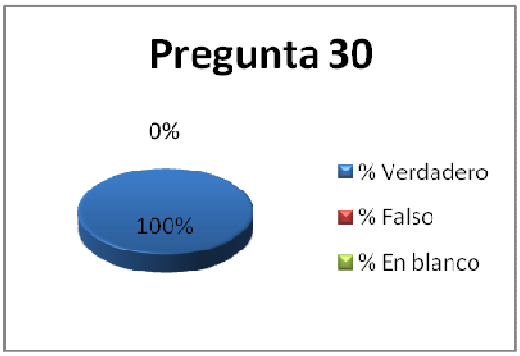


Figura 3.1.7 Resultado del Dominio: Seguridad Física y del Ambiente

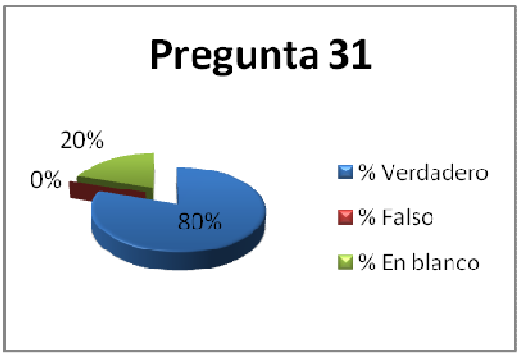
3.1.7.1. Existe perímetro de seguridad física (una pared, puerta con llave).

Si Hay	X
No hay	



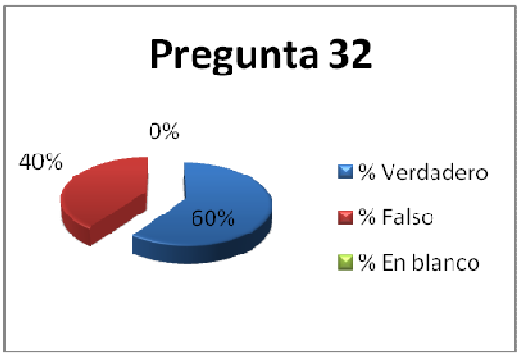
3.1.7.2. Existen controles de entrada para protegerse frente al acceso de personal no autorizado:

Si Hay	X
No hay	



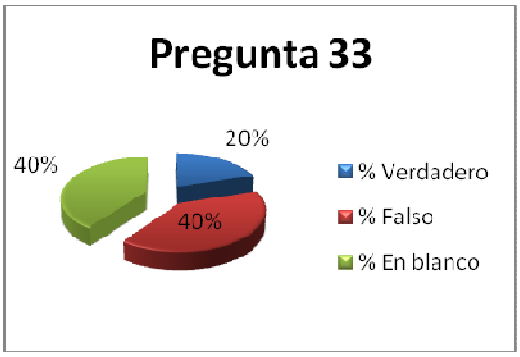
3.1.7.3. Un área segura ha de estar cerrada, aislada y protegida de eventos naturales.

Si Hay	X
No hay	



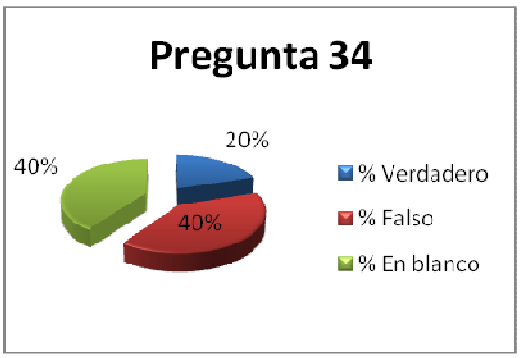
3.1.7.4. En las áreas seguras existen controles adicionales al personal propio y ajeno:

Si Hay	
No hay	x



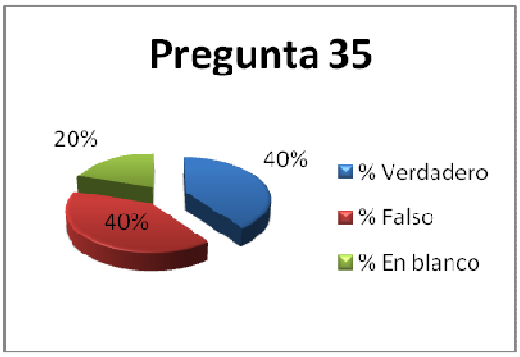
3.1.7.5. Las áreas de carga y expedición están aisladas de las áreas de S.I.

Si Hay	
No hay	x



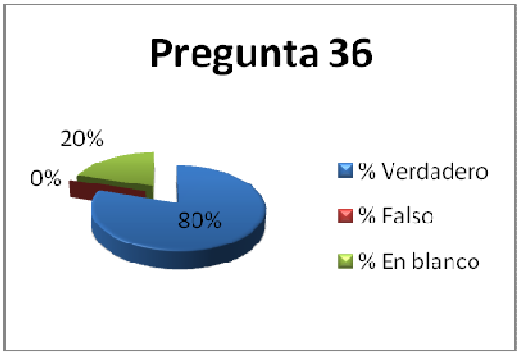
3.1.7.6. La ubicación de los equipos está de tal manera para minimizar accesos innecesarios.

Si Hay	
No hay	x



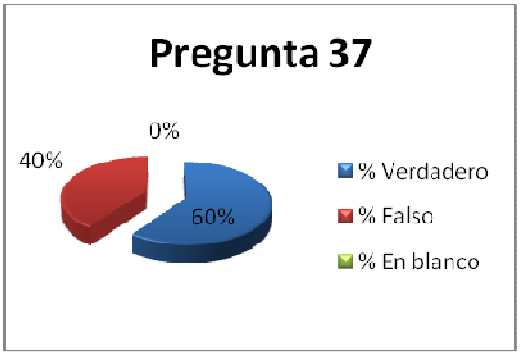
3.1.7.7. Existen protecciones frente a fallos en la alimentación eléctrica

Si Hay	x
No hay	



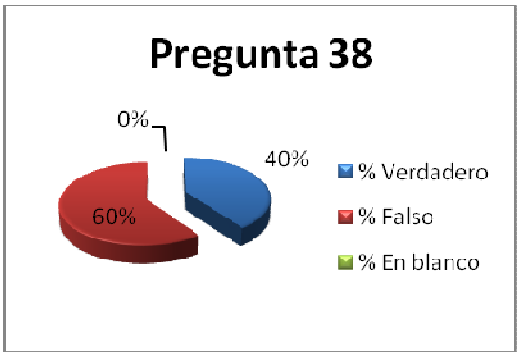
3.1.7.8. Existe seguridad en el cableado general del DataCenter, frente a daños e intercepciones:

Si Hay	x
No hay	



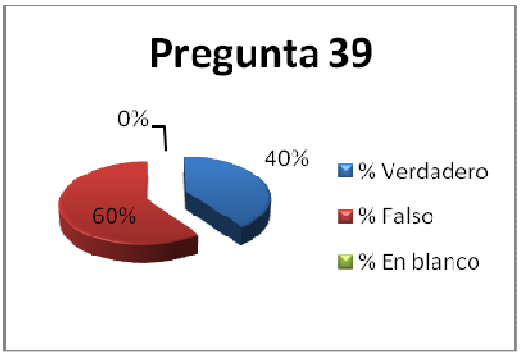
3.1.7.9. Se asegura la disponibilidad e integridad de todos los equipos

Si Hay	
No hay	x



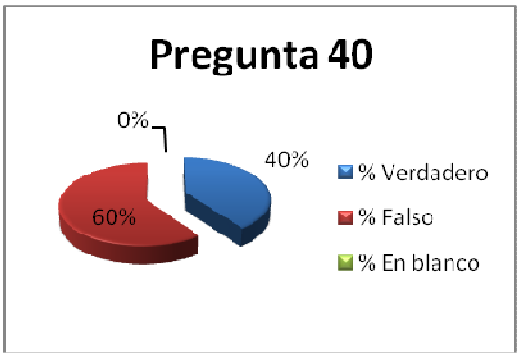
3.1.7.10. Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente:

Si Hay	
No hay	x



3.1.7.11. Se incluye la seguridad en equipos móviles

Si Hay	
No hay	x



3.1.8 Gestión de Comunicaciones y Operaciones

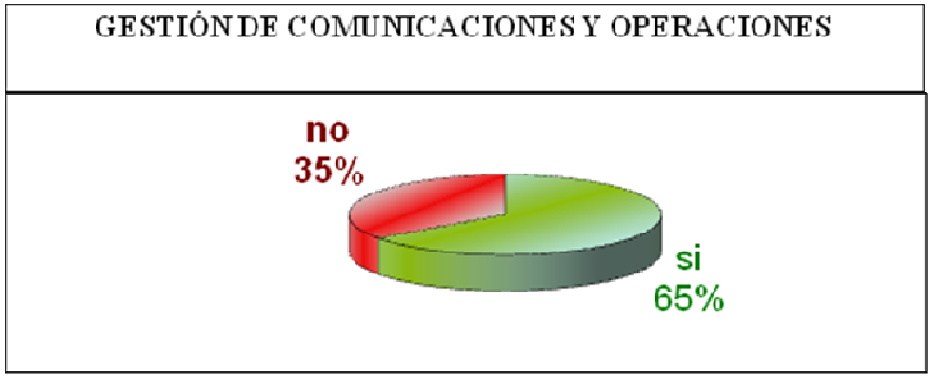
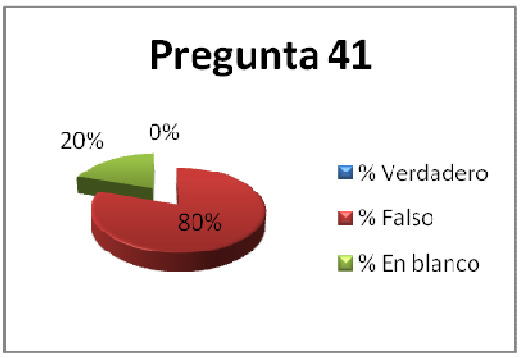


Figura 3.1.8 Resultado del Dominio: Gestión de Comunicaciones y Operaciones

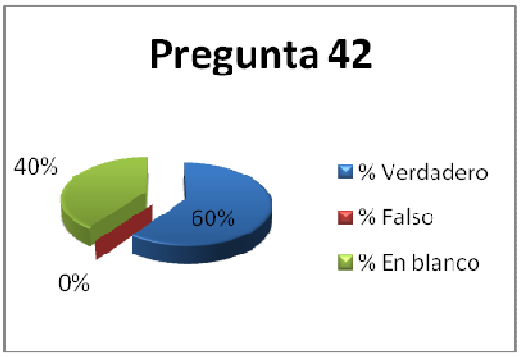
3.1.8.1 Todos los procedimientos operativos identificados en la política de seguridad están documentados:

Si Hay	
No hay	X



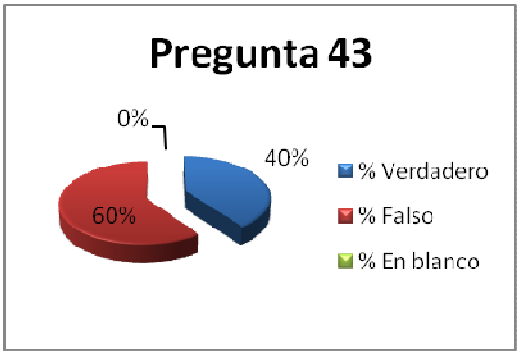
3.1.8.2. Están establecidas responsabilidades para controlar los cambios en equipos

Si Hay	X
No hay	



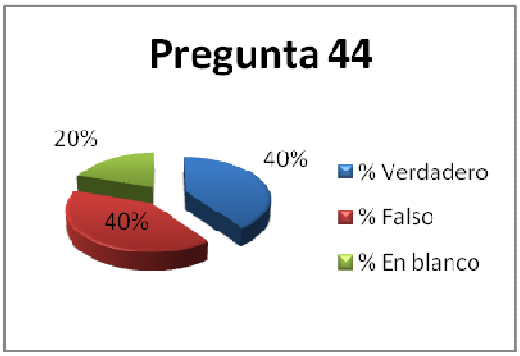
3.1.8.3. Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad

Si Hay	
No hay	X



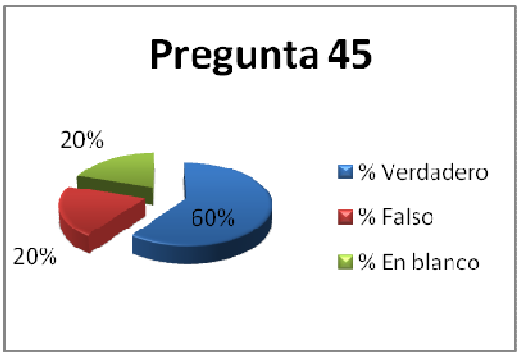
3.1.8.4. Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas

Si Hay	
No hay	X



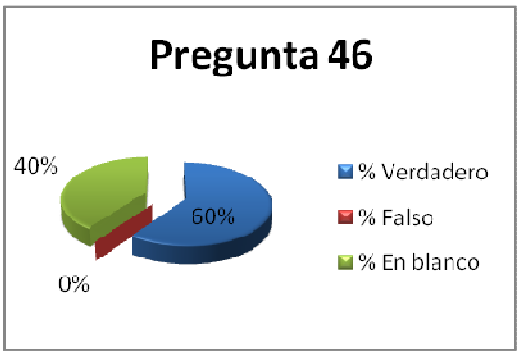
3.1.8.5. Existe una separación de los entornos de desarrollo y producción:

Si Hay	X
No hay	



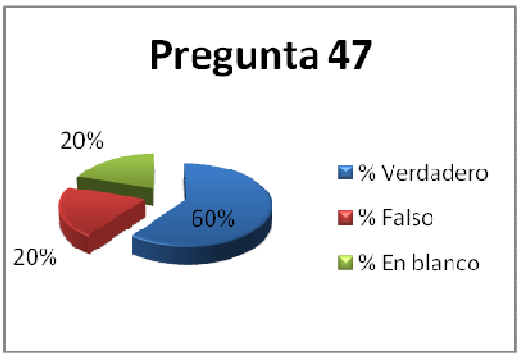
3.1.8.6. Existen contratistas externos para la gestión de los Sistemas de Información

Si Hay	X
No hay	



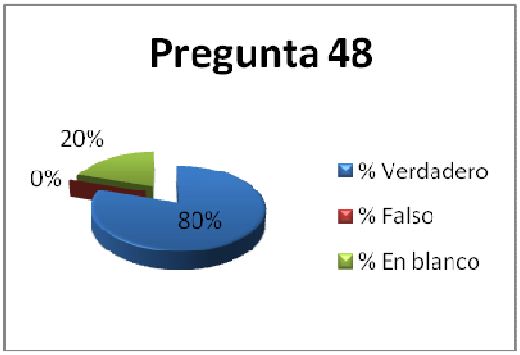
3.1.8.7. Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento:

Si Hay	X
No hay	



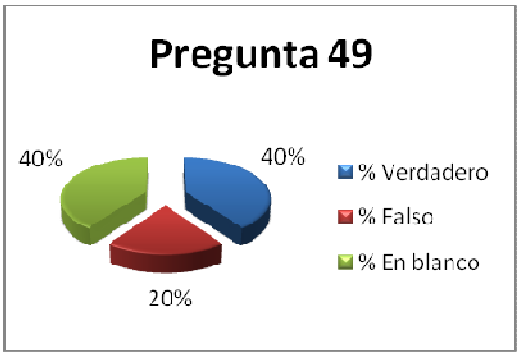
3.1.8.8. Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones

Si Hay	X
No hay	



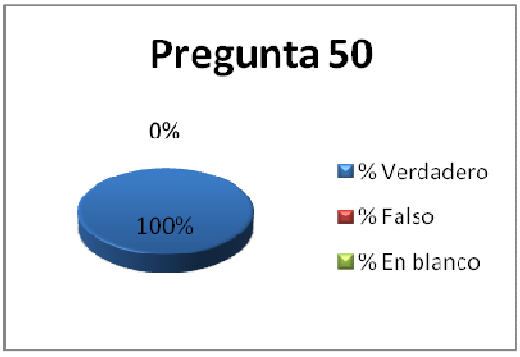
3.1.8.9. Controles contra software maligno

Si Hay	
No hay	X



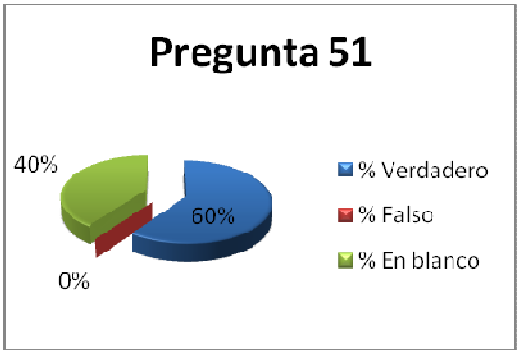
3.1.8.10. Realizar copias de backup de la información esencial para el negocio

Si Hay	X
No hay	



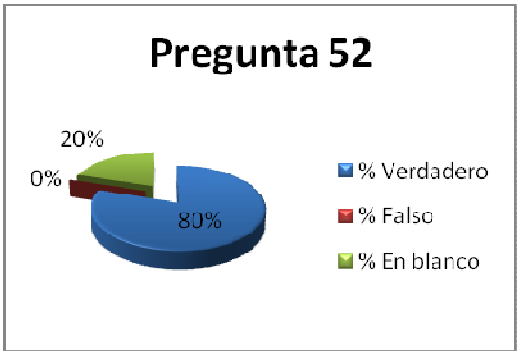
3.1.8.11. Existen logs (registro de actividad de un sistema) para las actividades realizadas por los operadores y administradores

Si Hay	X
No hay	



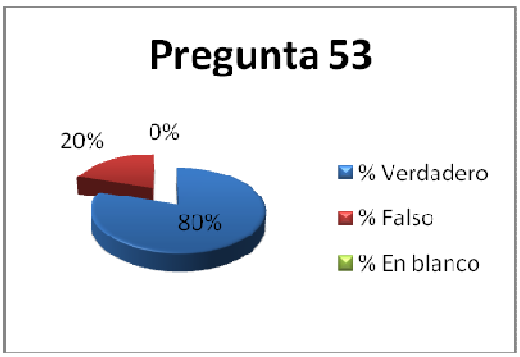
3.1.8.12. Existen logs de los fallos detectados

Si Hay	X
No hay	



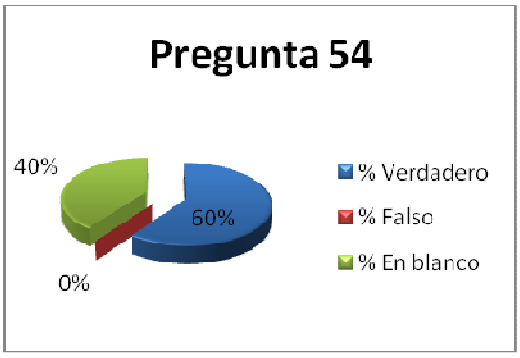
3.1.8.13. Existen rastro de auditoría

Si Hay	X
No hay	



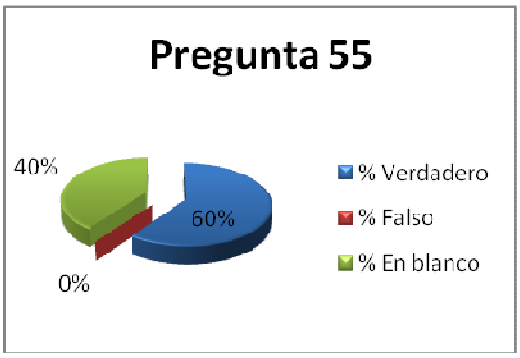
3.1.8.14. Existe algún control en las redes

Si Hay	X
No hay	



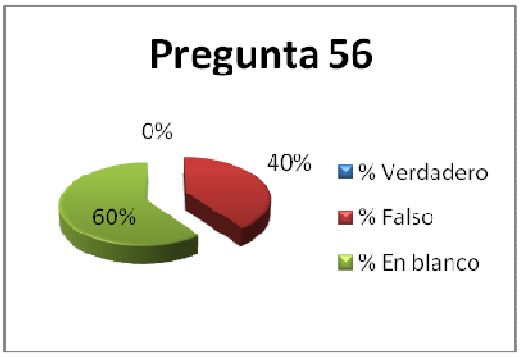
3.1.8.15. Hay establecidos controles para realizar la gestión de los medios informáticos. (Cintas, discos, removibles, informes impresos):

Si Hay	X
No hay	



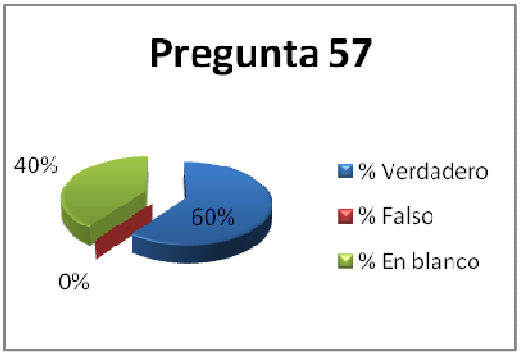
3.1.8.16. Eliminación de los medios informáticos. Pueden disponer de información sensible.

Si Hay	
No hay	X



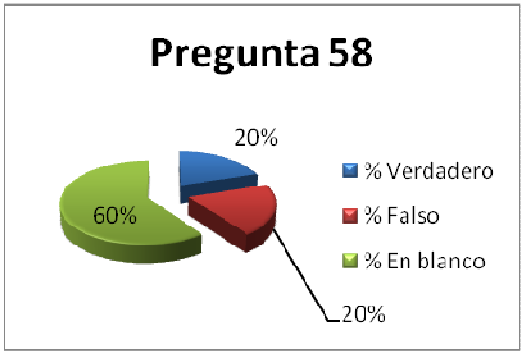
3.1.8.17. Existe seguridad de la documentación de los Sistemas

Si Hay	X
No hay	



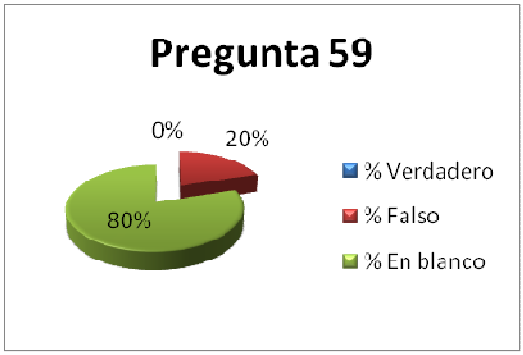
3.1.8.18. Existen acuerdos para intercambio de información y software.

Si Hay	
No hay	X



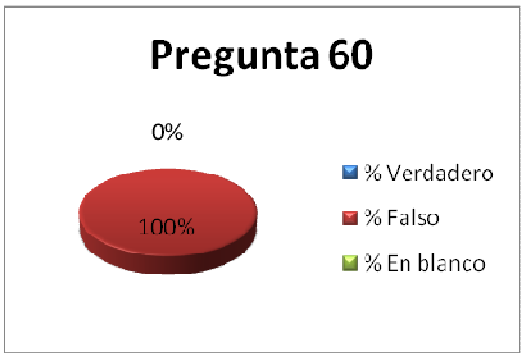
3.1.8.19. Existen medidas de seguridad de los medios en el tránsito

Si Hay	
No hay	X



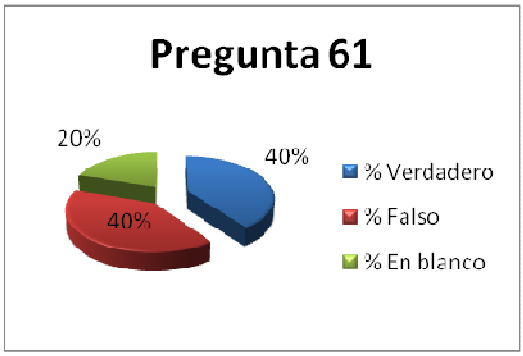
3.1.8.20. Existen medidas de seguridad en el comercio electrónico

Si Hay	
No hay	X



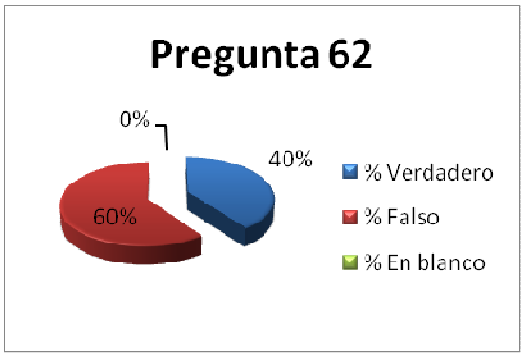
3.1.8.21. Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada

Si Hay	
No hay	X



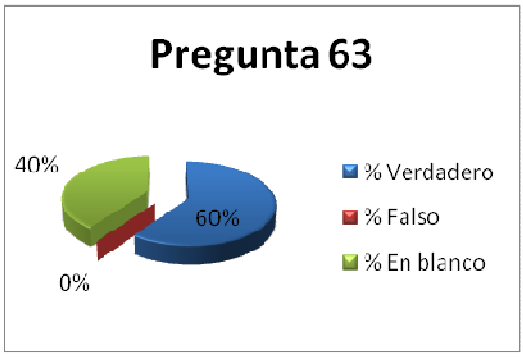
3.1.8.22. Existen medidas de seguridad en las transacciones en línea

Si Hay	
No hay	x



3.1.8.23. Se monitorean las actividades relacionadas a la seguridad

Si Hay	x
No hay	



3.1.9 Control de Accesos

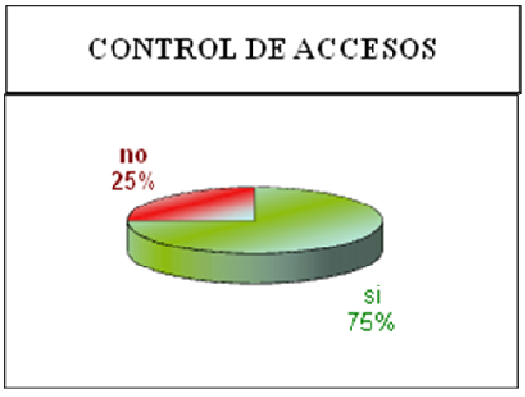
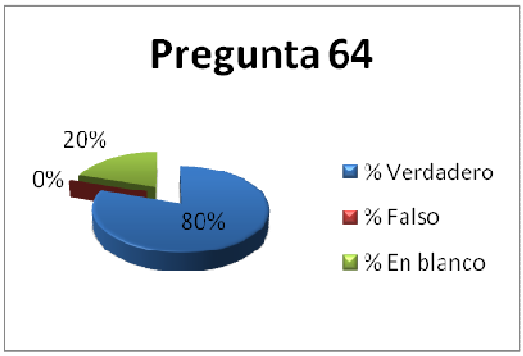


Figura 3.1.9 Resultado del Dominio: Control de Accesos

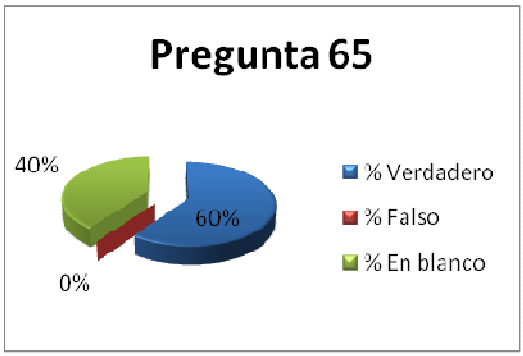
3.1.9.1. Existe una política de control de accesos

Si Hay	X
No hay	



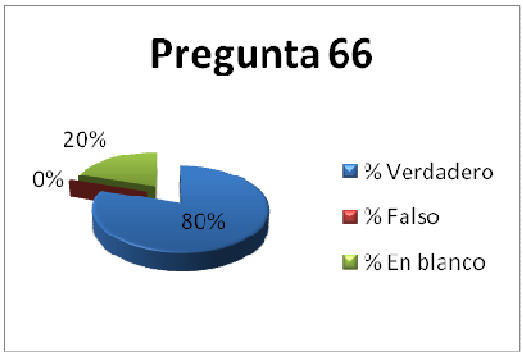
3.1.9.2. Existe un procedimiento formal de registro y baja de accesos

Si Hay	X
No hay	



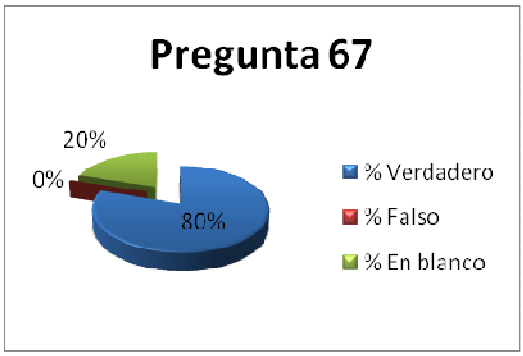
3.1.9.3. Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario

Si Hay	X
No hay	



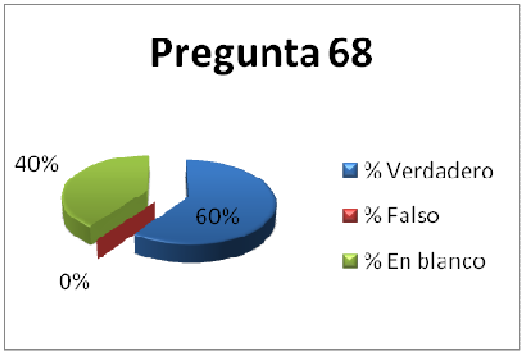
3.1.9.4. Existe una gestión de los password de usuarios

Si Hay	X
No hay	



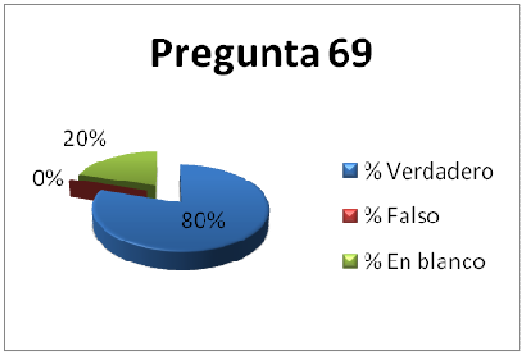
3.1.9.5. Existe una revisión de los derechos de acceso de los usuarios

Si Hay	X
No hay	



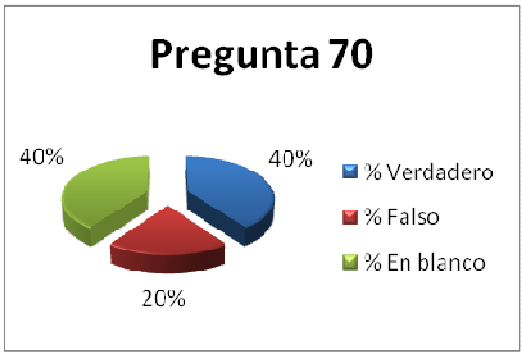
3.1.9.6. Existe el uso del password

Si Hay	X
No hay	



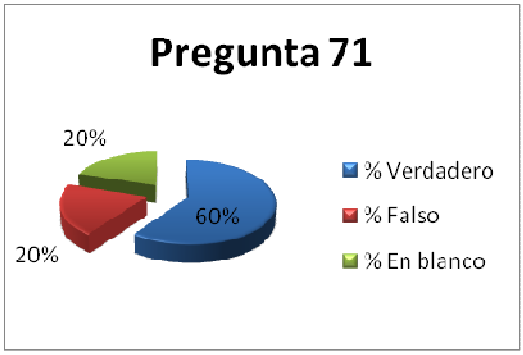
3.1.9.7. Se protege el acceso de los equipos desatendidos

Si Hay	
No hay	x



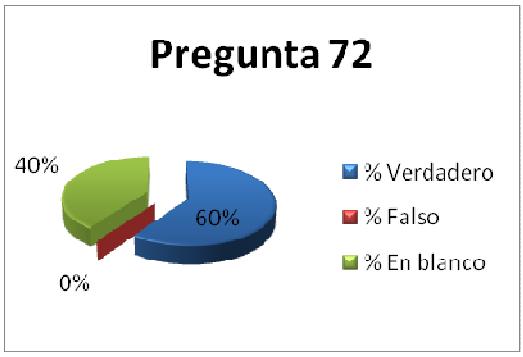
3.1.9.8. Existen políticas de limpieza en el puesto de trabajo

Si Hay	x
No hay	



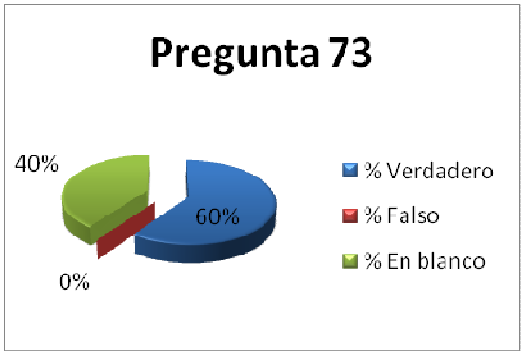
3.1.9.9. Existe una política de uso de los servicios de red

Si Hay	x
No hay	



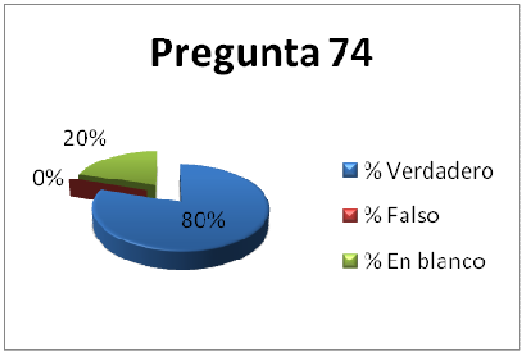
3.1.9.10. Se asegura la ruta (path) desde el terminal al servicio tanto internos como externos:

Si Hay [X]
No hay [ ]



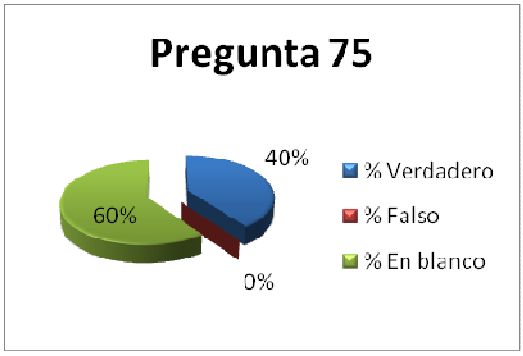
3.1.9.11. Existe una autenticación de usuarios en conexiones externas

Si Hay [X]
No hay [ ]



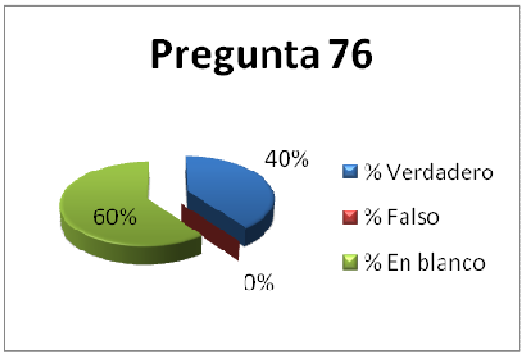
3.1.9.12. Existe una autenticación de los nodos

Si Hay [ ]
No hay [X]



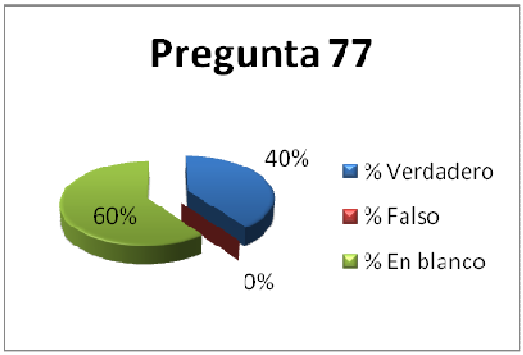
3.1.9.13. Existe un control de la conexión de redes

Si Hay	
No hay	x



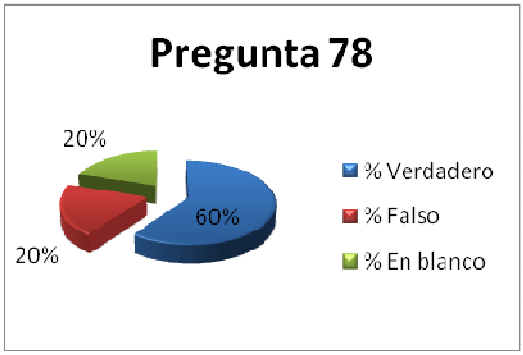
3.1.9.14. Existe un control del routing (dispositivo para la interconexión de redes informáticas) de las redes internas y externas:

Si Hay	
No hay	x



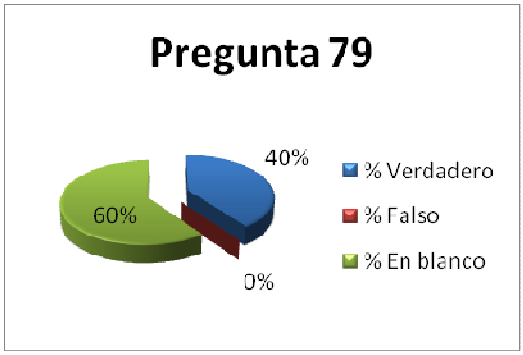
3.1.9.15. Existe una identificación única de usuario y una automática de terminales

Si Hay	x
No hay	



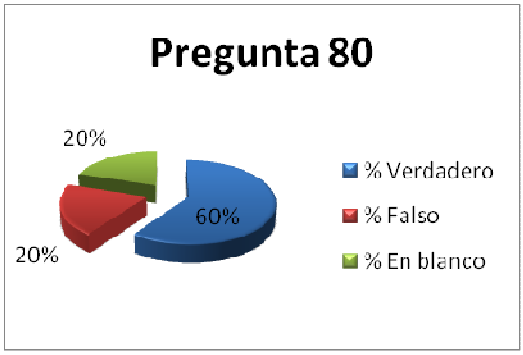
3.1.9.16. Existen procedimientos de log-on al terminal internos y externos:

Si Hay	
No hay	x



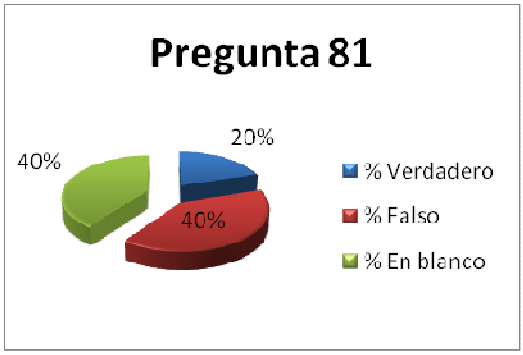
3.1.9.17. Se ha incorporado medidas de seguridad a la computación móvil.

Si Hay	x
No hay	



3.1.9.18. Está controlado el teletrabajo por la organización

Si Hay	
No hay	x



3.1.10 Adquisición Desarrollo y Mantenimiento de los Sistemas

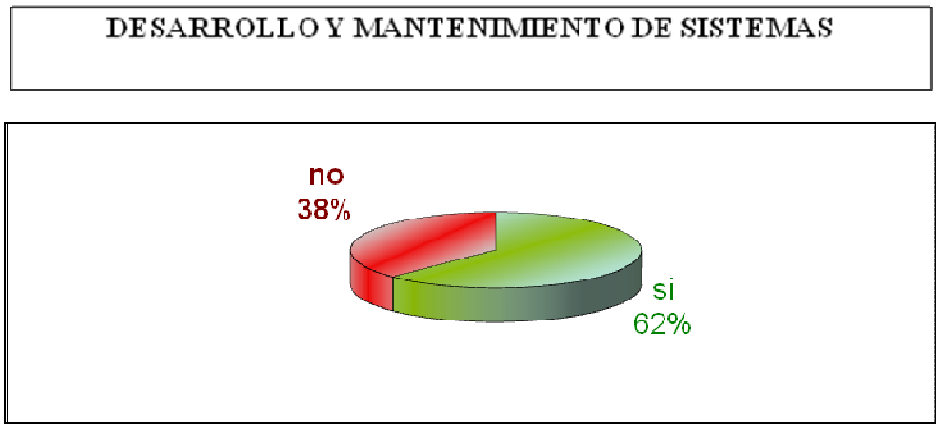
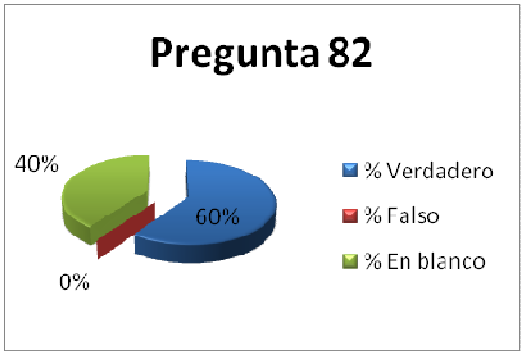


Figura 3.1.10 Resultado del Dominio: Adquisición Desarrollo y Mantenimiento de los Sistemas

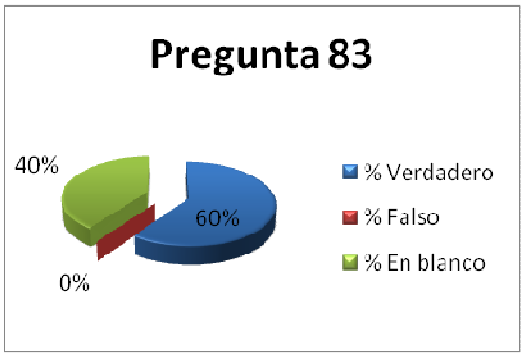
3.1.10.1. Se asegura que la seguridad está implantada en los Sistemas de Información

Si Hay	X
No hay	



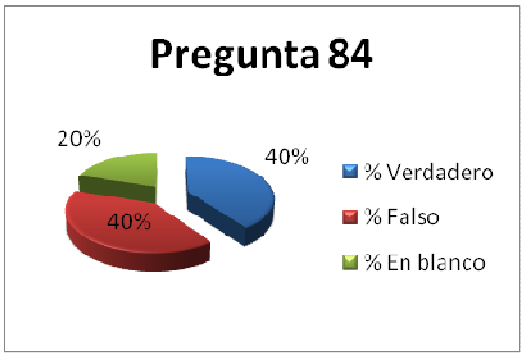
3.1.10.2. Existe seguridad en las aplicaciones

Si Hay	X
No hay	



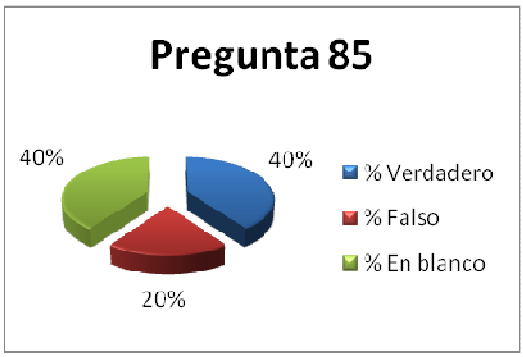
3.1.10.3. Existen controles criptográficos.

Si Hay	
No hay	x



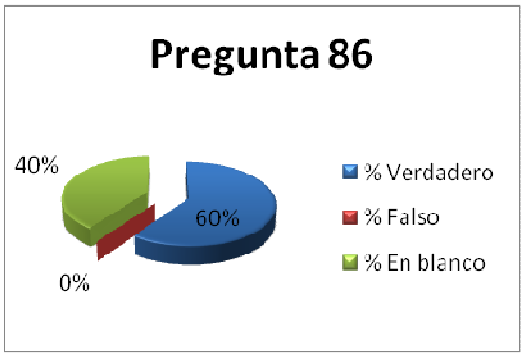
3.1.10.4. Existe seguridad en los ficheros de los sistemas

Si Hay	
No hay	x



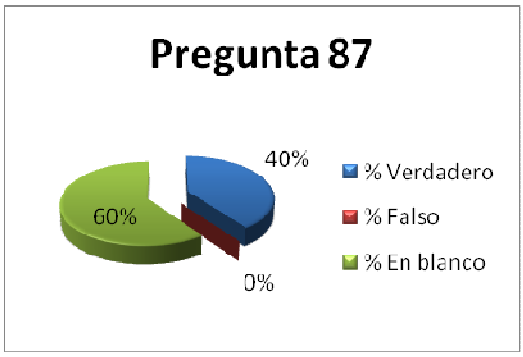
3.1.10.5. Existe seguridad en los procesos de desarrollo, testing y soporte

Si Hay	x
No hay	



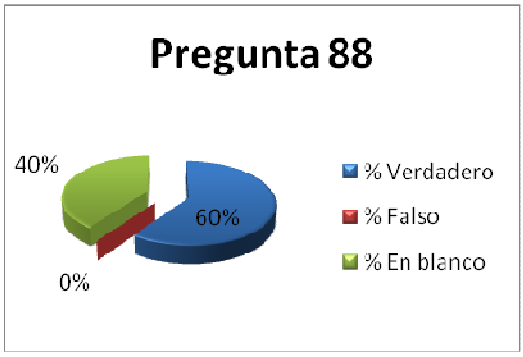
3.1.10.6. Existen controles de seguridad para los resultados de los sistemas

Si Hay [ ]
No hay [x]



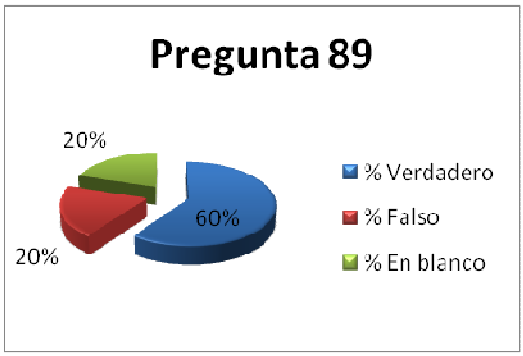
3.1.10.7. Existe la gestión de los cambios en los Sistemas Operativos (S.O.)

Si Hay [x]
No hay [ ]



3.1.10.8. Se controlan las vulnerabilidades de los equipos

Si Hay [x]
No hay [ ]



3.1.11 Administración de Incidentes

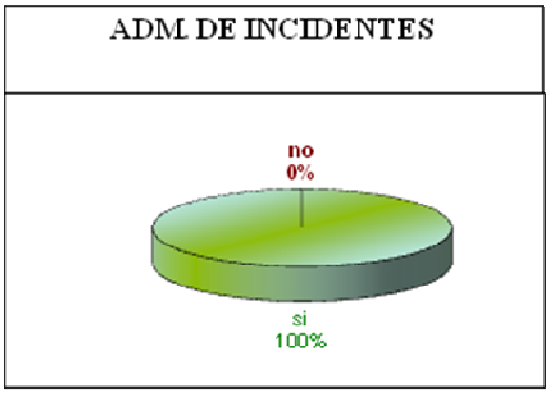
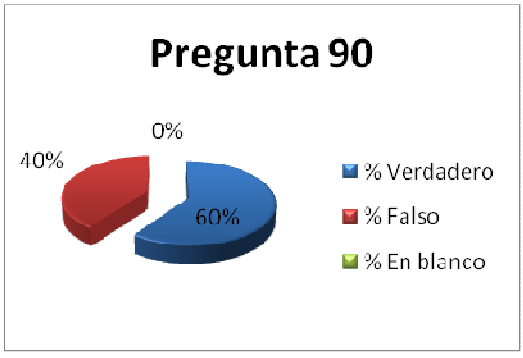


Figura 3.2.11 Resultado del Dominio: Administración de Incidentes

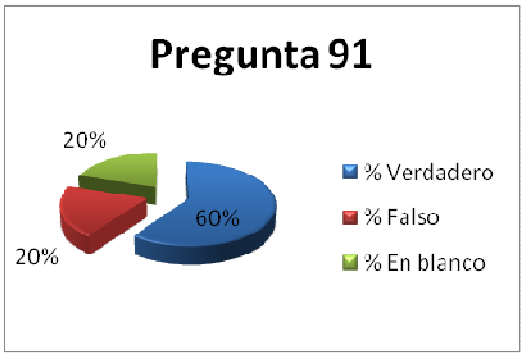
3.1.11.1. Se comunican los eventos de seguridad

Si Hay	X
No hay	



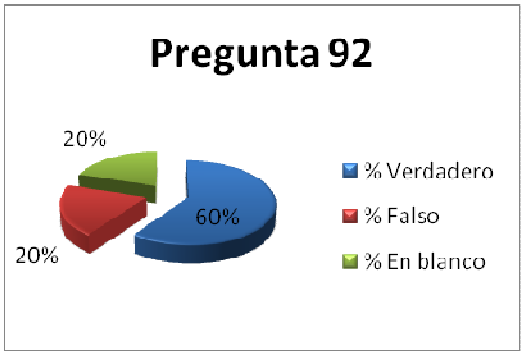
3.1.11.2. Se comunican las debilidades de seguridad

Si Hay	X
No hay	



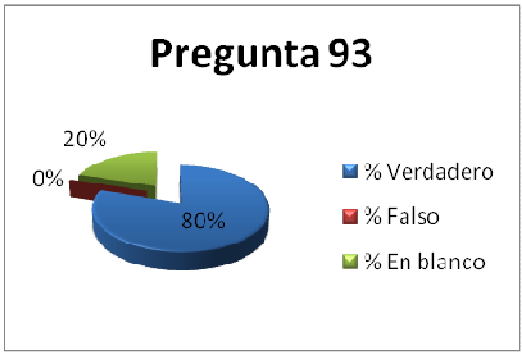
3.1.11.3. Existe definidas las responsabilidades antes de un incidente.

Si Hay [X]
No hay [ ]



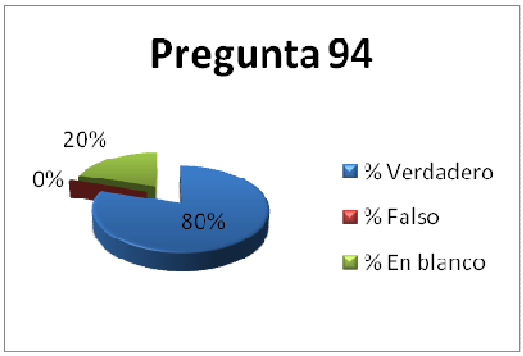
3.1.11.4. Existe un procedimiento formal de respuesta

Si Hay [X]
No hay [ ]



3.1.11.5. Existe la gestión de incidentes

Si Hay	X
No hay	



3.1.12. Gestión de la Continuidad del Negocio

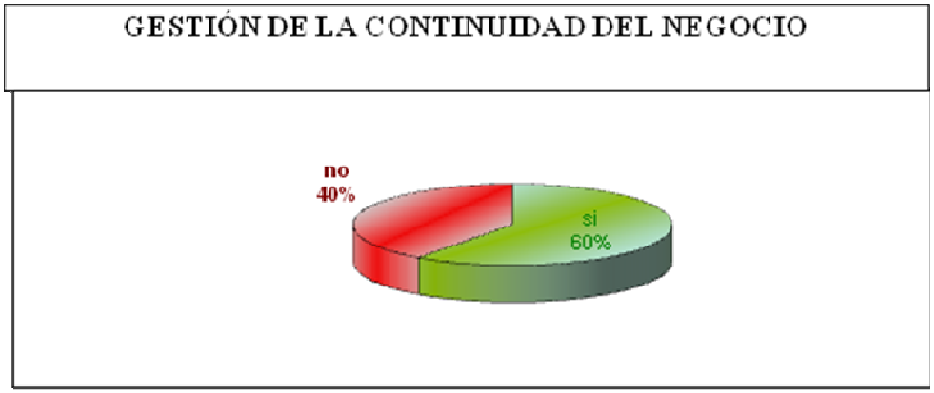
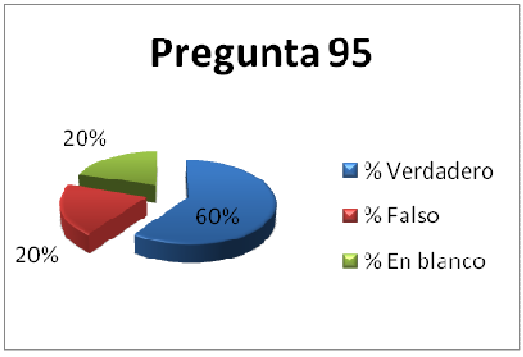


Figura 3.1.12 Resultado del Dominio: Gestión de la Continuidad del Negocio

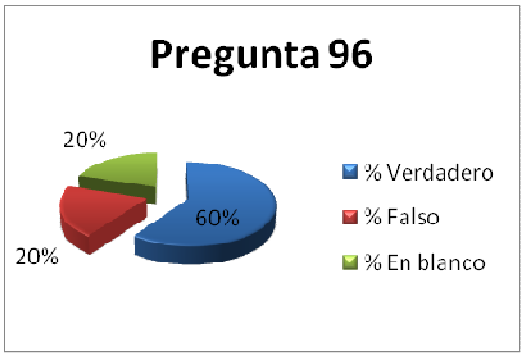
3.1.12.1. Existen procesos para la gestión de la continuidad.

Si Hay	X
No hay	



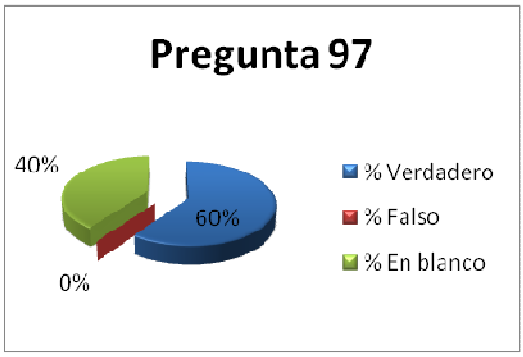
3.1.12. 2. Existe un plan de continuidad del negocio y análisis de impacto

Si Hay	X
No hay	



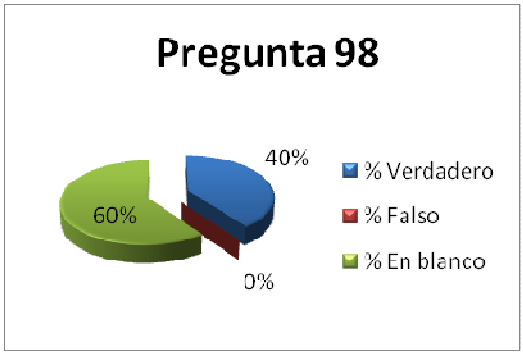
3.1.12.3. Existe un diseño, redacción e implantación de planes de continuidad

Si Hay	X
No hay	



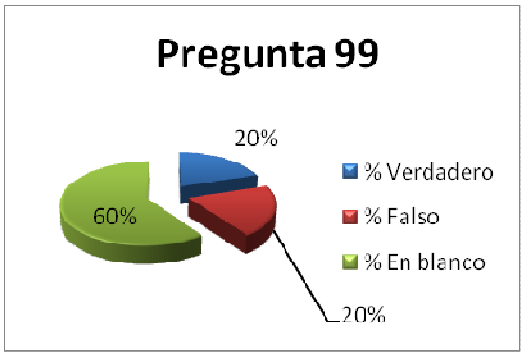
3.1.12.4. Existe un marco de planificación para la continuidad del negocio

Si Hay	
No hay	X



3.1.12.5. Existen prueba, mantenimiento y revisiones de los planes de continuidad del negocio.

Si Hay	
No hay	X



3.1.13 Cumplimiento

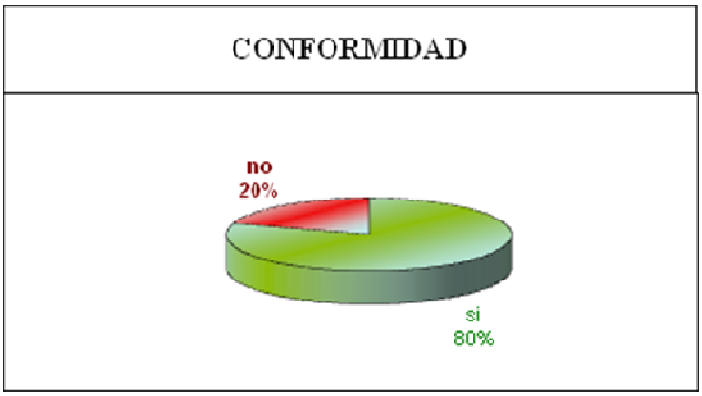
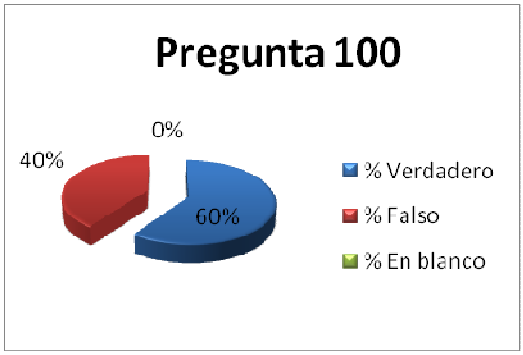


Figura 3.1.13 Resultado del Dominio: Cumplimiento

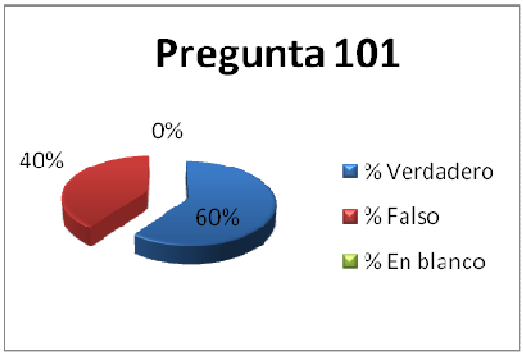
3.1.13.1 Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas

Si Hay	X
No hay	



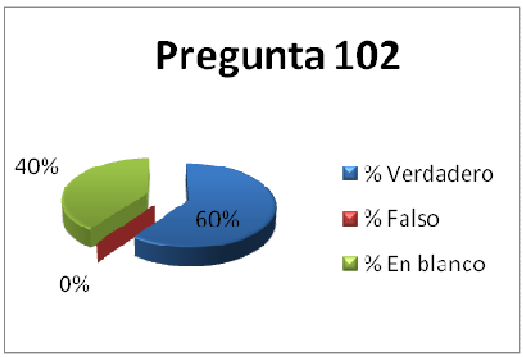
3.1.13.2. Existe el resguardo de la propiedad intelectual.

Si Hay	X
No hay	



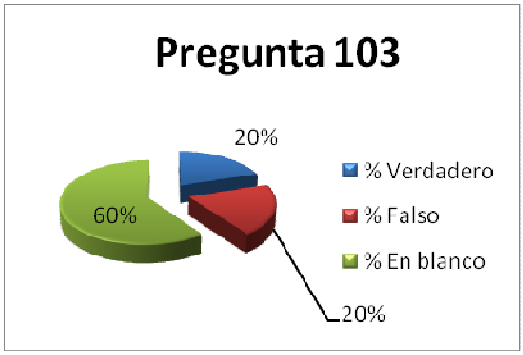
3.1.13.3. Existe el resguardo de los registros de la organización.

Si Hay	X
No hay	



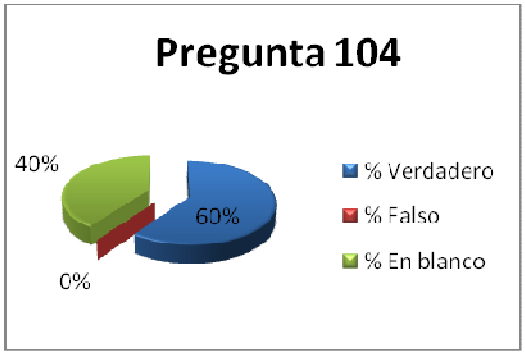
3.1.13.4. Existe una revisión de la política de seguridad y de la conformidad técnica.

Si Hay	
No hay	X



3.1.13.5. Existen consideraciones sobre las auditorías de los sistemas.

Si Hay	X
No hay	



3.2. Clasificación de Activos según MAGERIT

[S] Servicios
○ Acceso Seguro de Usuarios
○ Mensajería Electrónica
○ Archivo histórico central
○ Operaciones de Gestión Interna
• Servicio Técnico Auxiliares
○ Ficheros en Red
○ Acceso a Internet

[SW] Aplicaciones (software)
○ Sistema Banner Nativo
○ Sistema Autoservicios
○ Portal Web
○ Sistema de Base de Datos de Respaldo
○ Sistema de Acceso de Centros de Apoyo
○ Sistema Educativa
○ Espe Medic
○ Activos Fijos
○ Sistema Financiero Olimpo
○ Pedidos
○ WorkFlow
○ Banner Digitalization Document System
• Sistema Académico
○ Presencial
○ MED
○ Idiomas
○ Ciencias Militares
○ Latacunga

[COM] Redes de comunicaciones
○ red LAN

[AUX] Equipamiento auxiliar
○ Proyector Digital
○ Equipo Multimedia

[L] Instalaciones
○ Oficina Principal Área UTIC
○ Oficina ESPE - Digital
○ Cuarto de Servidores - Principal
○ Fibra Óptica

[HW] Equipos informáticos (hardware)
○ Puestos de Trabajo
○ Racks de Piso - Servidores SUN
• Servidores DataCenter
○ Servidor Base de Datos del Sistema ESPE Digital (Banner)
○ Servidor de Respaldo de Base de Datos
○ Servidor Base de Datos Académico
○ Servidor Base de Datos Portal Web Institucional
○ Servidor Base de Datos Portal Web Institucional
○ Servidor Autoservicio (SelfService Banner)
○ Servidor Portal Web (Luminis Service)
○ Servidor Digitalizacion de Documentos (BDMS)
○ Servidor Luminis Seccion De Pruebas
○ Portal Web Institucional
○ Servidor Educativa Respaldos, Aplicaciones Área de Desarrollo
○ Servidor Educativa Respaldos, Aplicaciones Área de Desarrollo
○ Servidor Sistema Financiero Sistema RRHH
○ Servidor Citrix
○ Exchange Administrativos
○ Active Directory Principal Administrativos
○ Active Directory Secundario Administrativos
○ Exchange Alumnos
○ Active Directory Principal Alumnos
○ Servidor Educativa Principal

Tabla 3.2. Clasificación de Activos según MAGERIT

3.3. Diagrama de Utilización de PILAR

Figura 3.3. Diagrama de Utilización de PILAR

3.4. Utilización de la herramienta PILAR 4.4.2.

La herramienta PILAR versión 4.4.2 para Windows XP y versión 4.4.5 para Windows 7, se basa en la metodología MAGERIT para el análisis y gestión de riesgos.

Para el uso de esta herramienta es necesario revisar el manual de PILAR en el que se utiliza en su instalación:

- Actualización de Java
- Licencia Educativa proporcionada por los desarrolladores.

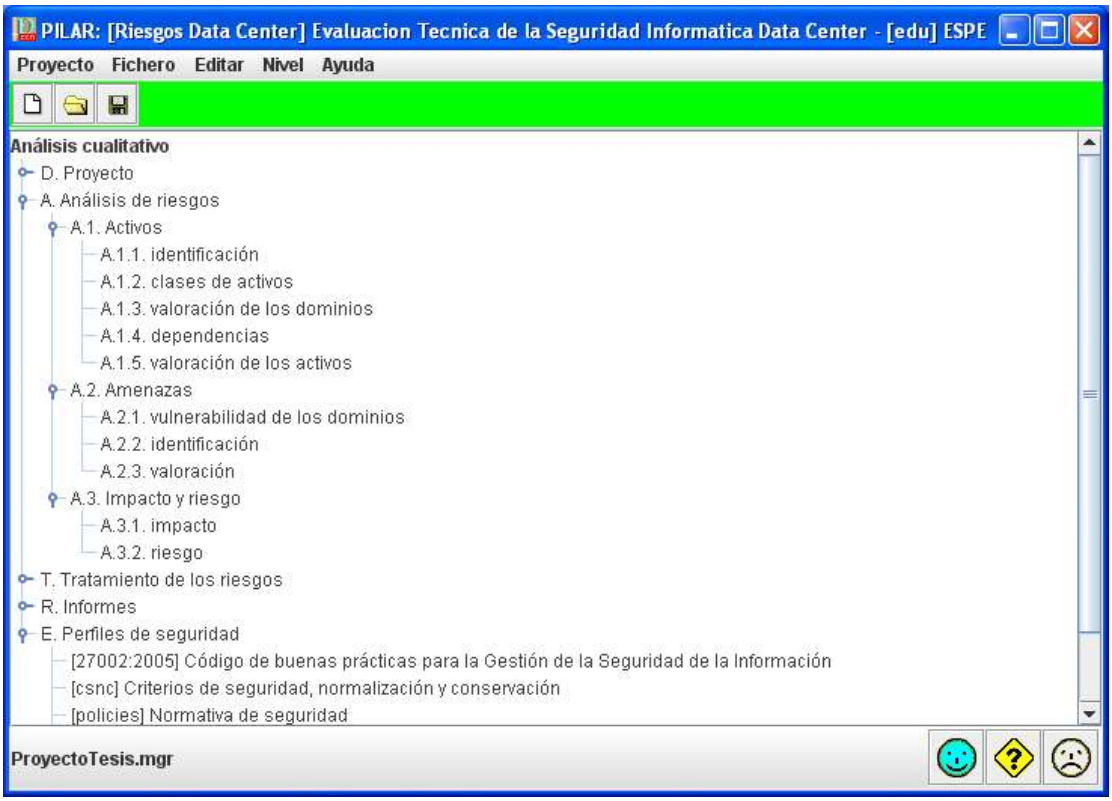


Figura. 3.1. Panel Principal del Proyecto

- **Identificación de Activos:** Dentro de la opción análisis de riesgo, primero se ingresan los activos clasificándolos por su función.

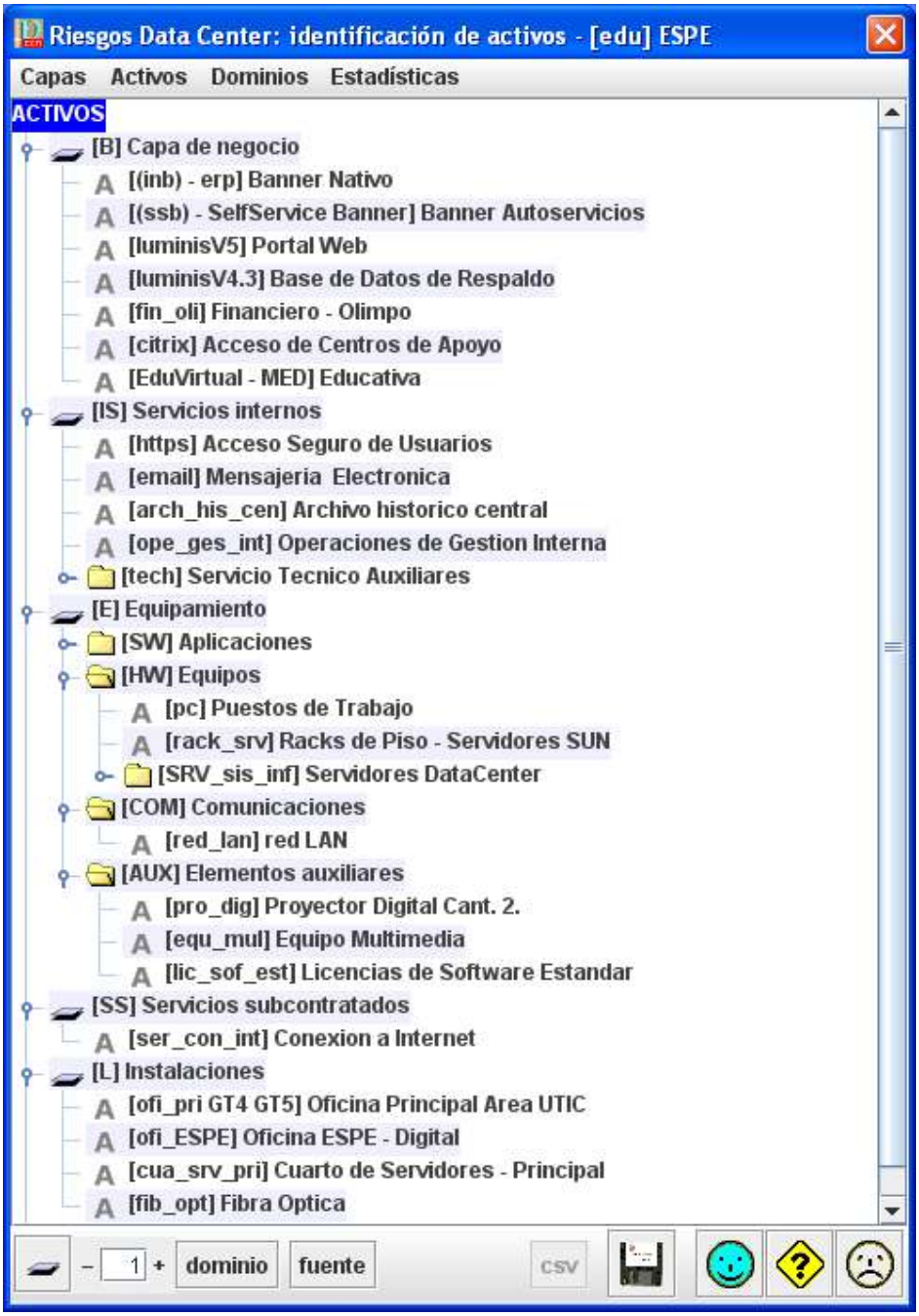


Figura. 3.2. Identificación de Activos

- **Dependencias entre Activos:** Se especifican relaciones entre activos principales de padres a hijos, obteniendo el árbol de activos.

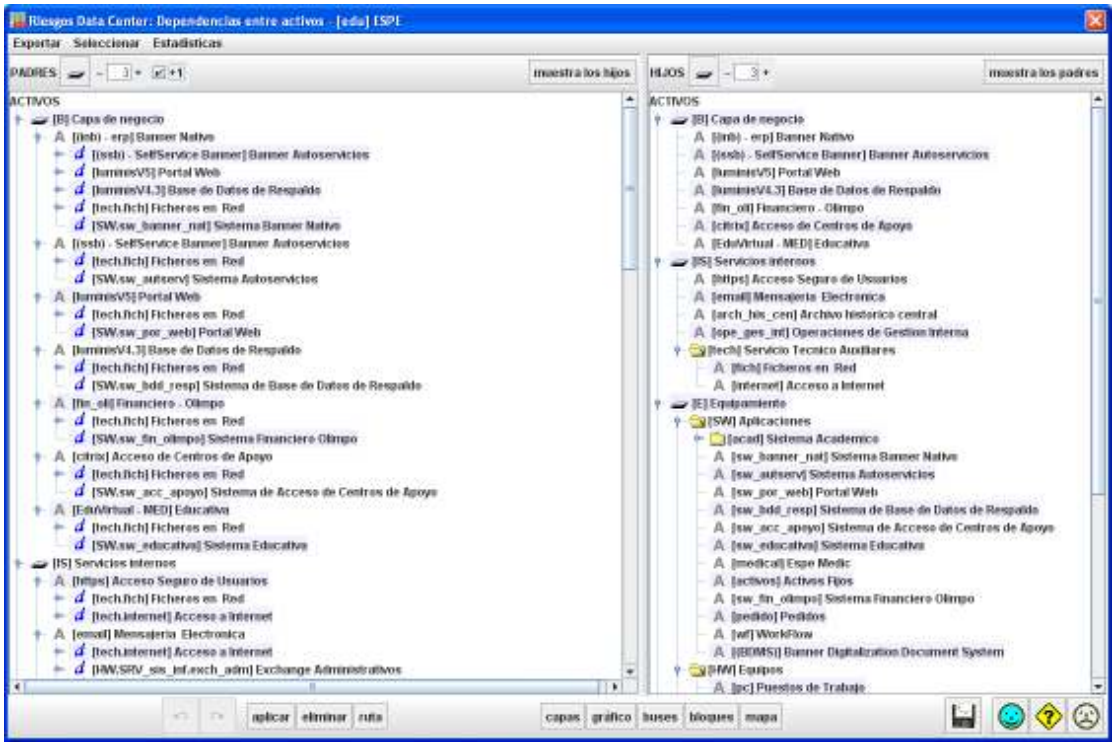


Figura. 3.3. Dependencias entre Activos

- **Valoración de Activos:** Para valorar los activos previamente escogemos el o los niveles, de acuerdo al criterio de valoración entre activos y sus vulnerabilidades reflejados en los pilares.

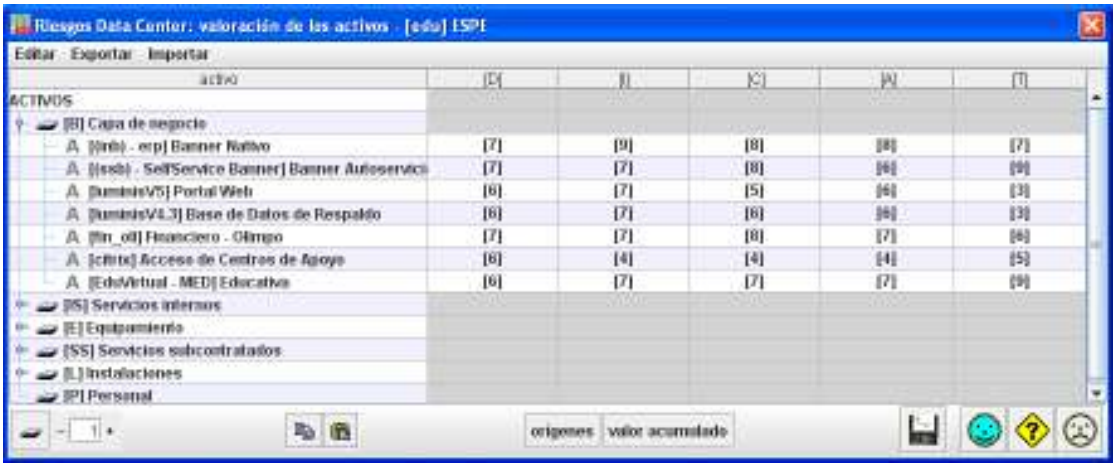


Figura. 3.4. Valoración de Activos

❖ **Identificación de Amenazas:** PILAR recomienda utilizar su biblioteca de amenazas y estas se pueden asociar a cada uno de los activos, tomando en cuenta sus clases y dependencias.

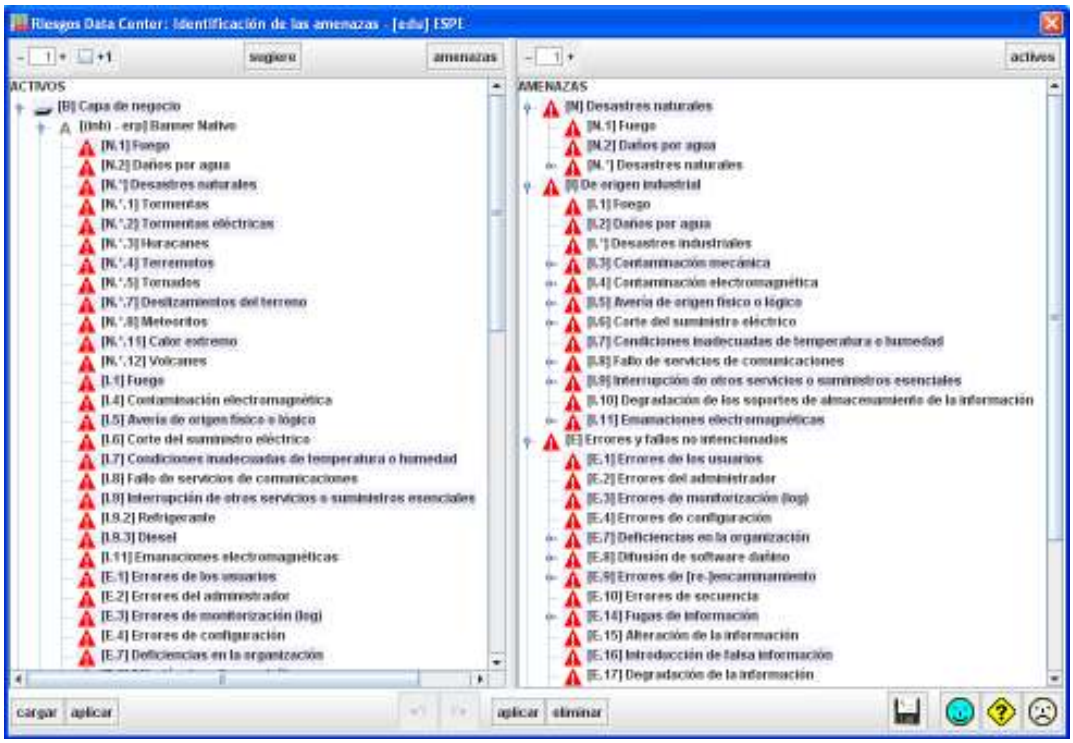


Figura. 3.5. Identificación de Amenazas

❖ **Valoración de Amenazas:** PILAR propone valorar las amenazas definiendo las frecuencias o probabilidad de posible materialización de las mismas y la degradación por niveles o porcentajes de los cinco pilares.

Para el presente proyecto se ha escogido la frecuencia y degradación por porcentaje:

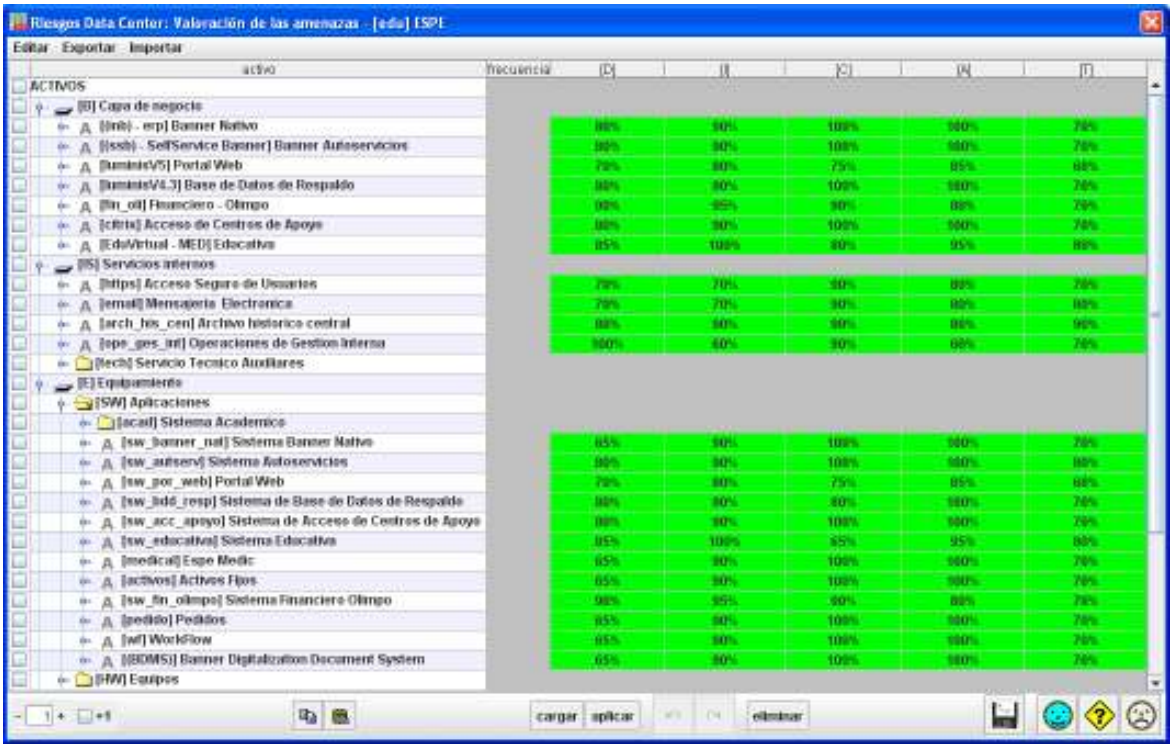


Figura. 3.6. Valoración de Amenazas

- **Impacto Acumulado:** El impacto acumulado es el impacto evaluado en los activos inferiores.

Figura. 3.7. Impacto Acumulado

- **Riesgo Acumulado:** Puesto que hay dependencias entre activos, los activos inferiores acumulan el valor de los activos superiores.

Figura. 3.8. Riesgo Acumulado

- **Identificación y Valoración de Salvaguardas:** Utilizando las sugerencias de la herramienta PILAR, utilizamos la plantilla de salvaguardas, y a continuación la valoración de acuerdo a los siguientes parámetros:

Valoración	**Fases del Proyecto**
L0 = Inexistente	Current = Actual
L1 = Inicial	3m = A 3 meses
L2 = Reproducible e Intuitivo	1y = A 1 año
L3 = Proceso Definido	Target = Objetivo Deseado
L4 = Gestionable y Medible	
L5= Optimizado	

Tabla 3.8. Identificación y Valoración de Salvaguardas

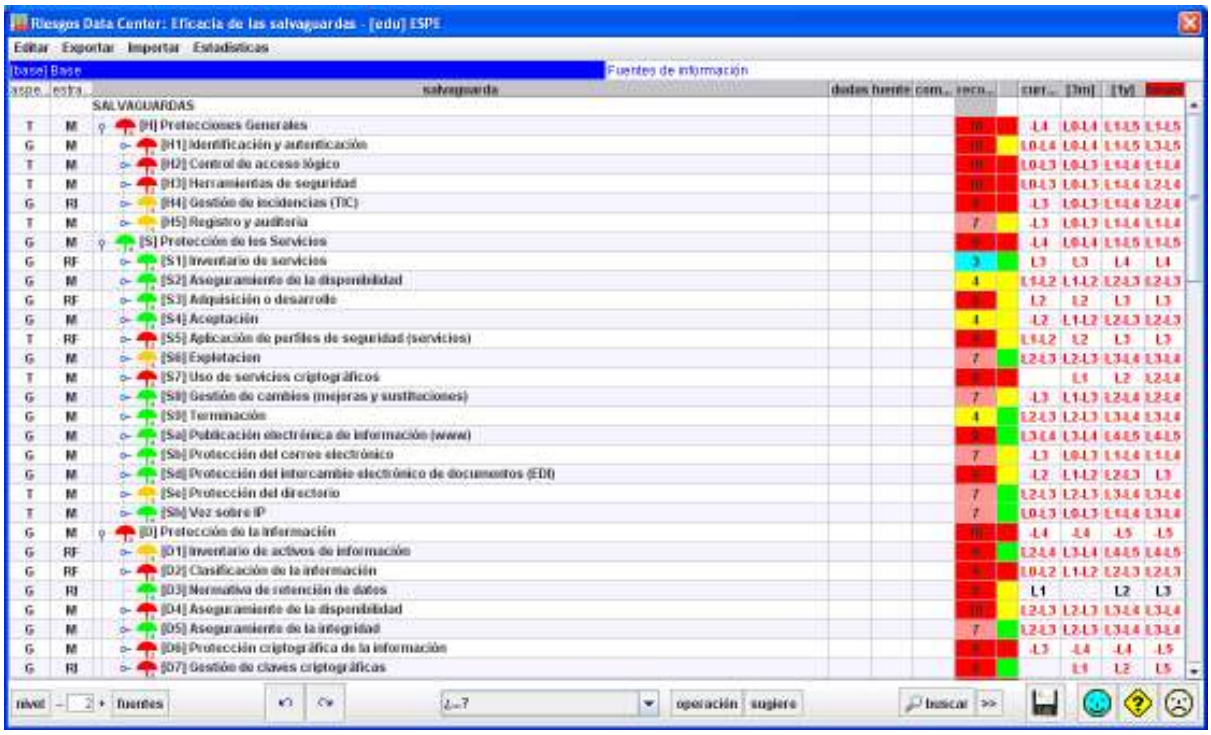


Figura. 3.9. Salvaguardas

- **Riesgo Residual:** Es el riesgo obtenido posterior a la valoración y aplicación de salvaguardas.

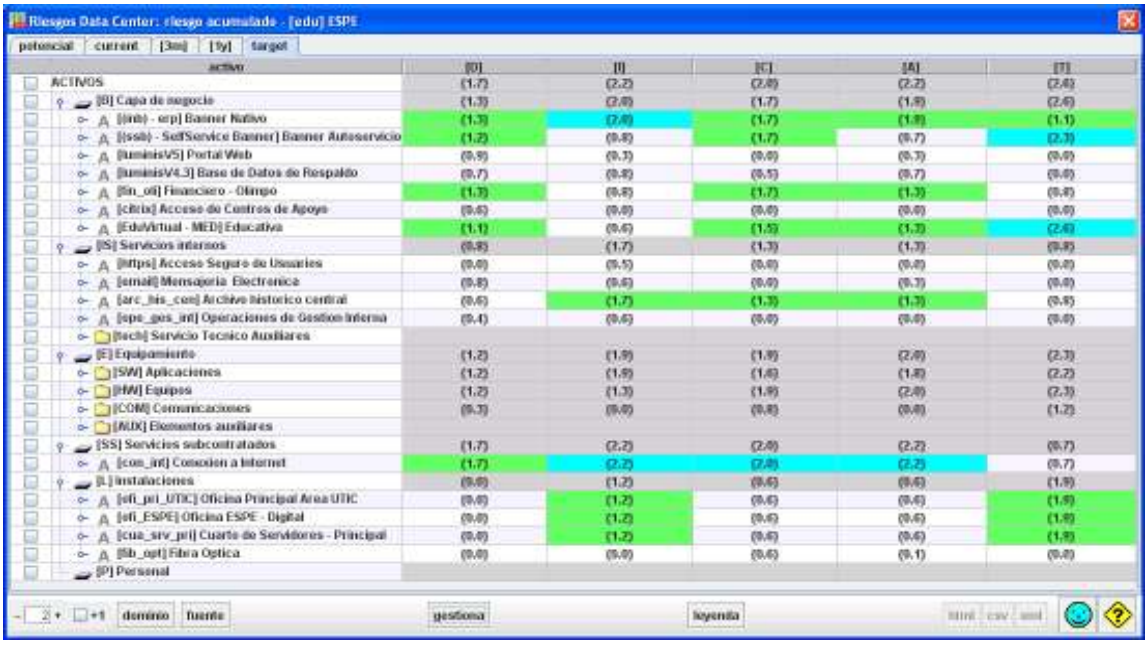


Figura. 3.10. Riesgo Residual

❖ **Grafica de Riesgo Acumulado:**

Los números del 0 al 7 son los niveles de riesgo y se muestran con una barra para cada fase por activo.

Riesgo acumulado: Equivale a los resultados de las fases del proyecto:

- ✓ Potencial: Riesgo que puede ocurrir sin la aplicación de salvaguardas.
- ✓ Current: Riesgo actual aplicando salvaguardas presentes en la organización.
- ✓ 3m: Riesgo residual aplicando salvaguardas a 3 meses.
- ✓ 1y: Riesgo residual aplicando salvaguardas a 1 año.
- ✓ Target: Objetivo deseado aplicando salvaguardas.

CAPA DE NEGOCIO

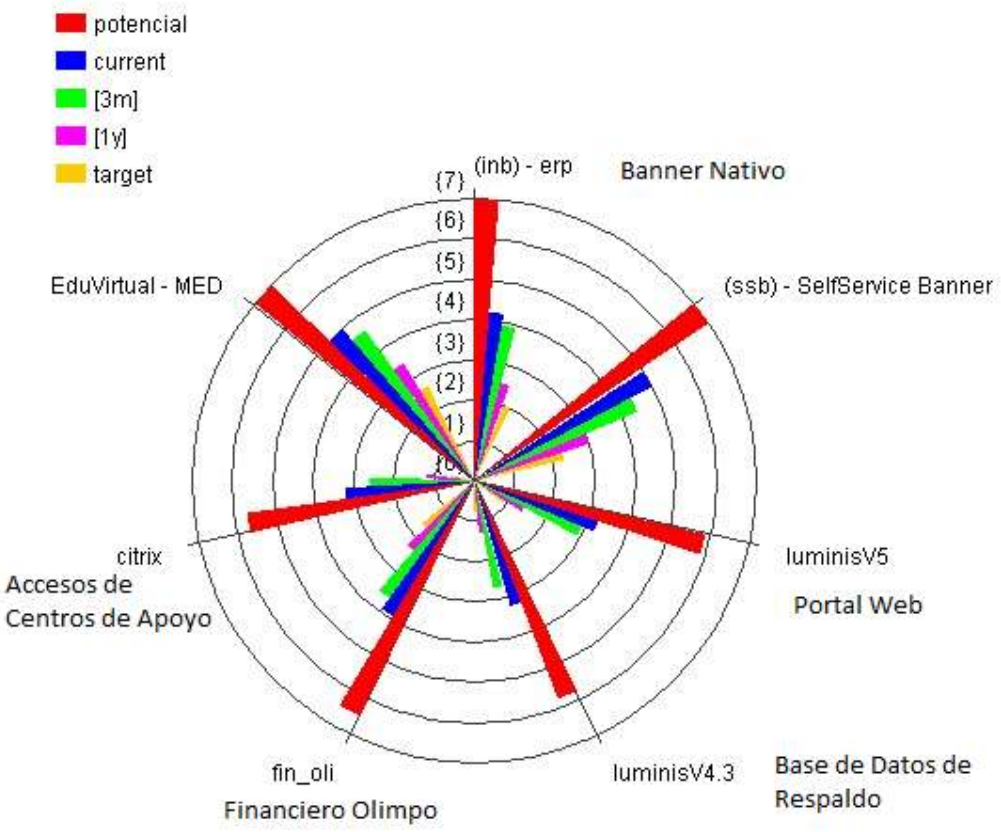


Figura. 3.11: Capa de Negocio

En el siguiente resultado (ver Fig. 3.12), se identifica en el eje de las abscisas la situación de la institución en el tiempo aplicando las salvaguardas y recomendaciones; y en el eje de la ordenada el nivel de seguridad porcentual de 0 a 100.

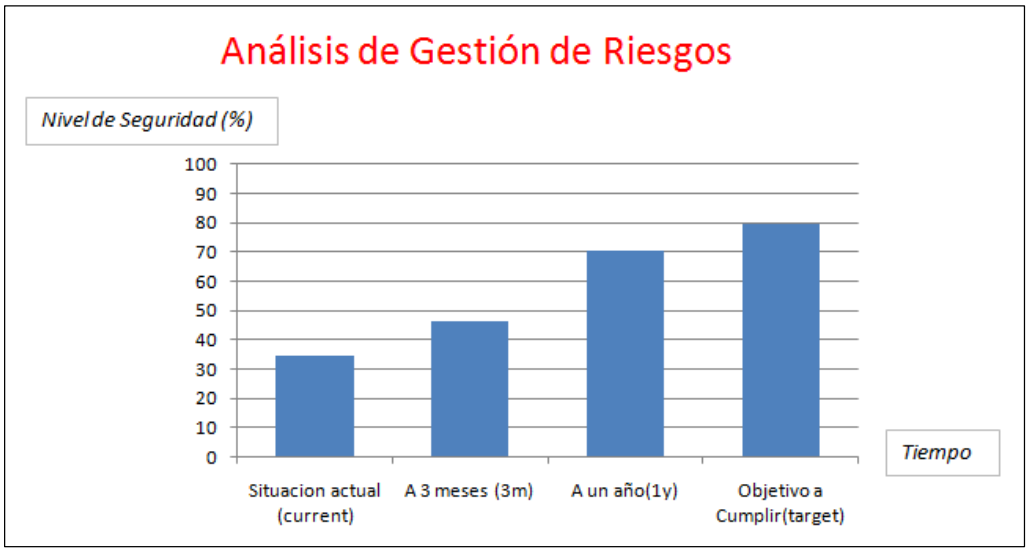


Figura. 3.12. Tiempo al aplicar las salvaguardas de PILAR, para el Análisis de Gestión de Riesgos.

La siguiente figura (ver Fig. 3.13), muestra los resultados de cada control y dominio de seguridad de la Norma ISO 27002, obtenidos en el resultado mediante la información ingresada en la herramienta PILAR:

[27002:2005] CODIGO DE BUENAS PRACTICAS PARA LA GESTION DE LA SEGURIDAD DE LA INFORMACION

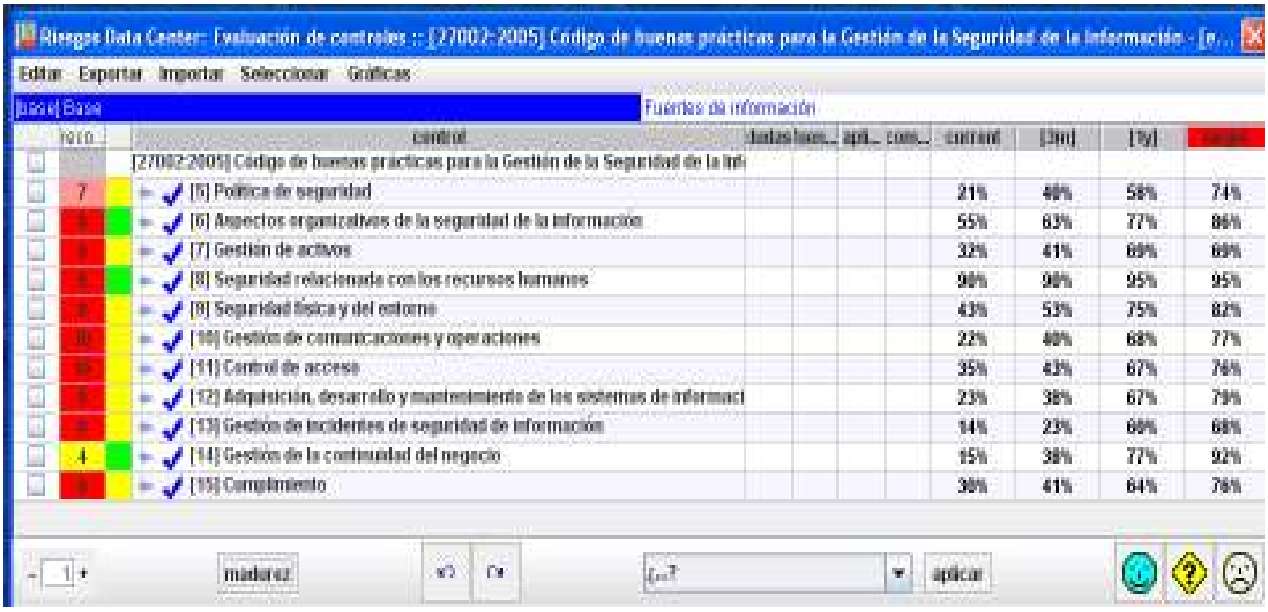


Figura. 3.13. Análisis de Gestión de Riesgos Aplicando Salvaguardas de PILAR

[27002:2005] CODIGO DE BUENAS PRACTICAS PARA LA GESTION DE LA SEGURIDAD DE LA INFORMACION

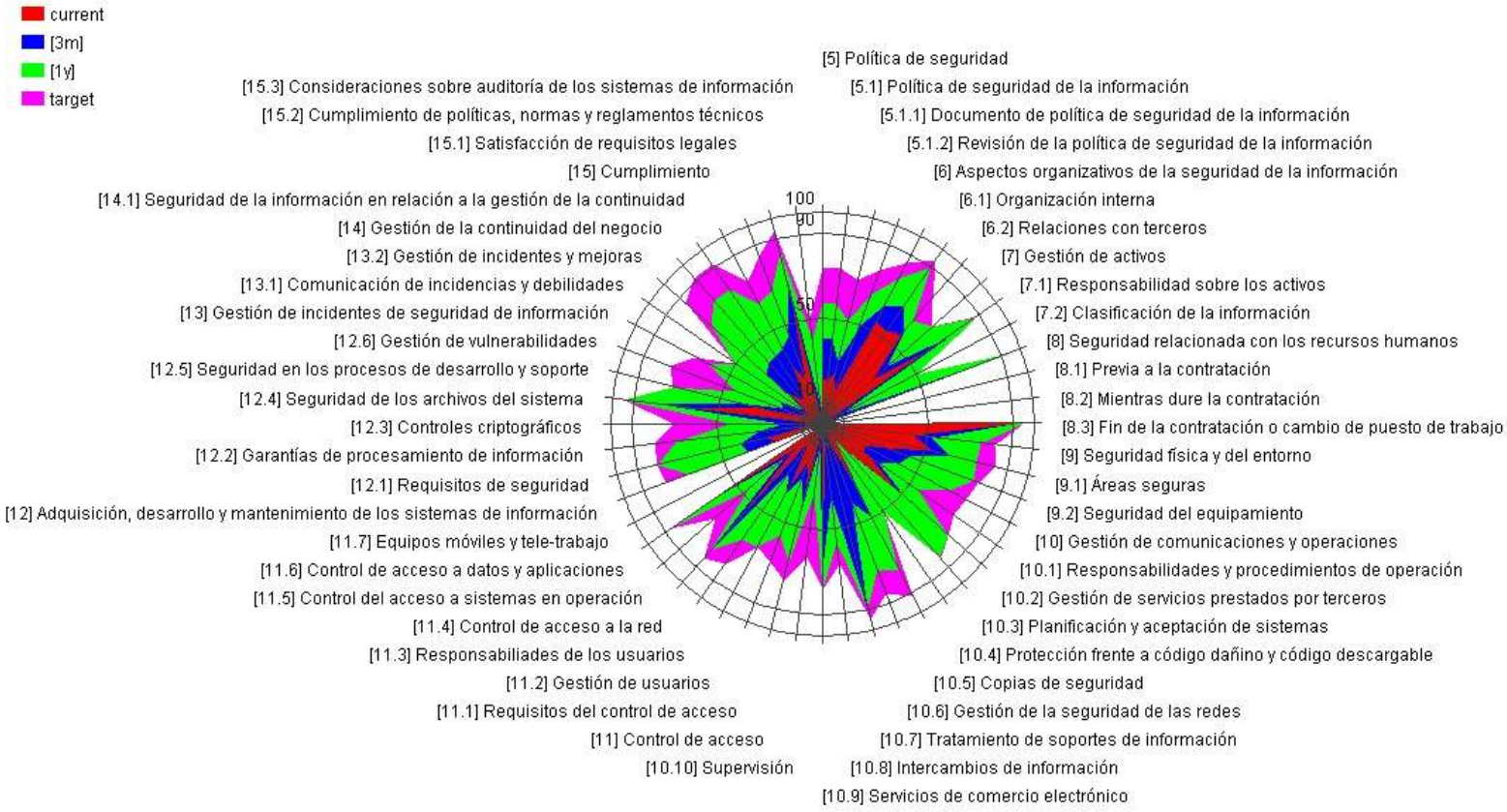


Figura. 3.14. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información

CAPITULO IV

INFORME EJECUTIVO

4.1. Informe Ejecutivo

La Evaluación Técnica de la Seguridad Informática del Data Center de la Escuela Politécnica del Ejercito fue elaborada en base a la información provista por UTIC'S y las observaciones tomadas durante las visitas realizadas al la institución durante los meses de Noviembre 2010 hasta Abril 2011.

Se aplicó la Norma ISO 27004 y los controles de la Norma ISO 27002:2005 e ISO 27001, además la metodología MAGERIT con su herramienta PILAR y mediante un cuestionario de investigación y las observaciones realizadas durante las visitas.

4.1.1 Introducción

Este informe de evaluación de la Seguridad de la Información del Data Center de la ESPE ha sido preparado por estudiantes de la misma como parte del proyecto de Tesis previa la obtención del Título de Grado.

4.1.2 Metodología

Para la elaboración de este informe se tomo como referencia la norma internacional ISO 27002:2005.

La norma ISO 27002 es un estándar para la seguridad de la información que proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

Este estándar está compuesto por once secciones principales o dominios, cada dominio se divide en objetivos de control, los cuales poseen los controles para la seguridad de la información.

La Norma ISO 27004: proporcionó las métricas para la gestión de seguridad de la información. Permitió elaborar las recomendaciones de quién, cuándo y cómo se realizaron mediciones de seguridad de la información

Con la ayuda de la herramienta PILAR se obtuvo las salvaguardas para cada control de la norma ISO 27002, y se tomaron de ellas las más importantes en el presente informe.

4.1.3 Resultados de la Evaluación al Data Center de la Escuela Politécnica del Ejército.

4.1.3.1 Dominio: Política de seguridad

Control: Documento de política de seguridad de la información

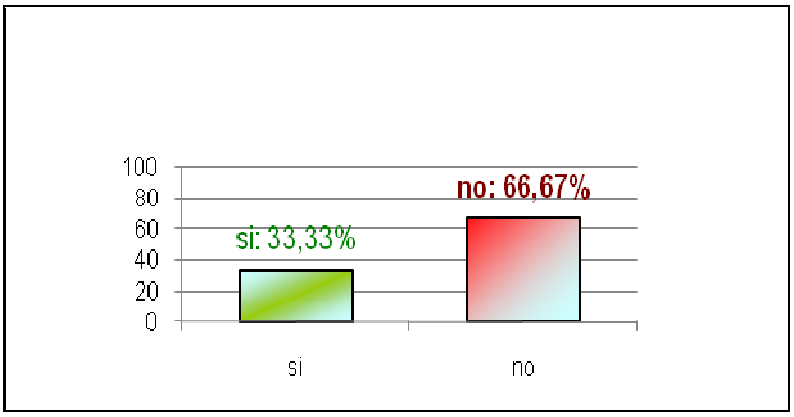


Figura 4.1.3.1 Resultado de la Encuesta: Política de seguridad

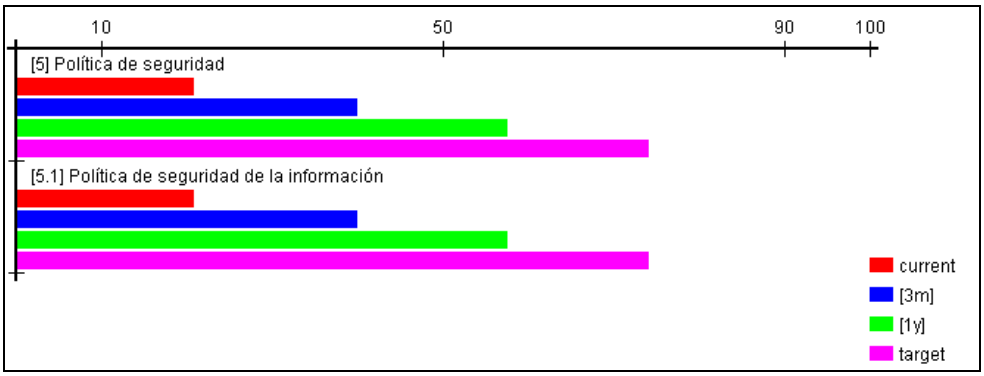


Figura 4.1.3.1 Resultado de la herramienta PILAR: Política de seguridad

Objetivo: La Dirección de la organización debe demostrar apoyo y compromiso con la seguridad de la información, encaminando el establecimiento de una política clara que vaya acorde a los objetivos comerciales para su publicación y mantenimiento.

Observación: Falta de una política de seguridad interna de la institución actualizada.

Condición:

- ✓ No disponen de documentos, normativas, procedimientos y controles de políticas de Seguridad.

Evidencia: Cuestionario de investigación de la Seguridad de la Información, basada en las preguntas de control de la Norma ISO 27004, para el Data Center de la Escuela Politécnica del Ejercito.

Riesgo: Al no tener documentos de políticas de seguridad informática estándar, podría ser probable la materialización de amenazas si no se aplica las respectivas salvaguardas.

Causa:

- Existe un manual de Contingencia en el Data Center de UTIC'S, en el que se indica todos los fallos de los servidores, pero no existe un procedimiento a la seguridad de los Sistemas de Información.

Recomendaciones:

- La Dirección de UTIC'S en conjunto con los jefes de cada área interna del Data Center debe elaborar un manual de políticas de Seguridad, estableciendo objetivos y procedimientos a seguir en materia de Seguridad Informática y actualizarlo.
- La Dirección debe verificar que los controles implantados se cumplan para verificar la efectividad de las políticas de seguridad.

Para ello se recomienda aplicar las siguientes salvaguardas:

Referente a documentos de políticas política de seguridad de la información:

- [G322] El documento de políticas de seguridad debe ser aprobado y respaldado por la Dirección, y posteriormente conocido y aceptado por los afectados.

- [G23] La Documentación de seguridad del sistema debe ser un proceso de revisión definido, considerando todos los posibles cambios que pueden afectar a los riesgos.

Referente a revisión de políticas de seguridad de la información:

- [G344] Debe haber revisiones periódicas del documento de política de seguridad de información y de los procedimientos operativos.

4.1.3.2 Dominio: Aspectos organizativos de la seguridad de la información

Controles:

- **Organización interna**
- **Relaciones con terceros**

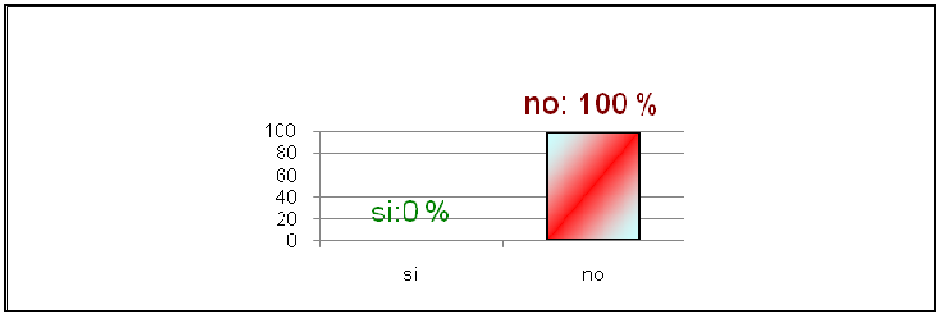


Figura 4.1.3.2 Resultado de la Encuesta: Aspectos Organizativos de la Seguridad de la Información

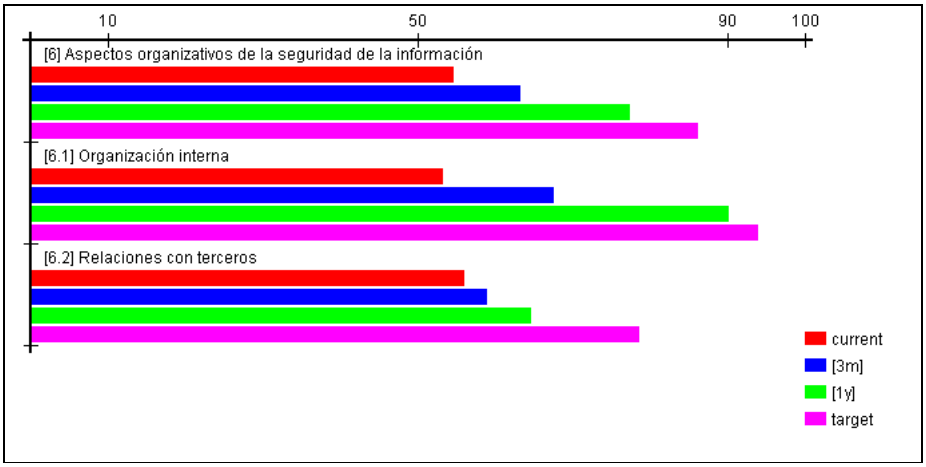


Figura 4.1.3.2 Resultado de la Herramienta PILAR: Aspectos Organizativos de la Seguridad de la Información

Objetivo: Manejar la seguridad de la información dentro de la organización y se requiere un compromiso por parte de la gerencia para apoyar activamente la seguridad dentro de la organización.

La organización en materia de seguridad de la información debe también considerarse respecto a terceros; el objetivo de esto es mantener la seguridad de la información y los medios de procesamiento de información de la organización.

Observación: Falta de mejoramiento interno en la organización en materia de seguridad de la información.

Condición:

- ✓ No existen roles ni responsabilidades bien definidos para las personas implicadas en la seguridad.
- ✓ No existe el compromiso de la dirección con respecto a la seguridad de la información.
- ✓ No existen condiciones contractuales de seguridad con terceros y outsourcing.
- ✓ No existen programas regulares de formación en seguridad para los empleados, clientes y terceros.
- ✓ No existe un acuerdo de confidencialidad a la información que se accede.
- ✓ No se revisa la organización de la seguridad periódicamente por una empresa externa.

Evidencia: Cuestionario de investigación de la Seguridad de la Información, basada en las preguntas de control de la Norma ISO 27004, para el Data Center de la Escuela Politécnica del Ejercito.

Riesgo: Falta de compromiso por parte de la gerencia para apoyar activamente la seguridad dentro y los medios de procesamiento de información de la organización.

Causa:

- En lo que respecta a formación en seguridad únicamente se impartió un curso de seguridad.
- En cuanto al acuerdo de confidencialidad, esto no existe, y lo que existe son documentos los cuales se firmaron para el sistema Banner y sistemas Académicos.

Recomendaciones:

La dirección de UTIC'S debe consolidar las iniciativas de seguridad en conjunto con las demás áreas dando la importancia a este tema e impulsando nuevos proyectos para el mejoramiento de la seguridad de información.

Para ello se recomienda aplicar las siguientes salvaguardas:

Referente al compromiso de la dirección con la seguridad de la información:

- [G111] Debe estar respaldado por la dirección

Referente a la Coordinación de la seguridad de la información:

- [G121] Debe existir una representación de todos los áreas de UTIC'S para tratar de estos temas en la organización.

- [G122] Se debe garantizar que todas las actividades de seguridad se llevan a cabo según la política de seguridad, necesitando ser implantada.

Referente a asignación de responsabilidades relativas a la seguridad de la información:

- [G131] Las responsabilidades en la seguridad de información de las UTIC'S deben ser medibles y gestionables, para la persona que esté a cargo.

- [G142] Se debe asignar responsabilidades al personal para cada activo o proceso de seguridad a personas con un perfil definido en la organización.

Referente a la autorización de recursos para el tratamiento de la información:

- [HWa11] Los nuevos recursos informáticos para las UTIC'S, deben tener la aprobación adecuada, autorizando su propósito, uso correcto y como objetivo llegue a ser un proceso formal.

Referente a los acuerdos de confidencialidad:

- [P52] Se debe actualizar periódicamente los acuerdos de confidencialidad al personal administrativo.

Referente a contacto con las autoridades:

- [G152] Se debe seguir manteniendo relaciones contractuales con los organismos reguladores.

Referente a contacto con grupos de especial interés:

- [G153] Se debe seguir manteniendo contactos con los proveedores de servicios de información.
- [G154] Mantener contactos con los operadores de telecomunicaciones.
- [G155] Participar continuamente en foros de seguridad

Referente a revisiones independientes de la seguridad de la información:

- [G61] Se debe mantener una política de certificación, acreditación y revisiones de seguridad de la información.

- [G62] Se debe elaborar procedimientos de certificación, acreditación y revisiones de seguridad de la información.
- [G632] Se debe realizar revisiones por un auditor y/o empresa especializada e independiente en temas de seguridad de la información.
- [G692] Se debe hacer una evaluación de la seguridad de la información después de realizar cambios significativos.

4.1.3.3 Dominio: Gestión de Activos

Controles:

- **Responsabilidad sobre los activos**
- **Clasificación de la información**

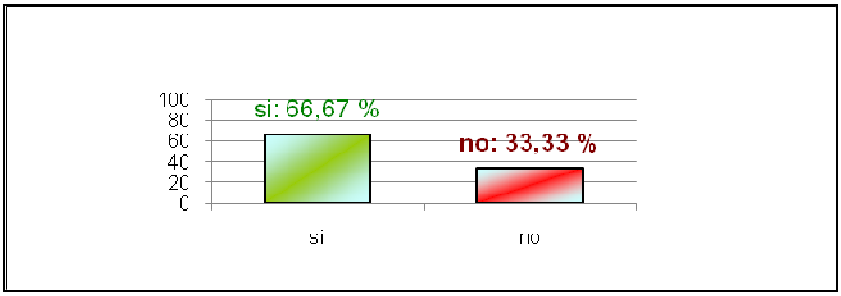


Figura 4.1.3.3 Resultado de la Encuesta: Gestión de Activos

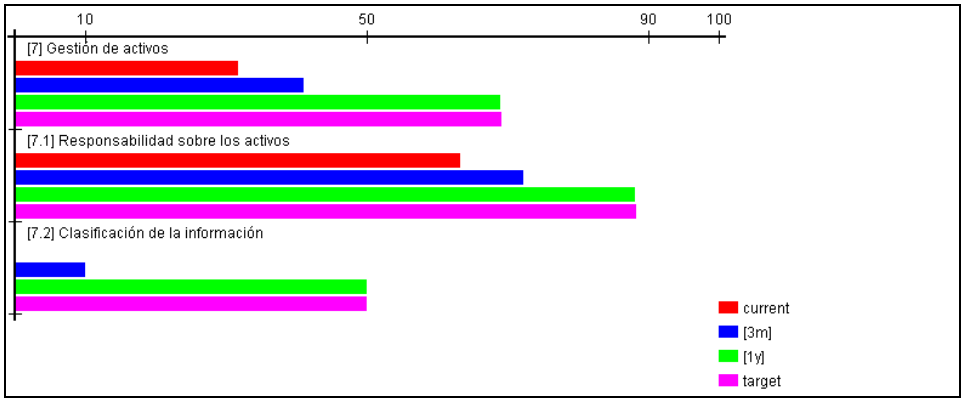


Figura 4.1.3.3 Resultado de la Herramienta PILAR: Gestión de Activos

Objetivo: Asignar responsabilidades por cada uno de los activos de la organización, así como poseer un inventario actualizado de todos los activos

que se tienen, a quien o quienes les pertenecen, el uso que se les debe dar, y la clasificación de todos los activos.

Observación: Falta de un procedimiento de clasificación de la información según la criticidad.

Condición:

- ✓ No disponen de una clasificación de la información según la criticidad de la misma.

Evidencia: Cuestionario de investigación de la Seguridad de la Información, basada en las preguntas de control de la Norma ISO 27004, para el Data Center de la Escuela Politécnica del Ejercito.

Riesgo: El personal podría no responsabilizarse por la pérdida, mal funcionamiento y uso del activo.

Difícil identificación de activos de acuerdo a su criticidad, función y uso.

Causa:

- o No existen responsabilidades sobre los activos bien definidos; se quiere determinar un área específica que administre los activos.
- o Existe documentación de inventario de activos referente a software y equipos actualizada desde Noviembre de 2010, pero referente a datos no hay, y se estima tener actualizada todo en el año 2011.

Recomendaciones:

La elaboración de un inventario de activos es un aspecto importante en la administración de riesgos. La organización debe contar con la capacidad de identificar sus activos y el valor relativo e importancia de los mismos. Sobre la base de esta información, la organización puede entonces, debe asignar niveles de protección proporcionales al valor e importancia de los activos.
Se debe mantener un inventario de los activos importantes asociados a cada sistema de información.
Para ello se recomienda aplicar las siguientes salvaguardas:

Referente a responsabilidad sobre los activos:

- [S14] Se debe asignar e identificar de manera formal al propietario o persona responsable del activo.
- [HW32] Se debe tener un registro de equipos ajenos que ingresen al Data Center.
- [Sb211] Se debe definir políticas de uso aceptable en el marco legal e internas.
- [Sb22] Se debe implantar mecanismos de detección de mala utilización de activos.
- [Sb23] Se debe elaborar y verificar regularmente que se cumplan la políticas de seguridad.
- [Sb242] Se debe formar a los usuarios en la utilización de los servicios, específicamente para el uso correcto, abuso, riesgo, y procedimientos en caso de incidencias.
- [Sb25] Se debe definir procedimientos y medidas disciplinarias en el caso de incumplir con las responsabilidades asignadas.
- [H233] Se debe tener un control de trabajo fuera del horario normal (autorización y supervisión).
- [H235] Se debe restringir el acceso a un número limitado de usuarios.
- [H237] Se debe definir y documentar las autorizaciones de acceso.
- [H238] Se debe desactivar / eliminar las utilidades innecesarias.
- [L21] Se debe tener políticas de protección de las instalaciones.
- [L23] Se debe prohibir equipos de registro para: fotografías, video, audio, telefonía, etc., salvo autorización especial.

Referente a clasificación de la información:

- ✓ [D26] Se debe mantener directrices de clasificación de la información definidas por la organización.

4.1.3.4 Dominio: Seguridad relacionada con los recursos humanos

Controles:

- ✓ **Previa a la contratación**
- ✓ **Mientras dure la contratación**
- ✓ **Fin de la contratación o cambio de puesto de trabajo**

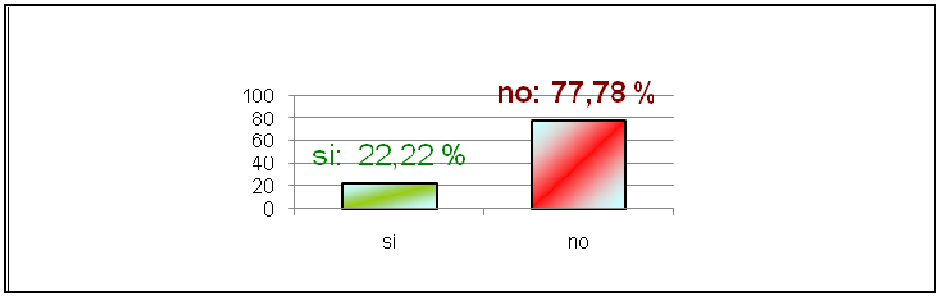


Figura 4.1.3.4 Resultado de la Encuesta: Seguridad relacionada con los recursos humanos

Figura 4.1.3.4 Resultado de la Herramienta PILAR: Seguridad relacionada con los recursos humanos

Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos en los roles para los cuales son considerados, reduciendo el riesgo de robo, fraude y mal uso de los medios. Es necesario definir claramente los roles y responsabilidades de cada empleado.

Observación: Falta de definición de responsabilidades de seguridad para los empleados.

Condición:

- ✓ No están bien definidas las responsabilidades y roles de seguridad, ya que se encuentra en fase de cambio.
- ✓ No se da mucha importancia a la seguridad en la selección y baja del personal.
- ✓ No se recogen los datos de los incidentes de forma detallada.
- ✓ No se informa detalladamente a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades.
- ✓ No existe un proceso disciplinario de la seguridad de la información en la mayoría de áreas de UTIC'S.

Evidencia: Cuestionario de investigación de la Seguridad de la Información, basada en las preguntas de control de la Norma ISO 27004, para el Data Center de la Escuela Politécnica del Ejercito.

Riesgos:

Alto riesgo de falla humana, robo, fraude proclive al mal uso de las instalaciones.

Puede ocurrir que el empleado en cuestión no realice la devolución completa de los activos a su cargo incluyendo información y la terminación de sus funciones no se lo haga de manera ordenada sin la correcta comunicación del hecho.

Causa:

- o Referente a responsabilidades y roles de seguridad se encuentran en fase de cambio.
- o En cuanto a incidentes de seguridad si existe un canal y procedimiento pero se quiere automatizar para que dichos procedimientos lo hagan auditores externos o internos.
- o Necesidad de un mejoramiento en la comunicación con todas las áreas de UTIC'S en cuanto a vulnerabilidades observadas o sospechadas.

Recomendaciones:

La comunicación de las responsabilidades de terminación deben incluir requerimientos de seguridad constantes y responsabilidades legales y, cuando sea apropiado, las responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad y los términos y condiciones de empleo continuando durante un período después de terminado el empleo del usuario empleado, contratista o tercera persona.

Mantener responsabilidades aún válidas después de la terminación del empleo, que deben estar contenidas en los contratos del empleado, contratista o tercera persona.

Para ello se recomienda aplicar las siguientes salvaguardas:

Referente a contrataciones:

- [P43] Se debe asignar responsabilidades de seguridad a todos los puestos de trabajo.
- [P7] Se debe formar y capacitar en seguridad de la información a todas las contrataciones que se haga.

En cuanto al fin de la contratación o cambio de puesto de trabajo se recomienda:

- [P6263] Se debe comunicar la baja a los responsables de seguridad, y administradores del sistema.
- [P6262] Se debe dar pronta recuperación de elementos de seguridad como: llaves, tarjetas, etc.…
- [H25d] Se debe cancelar los privilegios de acceso.

4.1.3.5 Dominio: Seguridad Física y del Entorno

Controles:

- ✓ **Áreas seguras**
- ✓ **Seguridad del equipamiento**

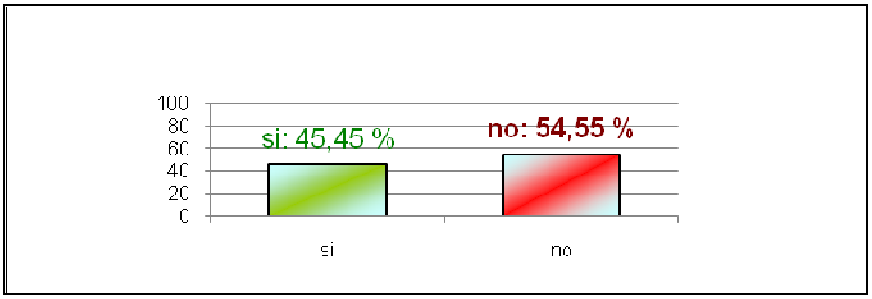


Figura 4.1.3.5 Resultado de la Encuesta: Seguridad Física y del Entorno

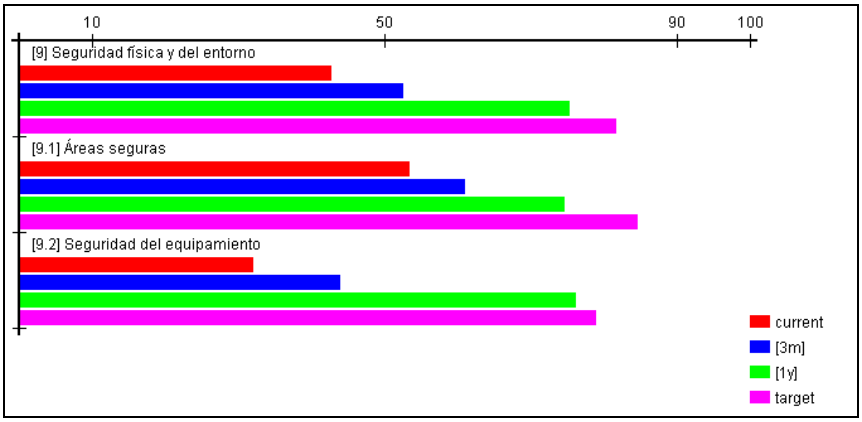


Figura 4.1.3.5 Resultado de la Herramienta PILAR: Seguridad Física y del Entorno

Objetivo: Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización. Las instalaciones de procesamiento de información sensible deben ubicarse en áreas seguras y protegidas dentro de un perímetro de seguridad definido por adecuadas barreras y controles de entrada.

Observación: Falta de un perímetro de seguridad física para las áreas de UTIC'S.

Condición:

- ✓ Únicamente existe una puerta para el acceso al Data Center en horarios de trabajo.
- ✓ En las áreas seguras no existen controles adicionales al personal propio y ajeno.
- ✓ Las áreas de carga y expedición no están aisladas de las áreas de Sistemas de Información.
- ✓ La ubicación de los equipos no impide minimizar accesos innecesarios.
- ✓ No se asegura la disponibilidad e integridad de todos los equipos en la mayoría de las áreas.
- ✓ No existe un procedimiento de seguridad para los equipos retirados o ubicados exteriormente.
- ✓ No se incluye la seguridad en equipos móviles.

Evidencia: Cuestionario de investigación de la Seguridad de la Información, basada en las preguntas de control de la Norma ISO 27004, para el Data Center de la Escuela Politécnica del Ejercito.

Riesgos:

Ingreso no autorizado por parte de terceros y trabajo de terceras personas no supervisado dentro de las áreas protegidas que pueden provocar la realización de actividades malintencionadas.

Interrupción del funcionamiento de los recursos de procesamiento de la información por la falta de suministro eléctrico.

La información puede verse comprometida por una utilización descuidada o mala reutilización del equipamiento.

Causa:

Existe una puerta de seguridad para acceder al Data Center, pero las áreas internas como: GT1, GT2, GT3 Y GT4, no tienen controles de entrada frente al acceso de personal no autorizado.

No existen controles adicionales para el personal propio o ajeno que ingresa.

En cuanto a las áreas de carga y expedición:

- En lo que respecta aislamiento de carga del área de redes (GT3) no existe.
- Y en el área de Sistemas de Información (GT4) se tiene aislamiento de carga, sin embargo no existe un área de pruebas general.

En lo que se refiere a un responsable directo que controle accesos innecesarios, el procedimiento se encuentra en un proceso de readecuación y se desea aplicar la Norma 942, la cual menciona una serie de procedimientos seguros para los equipos.

En cuanto a fallos en la alimentación eléctrica:

Existen protecciones pero no funcionan por las siguientes razones:

- La planta eléctrica tiene fallos, por lo cual se menciona que al variar los voltajes, afectan a los servidores y por ende los servicios.

- Se va a tener un generador únicamente para el Data Center.

En cuanto a seguridad en el cableado frente a daños e intercepciones existen problemas en la administración de las redes, pese a que el cableado es certificado (backbone), es decir las principales conexiones troncales de Internet están con las normas pertinentes.

En cuanto a la disponibilidad e integridad de todos los equipos:

- No se cumple la disponibilidad de los equipos a pesar de tener contratos de mantenimiento con empresas.
- Para el año 2011 se desean homogeneidad de marcas.

Recomendaciones:

Se recomienda mejorar los accesos de seguridad a todas las áreas del Data Center, y mantener supervisión de las personas que realizan cualquier actividad dentro de la misma.

Se debe tener un registro de usuarios empleados, contratistas y terceras personas que tienen la autoridad para permitir el retiro de los activos fuera de las áreas de UTIC'S y deben estar claramente identificados.

Se recomienda realizar revisiones periódicas para localizar a tiempo dispositivos de grabación no-autorizados, armas, etc., y evitar su ingreso al Data Center.

En cuanto a las áreas de carga y expedición se recomienda tener un área de prueba general.

En lo que tiene que ver a fallos en la alimentación eléctrica se sugiere mantener comunicaciones con las autoridades para que deleguen a los responsables de la planta eléctrica de la Escuela Politécnica del Ejército, los mantenimientos necesarios para evitar fallos que afecten a los equipos

Respecto a seguridad en el cableado tomar medidas de seguridad respectivas frente a daños e intercepciones regularizando mantenimientos cada tres meses.

Para ello se recomienda aplicar las siguientes salvaguardas:

Referente a controles físicos de entrada:

- [L51a] Se debe tener salidas de emergencia que garanticen el acceso del personal autorizado.
- [L522] Se debe comprobar la identidad de las visitas.
- [L524] Se recomienda que las visitas al Data Center tengan escolta y monitorización de las actividades (visitas acompañadas).
- [L531] Se debe usar un pase (ej. tarjeta) en el interior del Data Center.
- [L569] Se debe realizar auditorías periódicas del inventario de llaves, combinaciones o dispositivos de seguridad en las áreas seguras.

Referente a protección frente a amenazas externas:

- [L92d] Debe existir una revisión periódica de las instalaciones por los bomberos o personal especializado.
- [L92j] Frente a desastres naturales o industriales se debe realizar simulacros internos para minimizar el riesgo.
- [L931] Se debe tener un procedimiento de emergencia normado por instituciones externas de seguridad.
- [L973] Es necesario tener medios técnicos para la detección de metales y explosivos.
- [L98] Se debe mantener vigente la póliza de seguros frente a robo, incendio y daños.

Referente a la ubicación y protección de los equipos

- [L925] Se debe habilitar vías de evacuación en el caso de incendios.
- [L928] Se debe tener medios manuales de extinción de incendios (extintores portátiles, hidrantes.).

Los extintores deben ser asignados para los equipos, CO2 para servidores y Pc's, y polvo químico para archiveros de documentos.

- [L929] Se debe tener un sistema automático de extinción de incendios (sprinkler, etc.), que notifique de manera automática a los servicios de ayuda exterior.
- [L92b] Se debe tener un plan de mantenimiento y verificación de los dispositivos y los sistemas contra incendios.
- [L92d] Se debe hacer revisiones periódicas de las instalaciones por los bomberos o personal especializado y tener señalización como: planos de evacuación, de planta, etc.
- [L92i] Se sugiere elaborar un plan interno de autoprotección de los activos.
- [L92j] Se debe hacer simulacros internos de los eventos de incendio supervisado por personal experto.

- [L931] En cuanto a inundaciones se necesita tener un procedimiento de emergencia, pruebas y revisión del procedimiento.

- [L935] Se debe tener un sistema de detección y evacuación de agua habilitado.

Referente a suministros eléctricos y climatización

- [AUX464] Se recomienda mantener los UPS en paralelo para redundancia en la alimentación para tener el suministro eléctrico continuo y hacer revisiones de los controles de temperatura periódicamente, y también un sistema de climatización redundante.

Referente a Seguridad del cableado:

- [AUX61] Para tener una administración adecuada se sugiere mantener una gestión centralizada del cableado y utilizar herramientas de gestión para la misma.

Referente a Mantenimiento de Equipos.

- [HWbc] Se debe mantener un plan de continuidad actualizado para hardware.
- [HWa44] Se recomienda aplicar siempre una normativa de uso de equipos fuera de las instalaciones.
- [HWa46] Mantener una póliza de seguro para los equipos fuera de su lugar de trabajo.

Con respecto a retirada o reutilización de equipos que pasan a otro usuario.

- [HWc] Se debe tener una norma actualizada de terminación de equipos y mantener actualizaciones de los planes de continuidad.

4.1.3.6 Dominio: Gestión de comunicaciones y operaciones

Controles:

- ✓ **Responsabilidades y procedimientos de operación**
- ✓ **Gestión de servicios prestados por terceros.**
- ✓ **Planificación y aceptación de sistemas**

- ✓ **Protección frente a código dañino y código descargable**
- ✓ **Copias de seguridad**
- ✓ **Gestión de la seguridad de las redes**
- ✓ **Tratamiento de soportes de información**
- ✓ **Intercambios de información**
- ✓ **Servicios de comercio electrónico**
- ✓ **Supervisión**

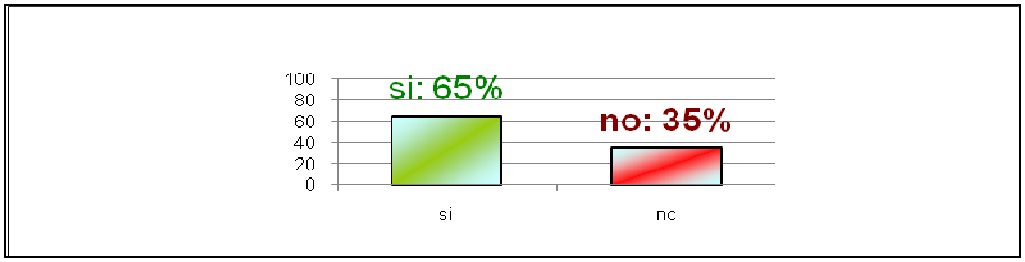


Figura 4.1.3.6 Resultado de la Encuesta: Gestión de comunicaciones y operaciones.

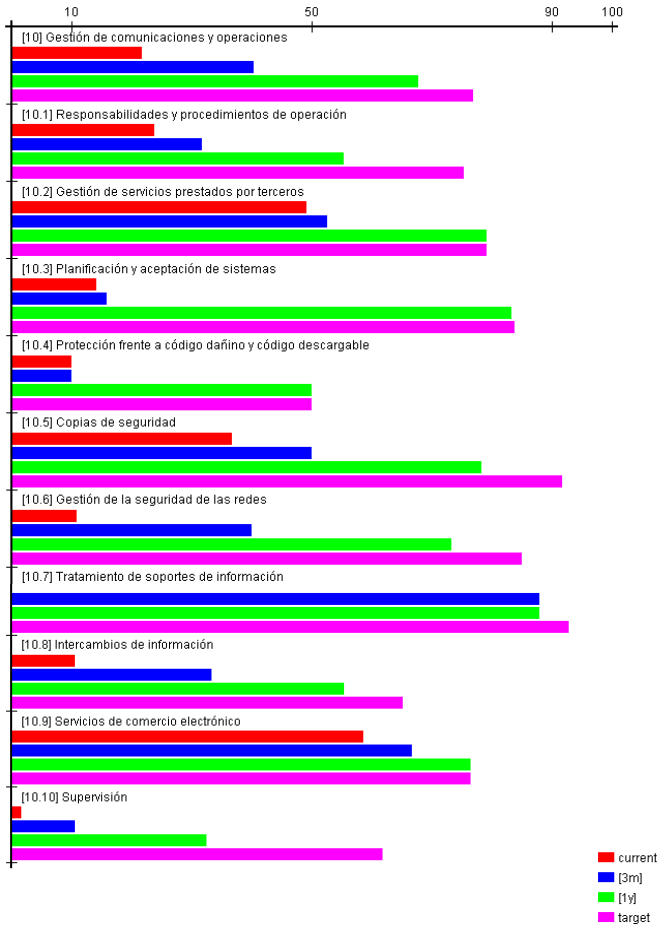


Figura 4.1.3.6 Resultado de la Herramienta PILAR: Gestión de Comunicaciones y Operaciones.

Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información, es decir que los procedimientos de operación estén bien documentados.

Observación:
Falta de documentación de los procedimientos de operación, controles de gestión de comunicaciones y operaciones que garanticen la integridad y el funcionamiento de los sistemas, así como las responsabilidades que deben ser formalmente establecidas.

Condición:

- ✓ Falta documentación respecto a los procesos de operación del Data Center
- ✓ No están establecidas las responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad
- ✓ Los medios informáticos eliminados podrían disponer de información sensible
- ✓ No existen acuerdos para intercambio de información y software
- ✓ No existen medidas de seguridad de los medios en el tránsito
- ✓ Falta establecer e implantar medidas para proteger la confidencialidad e integridad de información publicada.
- ✓ Faltan medidas de seguridad en las transacciones en línea

Evidencia: Cuestionario de investigación de la Seguridad de la Información, basada en las preguntas de control de la Norma ISO 27004, para el Data Center de la Escuela Politécnica del Ejercito.

Riesgos:
Cese del funcionamiento de los sistemas críticos de la institución
Cambios no autorizados en el sistema o en los recursos de tratamiento de la información que comprometan la integridad y seguridad de los mismos.

Uso negligente o mal uso deliberado del sistema
Compromiso, daño o pérdida de recursos de información
Fallos en los sistemas, que comprometan las actividades críticas de la organización.
Ejecución de códigos móviles no autorizados que atenten contra la seguridad.
Pérdida total o parcial de la información critica de la institución
Accesos no autorizados, mal uso o corrupción de la información

Causa:

- No todos los procedimientos operativos están documentados, únicamente hojas de servicio.
- Frente a incidentes de seguridad: se desearía tener un comité de riesgo.
- Se necesita cambiar en Sistemas de Información, las macros a sistemas Web, en este caso UTIC'S evalúa los Sistemas de Información, mientras que las actualizaciones necesarias dependerían de los usuarios que lo necesiten.

UTIC'S desea estabilizarse en los productos que realiza Banner.

Con respecto a las auditorias:

- A nivel de base de datos si habido auditorias pero no a los sistemas operativos.
- El área de GT3 (redes) tuvo auditoria pero no del tipo informático, GT4 (Sistemas de información) si tuvo auditoria informático.
- En el sistema antiguo no existió seguridad tampoco a nivel del usuario. En el nuevo sistema si existe seguridad por medio de la empresa externa Sanga, mientras su documentación está en ingles por lo que este documento se demora en la traducción.
- Referente a las medidas de seguridad en integridad y confidencialidad de información publicada Se ha intentado implementar, en lo que se refiere a confidencialidad si lo hay, pero en lo que respecta a integridad no.

Recomendaciones:

Documentar todos los procedimientos operativos y de gestión de los sistemas de información, e implementar medidas de seguridad para la integridad y confidencialidad de la información.

Para ello se recomienda aplicar las siguientes salvaguardas:

- ✓ **Referente a Responsabilidades y procedimientos de operación**

Con respecto documentación de los procedimientos de operación:

[G3412] Se debe bloquear la pantalla mediante salvapantallas con contraseña.

[G3413] Se debe mantener bloqueo o cierre de sesión

Custodia de portátiles y documentos en lugar seguro

[G342] Se debe tener guías para las funciones ordinarias de los empleados, guías para situaciones excepcionales y revisión periódica de los procedimientos operativos.

Con respecto a Gestión de cambios:

[SWb1] Mantener un seguimiento permanente de actualizaciones y parches (SW)

[SWb2] Realizar la evaluación del impacto potencial del cambio (servicios, confidencialidad integridad monitorización de los datos)

[SWb3] Minimizar interrupciones del servicio mediante la definición del proceso de cambio

Controlar versiones de toda actualización del software, hardware y comunicaciones.

Mantener un registro de toda actualización de software, hardware y comunicaciones.

Mantener archivos de documentación y actualización de todos los cambios del software, hardware y comunicaciones

Actualización de todos los procedimientos de explotación afectados y de los planes de continuidad.

Con respecto a segregación de tareas en seguridad:

Se debe documentar la segregación de tareas en roles y especialmente realizar Auditorías de Seguridad.

Con respecto al control de la efectividad de la estructura de segregación:

[H2421] Se debe prevenir la modificación de datos de producción por los operadores y el inicio de transacciones.

[H2424] Se debe restringir el acceso a las aplicaciones

[H2425] Mantener control de acceso a la consola de logs

[H2426] Se debe revisar los periodos de vacaciones previstos de los operadores y programadores

[H2428] Se debe asegurar que en todo momento haya más de un operador

[H243] Se debe llevar un registro de las operaciones.

[10.1.4] Se debe separar los recursos de desarrollo, prueba y operación

- ✓ **Referente a la gestión de servicios prestados por terceros**

Con respecto a supervisión y revisión de los servicios:

[E373] Se debe mantener controles de monitorización y verificación del rendimiento

[E376] Se debe mantener acuerdos para informar, notificar e investigar las incidencias y fallos de seguridad para tener un tratamiento frente a código dañino.

Con respecto a Gestión de cambios en los servicios:

[S8] Se debe tener una gestión de cambios (mejoras y sustituciones para los servicios) referente a documentación, actualización de procedimientos de explotación y de los planes de continuidad en servicios.

- ✓ **Referente a planificación y aceptación de sistemas:**

Con respecto a gestión de capacidades

[G451] Se debe monitorizar el uso de los recursos

[G452] Se deben establecer: las necesidades en cuanto a procesamiento, cambios de software, almacenamiento y de transmisión

[G4541] Se debe determinar las dependencias de servicios internos y externos

Con respecto a la aceptación de nuevos sistemas:

[S44] Se debe verificar los controles de seguridad y tener un plan de concienciación y formación en materia de seguridad.

[S46] Se debe hacer una campaña de ejecución de pruebas de regresión (no afecta a los demás servicios) y actualización de los planes de continuidad, documentando los procedimientos de operación y producción.

4.1.3.7 Dominio: Control de Acceso

Controles:

Requisitos del control de acceso

Gestión de usuarios

Responsabilidades de los usuarios

Control de acceso a la red

Control del acceso a sistemas en operación

Control de acceso a datos y aplicaciones

Equipos móviles y tele-trabajo

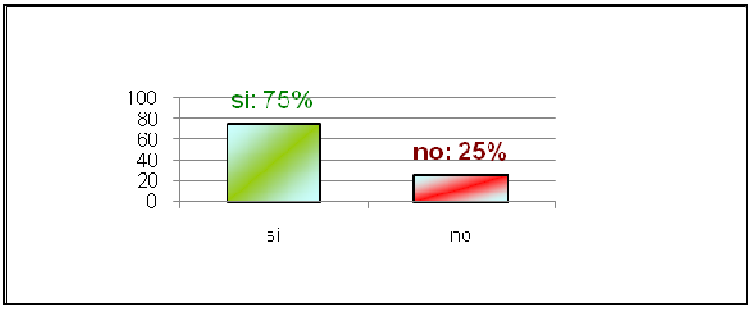


Figura 4.1.3.7 Resultado de la Encuesta: Control de Acceso

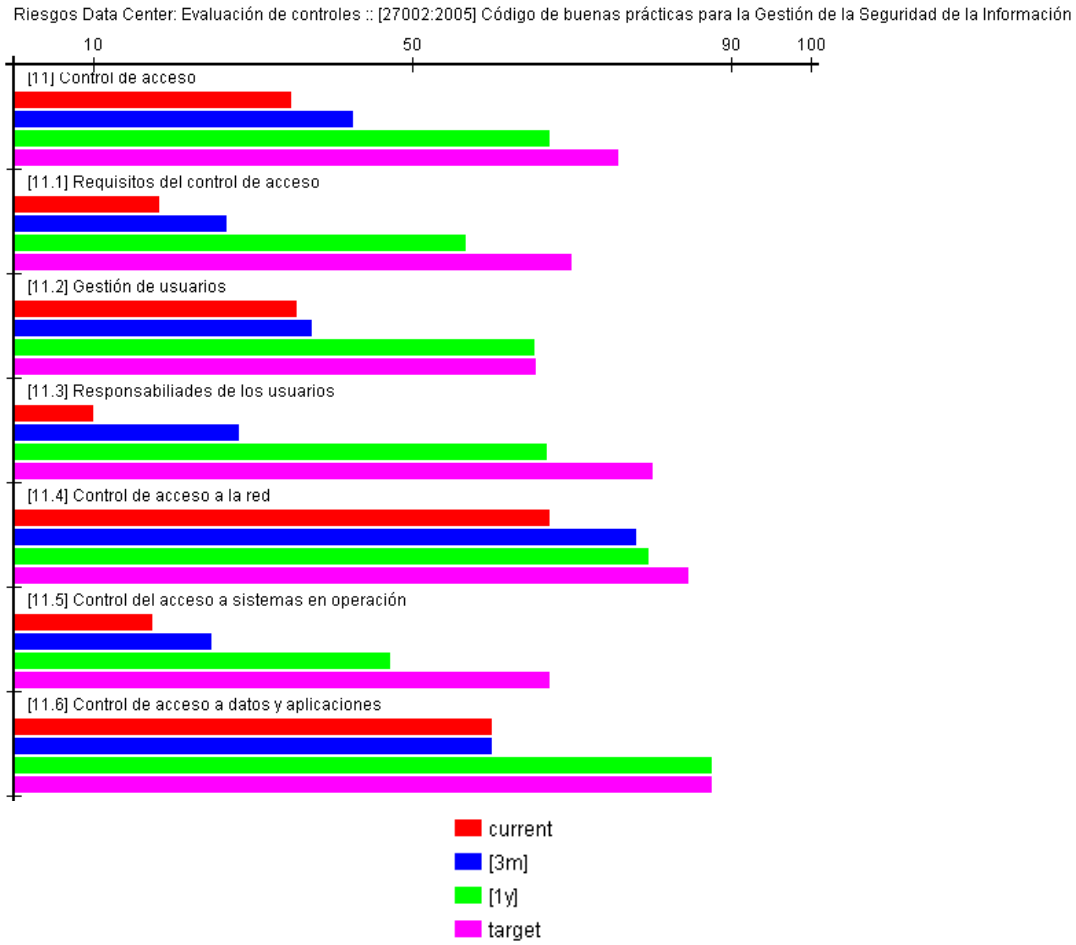


Figura 4.1.3.7 Resultado de la Herramienta PILAR: Control de Acceso

Objetivo:

Controlar los accesos a la información, medios de procesamiento de información y procesos comerciales, de acuerdo a los requerimientos del negocio y de seguridad. Las regulaciones para el control de los accesos deben considerar las políticas de divulgación de la información y de autorizaciones.

Observación:

Falta de documentación de procedimientos de gestión de usuarios, operación y políticas de seguridad en equipos desatendidos

Condición:

- ✓ No se protege el acceso de los equipos desatendidos en todas las aéreas de UTIC'S

Evidencia: Cuestionario de investigación de la Seguridad de la Información, basada en las preguntas de control de la Norma ISO 27004, para el Data Center de la Escuela Politécnica del Ejercito.

Riesgos:

Cambios no autorizados en los recursos de tratamiento de la información que comprometan la integridad y seguridad de los mismos.

Compromiso, daño o pérdida de recursos de información.

Pérdida total o parcial de los equipos y de información de la institución

Accesos no autorizados, mal uso o corrupción de la información

Causa:

- o No existe supervisión del individuo que ingresa a UTICS, pudiendo este acceder a la mayoría de equipos dentro del Data Center.

Recomendaciones:

Colocar cámaras de seguridad en toda el área para monitorear los accesos físicos a equipos.

Documentar y aplicar las Políticas de Seguridad para todos los usuarios internos con los perfiles asignados por la tarea que realizan.

Monitorizar los accesos a la Red y el tráfico con mayor frecuencia.

Para ello se recomienda aplicar las siguientes salvaguardas:

Referente a requisitos de control de acceso

- Documentar y establecer la Política de control de Accesos.

Referente a Gestión de Usuarios

- [H131] Se debe Identificar individualmente a todos los usuarios que acceden al sistema.
- [H14] Se debe gestionar la identificación y autenticación de usuario
- [H25d] Se debe realizar la cancelación de privilegios a usuarios que asuman nuevas responsabilidades y roles, o estén fuera de la institución.
- [H26] Revisar periódicamente los derechos de acceso de los usuarios y comunicar a los mismos por escrito.
- [S53] Eliminación de cuentas estándar de administrador
- [H262] Supervisión y revisión del personal que hace cumplir los controles
- [H266] Investigación de toda actividad inusual

Referente a responsabilidades de los usuarios

- [H1513] Los usuarios deben garantizar la confidencialidad de las contraseñas.
- [H1519] Las contraseñas se deben modificar al ser comprometidas o existir sospecha de ello
- [H1512] Se deben seleccionar contraseñas fáciles de recordar pero de difícil conjetura .y deben tener una duración limitada, inferior a 1 año.
- [H2c] Los equipos informáticos de usuarios desatendidos, deben bloquearse en sus sesiones, y apagarse al final de la jornada.

Referente control de acceso a la red

- [COM813] Se debe proteger los puertos de diagnóstico remoto.

4.1.3.8 Dominio: Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

Controles:

- **Requisitos de seguridad**
- **Garantías de procesamiento de información**
- **Controles criptográficos**

- **Seguridad de los archivos del sistema**
- **Seguridad en los procesos de desarrollo y soporte**
- **Gestión de vulnerabilidades**

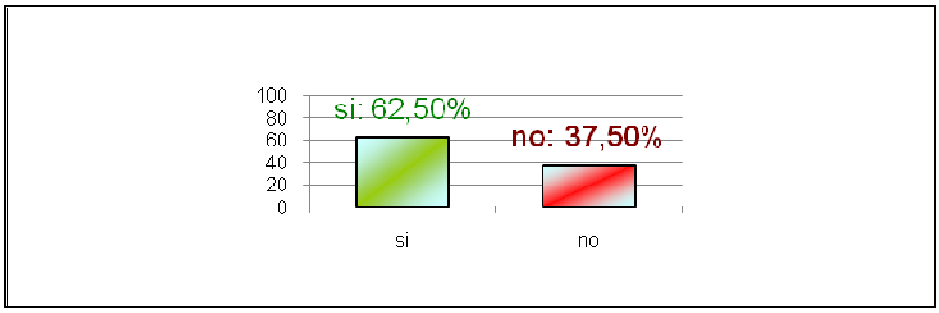


Figura 4.1.3.8 Resultado de la Encuesta: Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

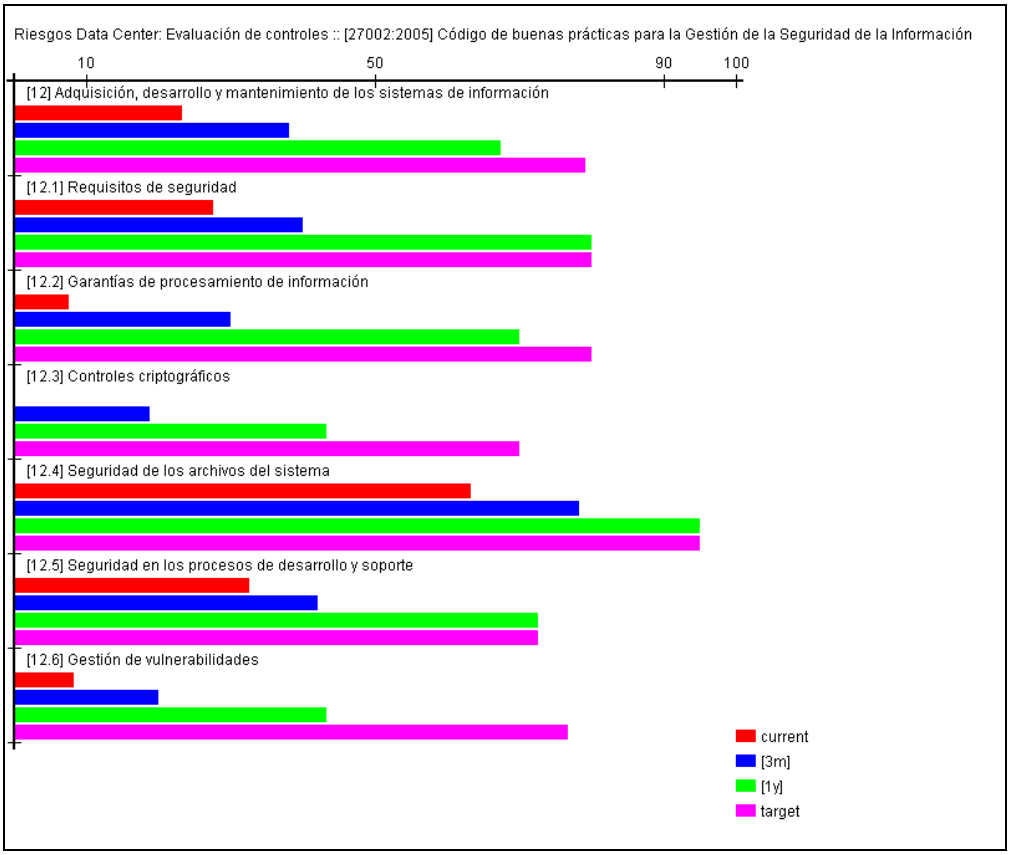


Figura 4.1.3.8 Resultado de la Herramienta PILAR: Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

Objetivo:

Adquirir o desarrollar sistemas siendo una prioridad la seguridad de la información, y estableciendo los procedimientos para el control en la instalación

del software, garantizando la seguridad de los archivos del sistema controlando los accesos al mismo y el código fuente, para evitar robos, alteraciones, o la aplicación de ingeniería inversa por parte de personas no autorizadas, mientras que las actividades de soporte se deben realizar de manera segura.

Observación:

No existen implantados controles criptográficos

Condición:

- ✓ No existen controles criptográficos.
- ✓ No existe seguridad en los ficheros de los sistemas.

Evidencia: Cuestionario de investigación de la Seguridad de la Información, basada en las preguntas de control de la Norma ISO 27004, para el Data Center de la Escuela Politécnica del Ejercito.

Riesgos:

Confiabilidad, comprometer información personal o de la empresa.
Compromiso, daño o pérdida de recursos de información
Fallos en los sistemas, que comprometan las actividades críticas de la organización.
Ejecución de códigos móviles no autorizados que atenten contra la seguridad.
Pérdida total o parcial de la información critica de la institución
Accesos no autorizados, mal uso o corrupción de la información

Causa:

- o Los controles criptográficos se encuentran en proceso de implementación
- o No tienen documentada la política de seguridad utilizada para otorgar permisos y privilegios a los respectivos accesos de ficheros en red, necesitando actualizar los planes de continuidad en seguridad.

Recomendaciones.

- Se necesita un Plan de políticas de seguridad para otorgar permisos y privilegios a los respectivos accesos de ficheros en red.
- Se debe hacer actualizaciones del Plan de continuidad en Seguridad.

Se recomienda además aplicar las siguientes salvaguardas.

Referente a requisitos de seguridad

- Se necesita realizar el análisis y especificación en cuanto a disponibilidad, autenticidad y los requisitos de seguridad de acuerdo al tipo de negocio.

Referente a las garantías de procesamiento de la información

- [12.2.1] Validación de datos de entrada y salida
- [12.2.2] Control de tratamiento interno
- [12.2.3] Integridad de los mensajes

Referente a controles criptográficos

- Documentar la Política de Uso y la Gestión de Claves criptograficas

Referente a la seguridad de los archivos del sistema

- Se debe realizar los controles de programas en producción, proteger los datos de prueba y mejorar el control de acceso al código fuente.

Referente a seguridad en los procesos de desarrollo y soporte

- [SWb9] Se deben revisar los procedimientos de control de cambios, realizar Pruebas de regresión, actualizaciones y mantenimiento cuando existan cambios, Inspección del código,
- [SWa4] Mejorar la seguridad de los ficheros de datos de la aplicación
- [H33] Utilizar Herramientas de monitorización de tráfico

Referente a Gestión de vulnerabilidades

- Establecer controles de vulnerabilidades técnicas de algoritmos periódicamente.

4.1.3.9 Dominio: Gestión de Incidentes de Seguridad de Información

Objetivo: Trabajar con reportes de los eventos y debilidades de la seguridad de la información, asegurando una comunicación tal que permita que se realice una acción correctiva oportuna, llevando la información a través de los canales gerenciales apropiados lo más rápidamente posible. De la misma manera se debe contar con reportes de las debilidades en la seguridad, requiriendo que todos los empleados, contratistas y terceros de los sistemas y servicios de información tomen nota de y reporten cualquier debilidad de seguridad observada o sospechada en el sistema o los servicios.

Controles:

- **Comunicación de incidencias y debilidades**
- **Gestión de incidentes y mejoras**

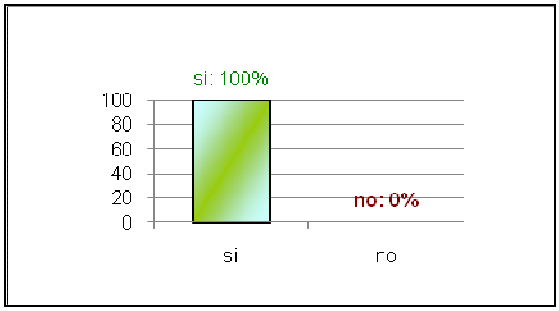


Figura 4.1.3.9 Resultado de la Encuesta: Gestión de Incidentes de Seguridad de Información

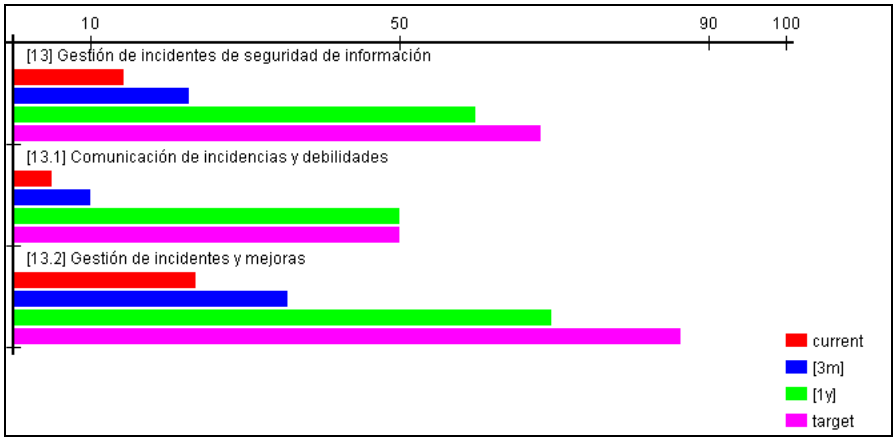


Figura 4.1.3.9 Resultado de la Herramienta PILAR: Gestión de Incidentes de Seguridad de Información

Observación: Para este dominio se cumplen a cabalidad los controles.

Condición:

- ✓ Se cumplen todos los controles del dominio de gestión de incidentes de seguridad de la información.

Evidencia: Cuestionario de investigación de la Seguridad de la Información, basada en las preguntas de control de la Norma ISO 27004, para el Data Center de la Escuela Politécnica del Ejercito.

Riesgo:

Problemas de comunicación en lo que respecta a incidentes de seguridad, vulnerabilidad a amenazas en el Data Center que podrían materializarse y no disponer de un procedimiento de respuesta ante las incidencias.

Causa:

- o Mantener el apoyo respecto a seguridades y la comunicación de eventos de seguridad, tener documentación, seguimiento de incidentes encontrados y revisión de las medidas correctoras para comprobar que son efectivas.

Recomendaciones:

- Mantener informes formales de los eventos y de los procedimientos de escalada.
- Todos los usuarios empleados contratistas y terceros deben estar al tanto de los procedimientos para el reporte de los diferentes tipos de eventos y debilidades que podrían tener un impacto en la seguridad de los activos organizacionales.

Para ello se recomienda aplicar las siguientes salvaguardas:

Referente a comunicación de incidencias:

- [H43] Se debe mantener comunicación de las incidencias de seguridad mediante registros en los que abarca el tipo de incidencia, momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y acciones tomadas, haciendo constantes pruebas y revisiones de los procedimientos.
- [H45] Al existir fallos en el software se debe comunicar mediante un procedimiento definido como: dejar de usar el sistema (aislarlo si es posible, pero no apagarlo) e informar inmediatamente al superior responsable por el canal determinado y a los usuarios que no deben intentar retirar el software sospechoso.

Referente a gestión de incidentes y mejoras:

- [H42] Se debe establecer un esquema de gestión en el que prime el análisis e identificación de la causa y la planificación e implantación de medidas tomadas en anteriores auditorías, atendiendo a su validez, calidad y completitud y posteriormente se haga un almacenamiento seguro de las evidencias tanto en papel como en medios electrónicos.
- [H47] Mantener un control formal del proceso de recuperación ante incidentes mediante identificación y autorización del personal que gestione el incidente y el registro de todas las acciones realizadas y aprobadas por la Dirección.
- [H41] Se debe tener procedimientos actualizados para todos los tipos potenciales de incidencias, haciendo revisiones periódicas de software, datos y sistemas críticos, al igual que un procedimiento en caso de denegación de servicio, fallos del sistema, datos del negocio inexactos o incompletos y procedimiento ante violaciones de la confidencialidad.
- [H46] Mantener una normativa para la gestión de los registros de fallos que han sido resueltos satisfactoriamente y medidas correctoras para comprobar que son efectivas.

4.1.3.10 Dominio: Gestión de la Continuidad del Negocio

Control:

- **Seguridad de la información en relación a la gestión de la continuidad**

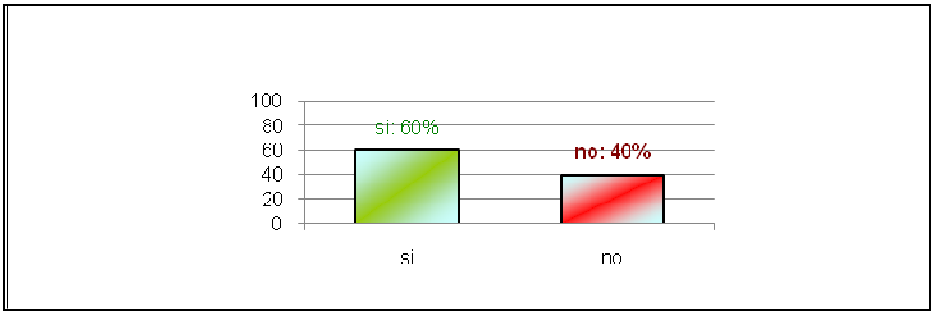


Figura 4.1.3.10 Resultado de la Encuesta: Gestión de la Continuidad del Negocio

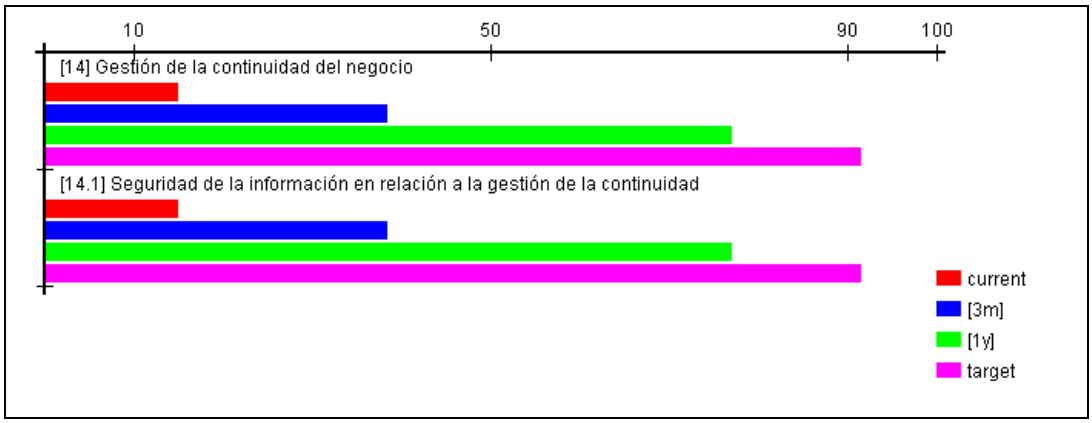


Figura 4.1.3.10 Resultado de la Herramienta PILAR: Gestión de la Continuidad del Negocio

Objetivo: Desarrollar planes para la continuidad del negocio para asegurar la reanudación oportuna de las operaciones esenciales. La seguridad de la información debiera ser una parte integral del proceso general de continuidad del negocio, y otros procesos gerenciales dentro de la organización.

Observación: Falta tener un comité para la planificación de continuidad del negocio y el análisis de impacto al que hace referencia a la asignación de recursos en seguridad, basándose en el impacto potencial para el negocio, respecto a los diversos incidentes que se deben resolver.

Condición:

- ✓ No existe un marco de planificación para la continuidad del negocio.
- ✓ No existe prueba, mantenimiento y reevaluación de los planes de continuidad del negocio.

Evidencia: Cuestionario de investigación de la Seguridad de la Información, basada en las preguntas de control de la Norma ISO 27004, para el Data Center de la Escuela Politécnica del Ejercito.

Riesgo:

No se podrá actualizar los procedimientos de emergencia establecidos si no se da cumplimiento al plan de continuidad, así como las personas responsables de ejecutar cada componente del mismo.

Los planes de continuidad de los negocios pueden fallar en el curso de las pruebas, frecuentemente debido a suposiciones incorrectas, negligencias o cambios en el equipamiento o el personal, por esta razón es necesario probarlos periódicamente para garantizar que están actualizados y son eficaces. Las pruebas también deben garantizar que todos los miembros del equipo de recuperación y demás personal relevante estén informados de dichos planes.

Causa:

- o Se debería mantener un esquema único de planes de continuidad del negocio para garantizar que dichos planes son consistentes, para tratar los requisitos de seguridad y para identificar las prioridades de prueba y mantenimiento.

- Falta de cumplimiento en planes de continuidad, realización de pruebas y simulacros que garanticen la eficacia de los mismos.

Recomendaciones:

- Los procedimientos de emergencia, los planes de reanudación y los planes de recuperación deben contarse entre las responsabilidades de los propietarios de los recursos o procesos de negocio pertinentes y cada plan deberá tener un propietario específico.

- Se debe tener un cronograma de pruebas para los planes de continuidad del negocio deberá indicar cómo y cuándo deberá probarse cada elemento del plan y así garantizar su eficacia permanente. Se deberán incluir procedimientos en el programa de administración de cambios de la institución para garantizar que se aborden adecuadamente los tópicos de continuidad del negocio.

Para ello se recomienda aplicar las siguientes salvaguardas:

Referente a seguridad de la información en relación a la gestión de la continuidad:

- [G522] Se debe desarrollar e implantar planes de continuidad incluyendo la seguridad de la información, designando: roles y responsabilidades, objeto y alcance, recursos necesarios, formación, pruebas de los planes, revisiones y mantenimiento de los planes con frecuentes copias de seguridad (backup) y almacenamiento seguro con la respectiva aprobación y difusión de la documentación.

- [G527] Se debe utilizar diversas técnicas para garantizar que los planes aprobados funcionen en la vida real y tengan un plan de gestión de crisis

que permita recuperar medios alternativos de almacenamiento y procesamiento de la información y también debe incluir:

- Pruebas de discusión de diversos escenarios, discutiendo medidas para la recuperación del negocio;
- Simulaciones, especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis;
- Pruebas de recuperación técnica, garantizando que los sistemas de información puedan ser restablecidos con eficacia.
- Pruebas de recuperación en un sitio alternativo, ejecutando procesos de negocio en paralelo, con operaciones de recuperación fuera del sitio principal.
- Pruebas de instalaciones y servicios de proveedores, garantizando que los productos y servicios de proveedores externos cumplan con el compromiso contraído.
- Ensayos completos, probando que la institución, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar las interrupciones.

4.1.3.11 Dominio: Cumplimiento

Controles:

- **Satisfacción de requisitos legales**
- **Cumplimiento de políticas, normas y reglamentos técnicos**
- **Consideraciones sobre auditoría de los sistemas de información**

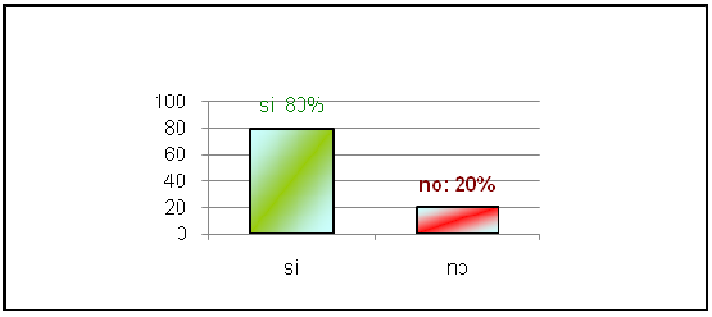


Figura 4.1.3.10 Resultado de la Encuesta: Cumplimiento

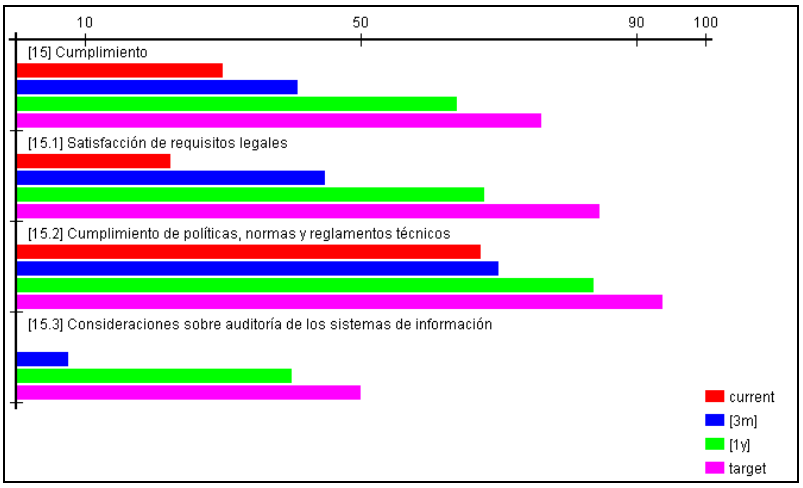


Figura 4.1.3.10 Resultado de la Herramienta PILAR: Cumplimiento

Objetivo: Dar prioridad al buen cumplimiento de los requisitos legales para evitar violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

Observación: Falta de revisiones periódicas de política de seguridad.

Condición:

- ✓ No existe una revisión de la política de seguridad y de la conformidad técnica.

Evidencia: Cuestionario de investigación de la Seguridad de la Información, basada en las preguntas de control de la Norma ISO 27004, para el Data Center de la Escuela Politécnica del Ejercito.

Riesgo:

Por no cumplir a cabalidad el primer dominio referente a políticas de seguridad, esto afecta al último dominio de la Norma ISO 27002 que hace referencia al cumplimiento de los requisitos legales que pueden evitar violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y a cualquier requerimiento de seguridad.

Causa:

- Pese a que en las áreas del Data Center se pone énfasis a lo que se refiere a contrato de prestación de servicios y también a las normas necesarias, no existe una revisión de las políticas de seguridad y de conformidad, esto complementa al primer dominio de políticas de seguridad que menciona que no hay documentos y procedimientos relativos a la seguridad; por ende no se podría hacer revisiones.

Recomendaciones:

- Los jefes de las áreas del Departamento de UTIC'S deben revisar regularmente el cumplimiento del procesamiento de la información dentro de su área de responsabilidad con las políticas y estándares de seguridad apropiados y actualizados , y cualquier otro requerimiento de seguridad.

Si se encuentra cualquier incumplimiento como resultado de la revisión, el director debe:

  - Determinar las causas del incumplimiento.
  - Evaluar la necesidad de acciones para asegurar que no vuelva a ocurrir el incumplimiento.
  - Determinar e implementar la acción correctiva apropiada.
  - Revisar la acción correctiva tomada.

- Los resultados de las revisiones y las acciones correctivas tomadas por los jefes de las áreas del departamento deben registrar y mantener estos registros. Cuando se lleva a cabo una revisión independiente en el área de su responsabilidad, los jefes de departamento deberán reportar los resultados a la persona que está llevando a cabo las revisiones independientes.

- Se debe verificar el cumplimiento técnico por medio de un ingeniero de sistemas experimentado y/o con la asistencia de herramientas

automatizadas, las cuales generarán un reporte técnico para su subsiguiente interpretación por un especialista técnico. Es importante y muy recomendable que estas evaluaciones sean realizadas por especialistas ajenos a la institución.

- Si se utilizan pruebas de penetración o evaluaciones de vulnerabilidad, se deberá tener cuidado ya que estas actividades pueden llevar a comprometer la seguridad del sistema.

- Estas pruebas se deben planear, documentar y repetir. Todo chequeo de cumplimiento técnico deberá ser llevado a cabo por personas autorizadas y competentes, o bajo la supervisión de dichas personas.

Para ello se recomienda aplicar las siguientes salvaguardas:

Referente a satisfacción de requisitos legales:

- [G31] Se debe tener un marco de referencia que identifique requisitos legales, reglamentarios o contractuales, mediante una asesoría legal y constantes revisiones del marco operacional
- [SW782] Se debe mantener acuerdos sobre licencia, propiedad del código y derechos de propiedad intelectual (IPR) de trabajos realizados.
- [G8] Se debe dar protección a los documentos de la organización mediante un inventario que cumpla requisitos legales, contractuales y de continuidad de negocio.
- [G232] Se debe mantener directrices de clasificación y protección a los datos de carácter personal.
- [H53] Se debe mantener una supervisión y control del mal uso de los mecanismos de registro de actividad.

Referente al cumplimiento de políticas, normas y reglamentos técnicos:

- [G35] Se debe revisar y verificar periódicamente los procedimientos operativos, el cumplimiento de políticas, normas y reglamentos técnicos por parte del personal del Data Center.

Referente a consideraciones sobre auditoría de los sistemas de información:

- [H51] Se debe mantener procedimientos y normativas de auditoría y registro de actividades de los sistemas mediante una planificación de los requisitos de las actividades de auditoría y gestión de incidentes.
- [H52] Se debe dar protección a las herramientas de auditoría de sistemas separadas de los sistemas de desarrollo y operación.

CAPITULO V

Conclusiones y Recomendaciones

5.1 Conclusiones:

1. La Seguridad Informática permite proteger la infraestructura computacional incluyendo la información contenida, por ello debe ser tratado con la mayor responsabilidad en todas las áreas del Data Center, siendo uno de los factores de éxito principales la comunicación en la organización, porque el recurso humano organizado con Normas y Políticas establecidas mas las herramientas computacionales colaboran en la prevención de amenazas y disminución de Riesgos en Seguridad.

2. Las Normas ISO 27000 son un estándar internacional que ha permitido conocer en forma general la situación actual de la Institución en términos de Seguridad Informática, y complementa los resultados obtenidos en la evaluación Técnica Informática junto con la Metodología MAGERIT durante el proceso.

3. La Metodología MAGERIT ha permitido el análisis y gestión de riesgos que soportan los sistemas de información; elaborada por el Consejo Superior de Administración Electrónica de España. Con la ayuda del software Pilar se pudo conocer y evaluar la información a través de los Pilares en Seguridad Informática como: Disponibilidad, Integridad, Confidencialidad, Autenticidad y trazabilidad, esto se complementa con resultados más reales y que son comparados con el código de buenas prácticas de la ISO 27002.

4. Siendo el Riesgo la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización, deben minimizarse aplicando los mecanismos de control y salvaguardas para evitar que se materialicen.

5.2 Recomendaciones:

- Iniciar parte de las de las instituciones certificadas que aplican las Normas ISO 27000, ya que las UTIC'S cumplen en buena parte con el código de buenas prácticas que sugiere la ISO 27002.

- Desarrollar un Plan de Seguridad Informático tomando en cuenta las consideraciones que aportan en seguridad la Metodología MAGERIT empleada, así como el cumplimiento de las salvaguardas que nos proporciona la herramienta PILAR.

- Adquirir una herramienta para el análisis y Gestión de Riesgos en UTIC'S, para prever vulnerabilidades y para minimizar los riesgos que puedan ocasionar problemas al Data Center en el presente y futuro.

- La Institución necesita aplicar un Sistema de Gestión de Seguridad Informática SGSI que enuncia la NORMA ISO 27001 para establecer implementar, operar, monitorear, revisar, mantener y mejorar el Sistema Informático actual.

- Se deben aplicar las salvaguardas mencionadas en el informe ejecutivo para proteger los activos de la Institución frente a las amenazas y mitigar el riesgo encontrado.

BIBLIOGRAFIA

[1.] William P. Leonard, “La evaluación de la gestión: Una Evaluación de los métodos de gestión y desempeño Englewood Cliffs, McGraw-Hill glosario de términos y siglas Pág.5, Prentice Hall, 1962 [Citado el: 19 de Junio2011], Sebastián Firtman “Seguridad Informática”, Pág. 18, MP Ediciones, 2005 [Citado el: 19 de Junio2011]

[2.] Publicación del Ministerio de Administraciones Públicas de España,”Libro de MAGERIT 2”, Resumen MAGERIT versión 2 [Citado el: 19 de Junio2011] [Online:] http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184#

[3.] Estándar Internacional ISO/IEC 27002 (página 2) International Standard Book Numbering (ISBN) [Citado el: 19 de Junio 2011].

[4.] El portal de ISO 27001 Pág. 4, Publicada el 1 de Mayo de 2009. [Citado el: 19 de Junio 2011] [Online:] http://www.iso27000.es/sgsi.html#section2d

[5.] Martin Pérez, “Sociedad de la Información, Telecomunicaciones e Internet, Nuevas Tecnologías, Seguridad de la Información”, 25 de 02 de 2007 [Citado el: 19 de Junio 2011] [Online:] http://sociedaddelainformacion.wordpress.com/2007/02/25/la-familia-de-normas-isoiec-27000/

[6.] El portal de ISO 27001, Publicada el 1 de Mayo de 2009. [Citado el: 19 de Junio 2011] [Online:] http://www.iso27000.es/iso27000.html

[7.] El portal de ISO 27001, Publicada el 1 de Julio de 2007 [Citado el: 19 de Junio 2011]

[8.] El portal de ISO 27001, Publicada el 7 de Diciembre de 2009. [Citado el: 19 de Junio 2011]

[9.] El portal de ISO 27001, Publicada el 4 de Junio de 2008. [Citado el: 19 de Junio 2011]

[10.] Libro de MAGERIT 2 – Publicación del Ministerio de Administraciones Publicas de España [En línea] Productos y servicios complementarios [Online:] https://www.ccn-cert.cni.es/index.php?option=com_wrapper&view=wrapper&Itemid=187&lang=es

[11.] Alberto Rusbel y Duchi Bastidas, Tesis: “Estudio y definición de Políticas Plan de contingencias aplicables al Centro de Computo de la UPS”, Escuela Politécnica del Ejército, Sangolquí – Ecuador, 2002.

[12.] Fanny Paulina Flores Estévez y Diana Carolina Jiménez Núñez, Tesis: “Diseño de un sistema de gestión de seguridad de la información para la empresa MEGADATOS S.A. en la ciudad de Quito, aplicando las Normas ISO 27001 e IS0 27002”, Escuela Politécnica Nacional, Quito-Ecuador, 2010.

[13.] Alarcón Chávez y Rómulo Vladimir, Tesis: Aplicación de la Norma técnica ISO 27001:2005 para la gestión de la seguridad de la información en el IESS. Caso práctico, dirección de desarrollo institucional, Escuela Politécnica del Ejército, Sangolquí – Ecuador, 2009.

[14.] María Angeles Salcedo Salgado y María Alexandra Tapia Mendieta, Tesis: “Evaluación y auditoría del sistema de información de la ESPE: dominio, planeación y organización”, Escuela Politécnica del Ejército, Sangolquí – Ecuador, 2008.

[15.] Adrián Bermúdez y Gabriela Salazar, Tesis: Plan de Seguridad Informática para la Escuela Superior Militar “Eloy Alfaro”, Escuela Politécnica del Ejército, Sangolquí – Ecuador, 2010.
[16.] David Rodríguez Sánchez, Tesis: “Control y Auditoría de correos electrónicos en Lotus Notes”, Escuela Politécnica Superior Universidad Carlos III de Madrid, Leganés- España, 2.009.