ESCUELA POLITÉCNICA DEL EJÉRCITO

DPTO. DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"EVALUACIÓN TÉCNICA DE LA SEGURIDAD INFORMÁTICA DEL DATA CENTER DE LA BRIGADA DE FUERZAS ESPECIALES NO. 9 PATRIA"

Previa a la obtención del Título de:

INGENIERA EN SISTEMAS E INFORMÁTICA

POR:

SOFÍA MONSERRATH VITERI DÍAZ

SANGOLQUÍ, Marzo de 2013

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por la Srta. SOFÍA MONSERRATH VITERI DÍAZ, como requerimiento parcial a la obtención del título de INGENIERA EN SISTEMAS E INFORMÁTICA, bajo nuestra supervisión.

Marzo 2013

_____

EC. Gabriel Chiriboga

DIRECTOR DE TESIS

_____

Ing. Víctor Páliz

CODIRECTOR DE TESIS

DECLARACIÓN DE RESPONSABILIDAD

SOFÍA MONSERRATH VITERI DÍAZ

DECLARO QUE:

El Proyecto de grado denominado **"EVALUACIÓN TÉCNICA DE LA SEGURIDAD INFORMÁTICA DEL DATA CENTER DE LA BRIGADA DE FUERZAS ESPECIALES NO. 9 PATRIA"** ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Marzo 2012

_____

Sofía Monserrath Viteri Díaz.

CI: 172043160-8

AUTORIZACIÓN

Yo, SOFÍA MONSERRATH VITERI DÍAZ, autorizo a la Escuela Politécnica del Ejército la publicación en la biblioteca virtual de la institución de la tesis que tiene como título **"EVALUACIÓN TÉCNICA DE LA SEGURIDAD INFORMÁTICA DEL DATA CENTER DE LA BRIGADA DE FUERZAS ESPECIALES NO. 9 PATRIA**", cuyo contenido, ideas y criterios son de mi responsabilidad y autoría.

Marzo 2012

_____

Sofía Monserrath Viteri Díaz.

CI: 172043160-8

DEDICATORIA

El presente trabajo está dedicado especialmente a mis padres EDGAR VITERI y NATIVIDAD DÍAZ, ya que gracias a su esfuerzo y sacrificio diario supieron darme fuerzas para seguir adelante en la consecución de la tesis. Por su cariño y amor que cada día me hacen llegar, y fueron mis pilares desde siempre para no decaer en los retos que me pone la vida.

A mis abuelitos CASIMIRO Y REGINA, que ya no se encuentran junto a mí, pero supieron darme su cariño, amor, comprensión y sobre todo me apoyaron durante una etapa de mis estudios escolares.

A mis hermanos SYLVIA, ADRIAN y SEBASTIAN por apoyarme incondicionalmente y cuidarme siempre.

SOFÍA MONSERRATH VITERI DÍAZ

AGRADECIMIENTO

A DIOS por permitirme escribir cada una de estas palabras, por siempre haberme brindado la fuerza necesaria para culminar esta etapa en mi vida a pesar de tantas dificultades que se me presentaron.

Agradezco a mis padres, ya que son quienes me apoyan moral y económicamente, y porque son el eje de mi vida y mi principal motivación de seguir adelante.

A la Universidad donde fui formada y a mis maestros que fueron más que docentes, por impartir el conocimiento durante todo el tiempo que duro mi carrera.

A mis tíos ROBINSON Y WILMA, que de una u otra forma contribuyeron para que me encuentre cumpliendo una meta más en mi vida.

SOFÍA MONSERRATH VITERI DÍAZ

ÍNDICE DE CONTENIDOS

LISTADO DE TABLAS

CAPÍTULO 3

LISTADO DE FIGURAS

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

LISTADO DE ANEXOS

RESUMEN

En la actualidad el uso del internet se ha vuelto muy necesario en el ámbito de la tecnología, economía, educación entre otros. Sin tener en cuenta que conlleva a tener mayor posibilidad de presentar amenazas y vulnerabilidades dentro de las organizaciones.

El presente trabajo está encaminado a proporcionar un panorama más claro sobre las Normas ISO 27000, la misma que está encargada gestionar la seguridad Informática, también se utilizarán los Normas ISO 27001 y 27002 para determinar si existe integridad, confidencialidad y disponibilidad de la información.

De acuerdo a este escenario se aplicó la metodología MAGERIT que es el método formal para investigar los riesgos que soportan los sistemas de información y tomar medidas apropiadas para controlarlos, en conjunto se utilizó la herramienta PILAR para ayudar a controlar y mitigar los riesgos.

La Evaluación Técnica de la seguridad informática, se la realizó en la Brigada de Fuerzas Especiales No. 9 “Patria”, ubicada en Latacunga, Provincia de Cotopaxi, la misma que cuenta con un Datacenter, el mismo que tiene sus aplicaciones centralizadas en la comandancia.

CAPÍTULO 1

1. GENERALIDADES

1.1 INTRODUCCIÓN

Se utilizará el Modelo de Auditoría Basado en Riesgos, para determinar la matriz de riesgos, luego se tomará en cuenta el Modelo de Auditoría de Cumplimiento utilizando la norma ISO 27001 y 27002.

La Norma ISO 27001, es la principal norma en requisitos de la Norma ISO 27000, está dedicada a especificar los requerimientos necesarios para: establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información, la misma que se ha concebida para garantizar la selección de controles de seguridad adecuados para cada organización.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, la misma que será implantada y documentada dentro de este estudio.

Los Documentos que deben analizados y revisados dentro del proceso de la Norma ISO 27001 son: Manual de seguridad, Procedimientos, Instrucciones, checklists y formularios y Registros.

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA

La Norma ISO 27002 está conformada de 11 dominios, 39 objetivos de control en donde constan los 133 controles recomendados para la seguridad

de la información, también da a conocer el estándar en el tema de Seguridad de la Información, el mismo que tiene en su base tres pilares 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.

En cuanto al proceso que sugiere la norma se determinan diferentes acciones y controles considerados como práctica recomendada de uso frecuente en la implementación de la seguridad de la información para las organizaciones

Se aplicará también la metodología MAGERIT, para la administración de riesgos y sus herramientas informáticas aplicadas como RISK2 y PILAR.

La metodología que se utilizará es MAGERIT, la misma que está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los usuarios, e interesa a todos aquellos que trabajan con información mecanizada y los sistemas informáticos que la tratan.

MAGERIT V2, 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, y persigue objetivos.

Las herramientas EAR soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit.

La Herramienta PILAR, es una Herramienta de Análisis y Control de Riesgos, que utiliza la metodología Magerit.

Permite analizar los riesgos en cuanto a: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Los riesgos son tratados mediante una serie elementos como: Normas de Seguridad, Contra medidas y Procedimientos de Seguridad, y el riesgo residual en cada etapa del tratamiento

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 cimentan 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 Brigada de Fuerzas Especiales No. 9 “Patria” es un ente que pertenece al estado, cuya finalidad esencial es formar militares de excelencia para salvaguardar al país. La Brigada no deja de lado la tecnología, porque posee un Datacenter que será sometido a una Evaluación Técnica Objetiva, con dicha evaluación se podrá obtener las fortalezas y debilidades en los procesos que se tiene dentro del Datacenter, también ayudará a medir la eficacia y tener como resultado la continuidad del servicio.

La Brigada de Fuerzas Especiales No. 9 “Patria ”, se encuentra ubicada en la Provincia de Cotopaxi, actualmente los sistemas que se utilizan se encuentran centralizados en la Comandancia, el área tecnológica está encargada de dar servicios de: Soporte a nivel de hardware y software, realizar respaldos de Información y administrar permisos de usuarios.

Es de conocimiento que La Brigada “Patria” recibe cada año a cientos de conscriptos y aspirantes a militares que ingresan a las diferentes ramas de la milicia, y 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 los resultados obtener las

recomendaciones que servirían a la Institución, ya que la Brigada “Patria” no está libre de tener riesgos y amenazas que atenten contra la información, por el gran crecimiento de hackers y programas maliciosos como (malware, virus, troyanos, etc.) que afectan a los datos y a la información que se manipula.

Cabe señalar que: la veracidad, integridad y actualización de la Información, en el procesamiento de datos, son importantes para la Brigada “Patria” y especialmente dentro del Datacenter.

Es de prioridad para el Datacenter de la Institución, proteger la información mediante políticas y controles de Seguridad Informática para no encontrarse en dificultades ante amenazas constantes que afectan a los sistemas, o si los afectan no causen mayor impacto dentro de la organización.

La Brigada de Fuerzas Especiales No. 9 “Patria”, para brindar un servicio Informático eficiente y administrar los recursos tecnológicos posee un Datacenter el mismo que cuenta con las normas básicas de Seguridad Informática.

1.3 JUSTIFICACIÓN

La Brigada “Patria” se beneficiaría de este Proyecto, porque con los resultados, descubrirán 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.

Durante el desarrollo del Proyecto de Grado, se realizará la Evaluación o Diagnóstico de la Seguridad Informática en el Datacenter, porque aparte de verificar las falencias, se podrían aplicar controles y políticas en base a las recomendaciones obtenidas en las NORMAS 27001 y 27002 para minimizar en el futuro que ocurran 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 de las seguridades del Datacenter de la Brigada “Patria” en Latacunga, considerando como referencia los estándares ISO 27001 e ISO 27002.

1.4.2 OBJETIVOS ESPECÍFICOS

- Desarrollar el plan de trabajo que será ejecutado en la Institución.
- Determinar los recursos de TI, la infraestructura de la Institución y el periodo que comprende el proyecto.
- Definir actividades y cargos del personal tecnológico de la Brigada.
- Elaborar el plan de investigación de campo.
- Elaborar y aplicar los instrumentos de investigación de campo.
- 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.
- 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 del Data Center de la Brigada Patria, ubicada en Latacunga, contempla las normas internacionales ISO 27001 y 27002 para verificar el cumplimiento del SGSI (Sistema de la Seguridad de la Información), no se examinara el Plan de Seguridad Informática, este plan se realizará como otro proyecto en la posteridad.

Para la recopilación de la información se utilizara el plan de investigación de campo.

Para obtener los activos de riesgo se aplicará la metodología MAGERIT y posteriormente se empleara la herramienta PILAR, la misma que proporciona las Matrices de Riesgo e Impacto Acumulado.

El diagnóstico, 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 aportará para diseñar un programa de mejora continua con un plan de Seguridad Informática, el mismo que servirá para que los usuarios del Datacenter de la Brigada “Patria”, se encuentren en capacidad de aplicar medidas de seguridad para mantener la información Disponible, Confiable y Oportuna.

CAPÍTULO 2

2. FUNDAMENTACIÓN TEÓRICA

2.1 CONCEPTOS PRINCIPALES DE AUDITORÍA Y SEGURIDAD INFORMÁTICA

Los conceptos más importantes dentro de auditoría y seguridad informática son:

Información: Es la agrupación de datos organizados y presentados en un contexto. La información permite traer a nuestras mentes las impresiones del mundo exterior de forma que podamos construir su representación. Se debe procesar los datos para crear información, esto implica su clasificación y análisis.

Dato: Los datos representan únicamente una parte de lo que pasa en la realidad y no proporcionan juicios de valor o interpretaciones, sin embargo es la base para la generación de información.

Amenaza: Cualquier circunstancia o acontecimiento con el potencial de afectar a un sistema de información como es el acceso desautorizado, la destrucción, la modificación de datos, y/o la negación del servicio[1]

Vulnerabilidad: Debilidad en los procedimientos del sistema de información, de la seguridad del sistema, controles internos, o de implementación que podría ser explotada por una amenaza.

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

Control: Los controles incluyen características de seguridad, restricciones propuestas por la gerencia, seguridad del personal, y seguridad de estructuras, de áreas, y de dispositivos físicos

Riesgo[2]: Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro.

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

Disponibilidad o disposición de los servicios: Se refiere a cuando y como se encuentran dispuestos los servicios al momento de ser usados. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

[2] **Fuente:** Libro I – Magerit (Método), Ministerio de Administraciones Públicas, Madrid

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Integridad: Mantenimiento de las características de completitud y corrección de los datos.

Confidencialidad[3]: Aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.

Autenticidad[4] (De quien hace uso de los datos o servicios): o que no haya duda a quien se hace responsable de una información o una presentación de un servicio, tanto a fin de confiar en él como de poder perseguir posteriormente los incumplimientos o errores, Contra la autenticidad se dan suplantaciones y engaños que buscan realizar un fraude.

Activos: Son los recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.

Impacto: Es la medida del daño sobre el activo derivado de la materialización de una amenaza.

Norma[5]: Regla, disposición o criterio que establece una autoridad para regular los procedimientos que se deben seguir para la realización de las tareas asignadas. Se traduce en un enunciado técnico que a través de parámetros cuantitativos y/o cualitativos sirve de guía para la acción. Generalmente la norma conlleva una estructura de sanciones para quienes no la observen.

[3] **Fuente:** Libro II – Magerit (Catálogo de Elementos), Ministerio de Administraciones Públicas, Madrid
MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
[4] **Fuente:** Libro I – Magerit (Método), Ministerio de Administraciones Públicas, Madrid
[5] **Fuente:** http://www.sre.gob.mx/images/stories/docnormateca/historico/dgpop/guia_elab_manu_org.pdf

Estándar[6]: Un estándar es una especificación que regula la realización de ciertos procesos, normas o la fabricación de componentes para garantizar la interoperabilidad.

Metodología: Conjunto de métodos empleados para el desarrollo de sistemas automatizados. Una metodología completa es una notación, un proceso, un conjunto de herramientas.

Seguridad Informática[7].- Es el conjunto de actividades y medidas orientadas a la protección de la información contenidas en los sistemas e instalaciones informáticas frente a su posible destrucción, modificación, utilización y difusión indebidas.

2.2 MARCO TEÓRICO NORMAS ISO 27000, 27001 Y 27002

2.2.1 NORMA ISO 27000[8]

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

Las Normas ISO 27000 contienen las mejores prácticas recomendadas en Seguridad de la información para: desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión

[6] **Fuente:** http://osluz.unizar.es/files/presentacion_pdi.pdf
[7] **Fuente:** http://dspace.ups.edu.ec/bitstream/123456789/216/3/Capitulo%202.pdf
[8] **Fuente:** http://www.iso27000.es

de la Seguridad de la Información (SGSI) para contribuir en la desvalorización de riesgos, amenazas y vulnerabilidades informáticas.

2.2.2 NORMA ISO/IEC 27001

La Norma ISO 27001, siendo la principal norma en requisitos de la Norma ISO 27000, 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 seis meses a un año.

2.2.3 NORMA ISO/IEC 27002

Llamada anteriormente ISO/IEC 17799, es una guía de buenas prácticas en la gestión de la seguridad de la información, 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
- 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

Esta Norma da a conocer el estándar en el tema de Seguridad de la Información, el mismo que tiene en su base tres pilares 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.

La confidencialidad garantiza que la información sea accesible solo para aquellas personas autorizadas, la integridad salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento, y la disponibilidad asegura que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que sea requerida.

En cuanto al proceso se sugiere se determinen las siguientes acciones:

- Establecer los requerimientos de seguridad
- Implementación de controles
- Identificación de los factores críticos de éxito
    - Existen tres recursos para poder establecer los requerimientos de seguridad.
    - El primero es la evaluación de los riesgos, donde se identifican las amenazas a los activos, se evalúan vulnerabilidades y probabilidades de ocurrencia, y se estima el impacto potencial.
    - El segundo está constituido por los requisitos legales, normativos, reglamentarios y contractuales que deben ser cumplidos por la organización.
    - El tercer recurso es el conjunto de principios, objetivos y requisitos para el procesamiento de la información que ha desarrollado la organización para respaldar sus operaciones.
    - Posteriormente, luego de identificar los requerimientos de seguridad se deben implementar los controles para que los riesgos se reduzcan a un nivel aceptable.
    - Algunos controles que son sugeridos desde el punto de vista legal para una organización brindan:
    - Protección de datos y confidencialidad de la información personal

- Protección de registros y documentos de la Organización.
- Derechos de propiedad Intelectual

Los controles considerados como práctica recomendada de uso frecuente en la implementación de la seguridad de la información para las organizaciones y en la mayoría de los ambientes son los siguientes:

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

La Norma Indica 8 factores críticos de éxito, la misma que presenta factores concretos:

- Política de seguridad, objetivos y actividades que reflejen los objetivos de la empresa.
- Una estrategia de implementación de seguridad que sea consecuente con la cultura organizacional
- Apoyo y compromiso manifiestos por parte de la Gerencia
- Un claro entendimiento de los requerimientos de Seguridad, la evaluación de riesgos y la administración de los mismos
- Comunicación eficaz de los temas de seguridad al personal

- Distribución de guías sobre políticas y estándares de seguridad de la información a todos los empleados y contratistas.
- Instrucción y entrenamiento adecuados.

Un sistema integral y equilibrado de medición para evaluar el desempeño de la gestión de seguridad de la información y para brindar sugerencias tendientes a mejorarlo.

2.3 MARCO TEÓRICO MAGERIT

MAGERIT es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas"

MAGERIT V2[9] es una metodología de carácter público que fue desarrollada por el Ministerio de Administraciones Públicas de Madrid y consta del análisis y gestión de riesgos de los sistemas de información que tendrá como resultado recomendar medidas apropiadas para controlar los riesgos encontrados durante la aplicación de la metodología.

MAGERIT hasta la actualidad tiene dos versiones, la primera versión, fue publicada en el año de 1997 y la segunda en el 2005.

Entre las dos versiones de Magerit se tienen conceptos muy similares, pero con ciertas evoluciones.

En particular se reconocerá lo que se denominaba submodelo de elementos: activos, amenazas, vulnerabilidades, impactos, riesgos y

[9] **Fuente:** http://administracionelectronica.gob.es

salvaguardas. Esta parte conceptual ha sido refrendada por el paso del tiempo y sigue siendo el eje alrededor del cual se vertebran las fases fundamentales de análisis y gestión. Se ha corregido y ampliado lo que se denominaba “subestados de seguridad” dándole el nuevo nombre de “dimensiones” e introduciendo nuevas varas de medir lo que interesa de los activos. El submodelo de procesos aparece bajo el epígrafe de “estructuración del proyecto de análisis y gestión de riesgos”.

En la Figura 2.1 se puede ver los submodelos que posee el modelo Magerit.

Figura 2.1 Modelo de Magerit

Magerit V2 trae consigo el capítulo de “Desarrollo de Sistemas Informáticos”, enfatizando primero el desarrollo de aplicaciones aisladas y luego el proceso de desarrollo de sistemas de información completos.

La metodología persigue objetivos directos e indirectos que se detallan a continuación:

Objetivos Directos:

- 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
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control

Objetivos Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

2.4 DESCRIPCIÓN DE LA METODOLOGÍA[10]

La metodología MARGERIT se presenta en tres libros: El método, El catálogo de Elementos y la Guía de Técnicas que son detallados a continuación.

2.4.1 "EL MÉTODO" (LIBRO I)[11]

En este libro se describen los pasos y las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, y proporciona una serie de aspectos prácticos.

Se describen los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación, este contiene únicamente conceptos.

[10] **Fuente:** http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=magerit
[11] **Fuente:** Libro I – Método, Metodología de Análisis y Gestión de riesgos de los Sistemas de Información

Se describen las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, entendiendo que no basta con tener los conceptos claros, sino que es conveniente pautar roles, actividades, hitos y documentación para que la realización del proyecto de análisis y gestión de riesgos esté bajo control de forma continua.

Se aplica la metodología al caso del desarrollo de sistemas de información, en el entendimiento que los proyectos de desarrollo de sistemas deben tener en cuenta los riesgos desde el primer momento, tanto los riesgos a que están expuestos, como los riesgos que las propias aplicaciones introducen en el sistema.

Este libro también trae con sigo apéndices que recogen material de consulta:

- Glosario
- Referencias bibliográficas consideradas para el desarrollo de esta metodología
- Referencias al marco legal que encuadra las tareas de análisis y gestión
- El marco normativo de evaluación y certificación
- Las características que se requieren de las herramientas, presentes o futuras, para soportar el proceso de análisis y gestión de riesgos
- Guía comparativa de cómo Magerit versión 1 ha evolucionado en esta versión 2.

2.4.2 "EL CATÁLOGO DE ELEMENTOS" (LIBRO II)[12]

Este catálogo ayuda a facilitar la labor de las personas encargadas de evaluar la seguridad informática, en el sentido de ofrecerles ítem estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.

Por otra parte también permite homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

En este libro se tienen pautas en cuanto a:

- Tipos de activos
- Dimensiones de valoración de los activos
- Criterios de valoración de los activos
- Amenazas típicas sobre los sistemas de información
- Salvaguardas a considerar para proteger sistemas de información

Dentro de esta guía se persiguen dos objetivos que son:

- Facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.

[12] **Fuente:** Libro II – Catálogo de Elementos, Metodología de Análisis y Gestión de riesgos de los Sistemas de Información

- Homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

2.4.3 "LA GUÍA DE TÉCNICAS" (LIBRO III)[13]

Esta guía aporta conocimiento adicional y guías sobre algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos:

- Técnicas específicas para el análisis de riesgos
- Análisis mediante tablas
- Análisis algorítmico
- Árboles de ataque
- Técnicas generales
- Análisis coste-beneficio
- Diagramas de flujo de datos
- Diagramas de procesos
- Técnicas gráficas
- Planificación de proyectos
- Sesiones de trabajo: entrevistas, reuniones y presentaciones
- Valoración Delphi

Se trata de una guía de consulta. Según el lector avance por las tareas del proyecto, se le recomendará el uso de ciertas técnicas

[13] **Fuente:** Libro III – Guía de Técnicas, Metodología de Análisis y Gestión de riesgos de los Sistemas de Información

específicas, de las que esta guía busca ser una introducción, así como proporcionar referencias para que el lector profundice en las técnicas presentadas.

2.5 MARCO TEÓRICO PILAR

Es una Herramienta de Análisis y Control de Riesgos que utiliza la Metodología Magerit.

PILAR conjuga los activos TIC de un sistema con las amenazas posibles, calcula los riesgos y permite incorporar salvaguardas para reducir el riesgo a valores residuales aceptables.

Permite analizar los riesgos en cuanto a: Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad. Los riesgos son tratados mediante una serie elementos como: Normas de Seguridad, Contra medidas y Procedimientos de Seguridad, y el riesgo residual en cada etapa del tratamiento.

La razón de ser de PILAR está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos que supone unos beneficios evidentes para los usuarios; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios.

PILAR interesa a todos aquellos que trabajan con información mecanizada y los sistemas informáticos que la tratan. Si dicha

información o los servicios que se prestan gracias a ella son valiosos, PILAR les permitirá saber cuánto de este valor está en juego y les ayudará a protegerlo.

Objetivo:

Los objetivos perseguidos por la Herramienta Pilar son:

- Realizar el análisis de riesgos según la Metodología Magerit e ISO/IEC 27000.
- Diseño del Plan de Mejora de la Seguridad.

2.5.1 DESCRIPCIÓN PILAR[14]

PILAR consiste en una aplicación informática que compila los activos del sistema, sus relaciones de interdependencia y su valor para la organización. Conocido el sistema, permite introducir las amenazas posibles en los aspectos de Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad, para derivar los riesgos potenciales sobre el Sistema.

Una vez conocidos los riesgos, se pueden determinar una serie de salvaguardas y estimar el riesgo residual. El tratamiento del riesgo es un proceso continuo y recurrente en el que el sistema de protección se va mejorando regularmente para afrontar nuevos riesgos y aumentar la confianza que el sistema merece para los responsables y los usuarios.

[14] **Fuente:** Herramienta Pilar, Utilización de EAR/ PILAR José Mañas

2.5.2 RESULTADOS EN PILAR

Herramienta para la monitorización continúa del estado de riesgo y seguimiento de proyectos de mejora de la seguridad.

Los resultados que se obtienen con el uso de esta herramienta son los siguientes:

- Impacto potencial y residual.
- Riesgo potencial y residual.
- Mapa de riesgos.
- Plan de mejora de la seguridad
- Monitorización continúa del Estado de Riesgo

Las ventajas:

Las ventajas que aportan la utilización de la herramienta:

- Conocer los riesgos a fin de poder tratarlos.
- Conocer el grado de cumplimiento de diferentes perfiles de seguridad: 27002, protección de datos de carácter personal, esquema nacional de seguridad, etc.
- Implementar la metodología Magerit e ISO/IEC 27000

2.5.3 PERSONALIZACIÓN DE LAS HERRAMIENTAS PILAR

PILAR se puede personalizar en varios aspectos:

EVL: Perfiles de protección

TSV: Perfiles de amenazas

KB: Protecciones adicionales

Esta herramienta permite preparar y mantener personalizaciones, que se incorporan dinámicamente a la biblioteca, extendiéndola para adaptarse a un determinado contexto.

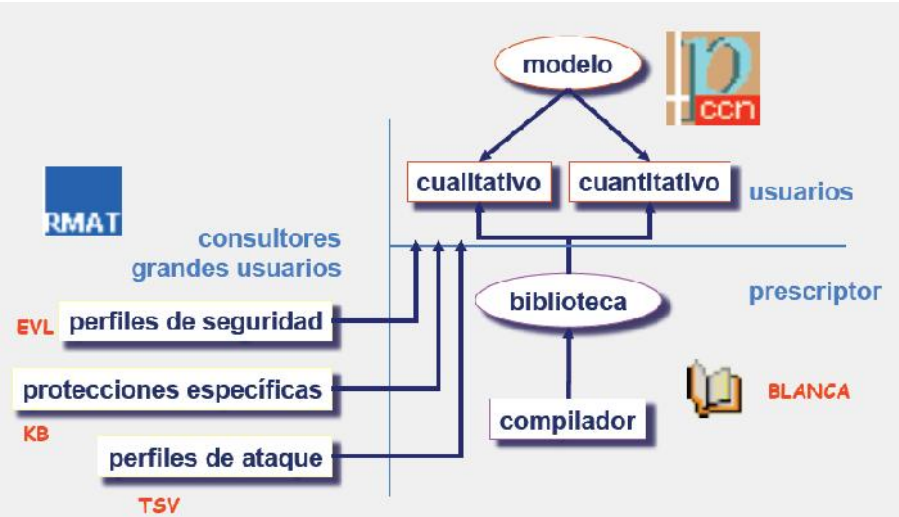

Figura 2.6.2 RMAT (Risk Management Additional Tools)

CAPÍTULO 3

3. EJECUCIÓN DE LA EVALUACIÓN TÉCNICA.

3.1 ELABORAR Y APLICAR LOS INSTRUMENTOS DE INVESTIGACIÓN DE CAMPO

Para conocer la situación actual del Datacenter de la Brigada de Fuerzas Especiales No. 9 “Patria” se tomó en cuenta la encuesta como primer instrumento para recoger, proponer y analizar la información. La encuesta fue realizada a partir de un cuestionario como registro de la información obtenida mediante los encargados del Datacenter

Los objetivos de la encuesta son:

OBJETIVOS:

- Revisar las políticas y Normas sobre seguridad que posee actualmente el Centro de datos
- Verificar la seguridad de personal, datos, hardware, software e instalaciones
- Identificar controles preventivos, detectivos y correctivos, así como el cumplimiento de los mismos por los usuarios.
- Verificar si existen garantías para proteger la integridad de los recursos informáticos.

Los resultados que se mostrarán a continuación parten de los resultados obtenidos mediante las encuestas, la misma que abarca los 11

dominios que indican las NORMAS ISO 27001 e ISO 27002 y de la matriz de riesgo que se realizó durante las visitas al Datacenter.

3.2 PROCESAR LOS DATOS OBTENIDOS DE LA INVESTIGACIÓN

Como principal instrumento de investigación se tienen la encuesta, la misma que fue realizada a todo el personal del área tecnología, porque es un grupo muy pequeño.

La encuesta fue estructurada de acuerdo a los siguientes aspectos:

- **Organización Del Centro De Cómputo.-** Se quiere conocer qué aspectos se tienen en cuenta al momento de operar el centro de cómputo, ya que es considerado por varios autores como simples restricciones, es decir, saber cómo el encargado del Datacenter debe decidir quiénes tienen acceso y a qué tipo de información.
- **Manejo De La Información.-** El manejo de información requiere de diferentes perfiles determinados por los administradores.

A la información se la ha dividido en:

  - **Seguridad Física.-** Con respecto a la seguridad física se quiere tener referencia sobre las barreras físicas y mecanismos de control en el entorno a los sistemas informáticos, para proteger el hardware de amenazas físicas.
  - **Seguridad Lógica.-** Con respecto a la parte lógica se quiere tener reseña de los mecanismos y barreras para mantener el

resguardo y la integridad de la información dentro de un sistema informático.

- **Respaldos.-** Determinar que dispositivos de almacenamiento masivo de información poseen dentro de la organización, y saber que probabilidad tienen de fallar.
- **Equipo De Soporte.-** Conocer los equipos de soporte que se tienen en el Datacenter y cuales se encuentran funcionando de manera correcta.
- **Recursos Humanos.-** Establecer cómo se hace la segregación de funciones y si el personal se encuentra capacitado para cubrir puestos dentro del centro de datos.
- **Financiero.-** Conocer cómo se destinan fondos para adecuar el centro de datos y como ayuda la gestión económica
- **Redes.-** Se elaborará un análisis del mantenimiento de la red, diseño de la red, topología, protocolos de comunicación, conexiones, accesos privilegios, administración y demás aspectos que repercuten dentro de la red.

Se procederá a procesar la información de forma general, la misma que se mostrará en porcentajes y se hará la gráfica correspondiente a las secciones que se obtuvieron durante la creación y aplicación de la encuesta.

Los resultados obtenidos mediante la aplicación de la encuesta muestran resultados generales, con respecto al SI y NO.

Como se muestra a continuación el resultado de SI es del 52.33%, mientras que para el resultado NO es el 47.67%, estos resultados muestran que se tiene un buen porcentaje de seguridades dentro de la Brigada “Patria”.

Si			No	
86	100		86	100
45	**X**		41	**X**
X=	52.33%		**X=**	47.67%

Tabla 3.2.1 Resultados Globales de la encuesta

La siguiente figura muestra las proporciones en las que el Datacenter de la Brigada de Fuerzas Especiales No.9 “Patria”, está cumpliendo los lineamientos de las Normas ISO 27001 y 27002.

Figura 3.2.1 Resultados Globales de la encuesta

A continuación se muestran los resultados que se obtuvieron dentro de cada dominio de la Norma ISO 27002 y sección que fue dividida la encuesta:

- **Política de seguridad.**

Los resultados de forma global para el presente dominio se muestran a continuación: para el SI se tiene el 40%, mientras los resultados para la respuesta NO es el 60%, con estos resultados se puede concluir que las políticas de seguridad dentro de la Brigada de Fuerzas Especiales No.9 "Patria", no se están cumpliendo de manera adecuada.

Si			**No**	
5	100		5	100
2	**X**		3	**X**
X=	40.00%		**X=**	60.00%

Tabla 3.2.2 Resultados del Dominio: Políticas de Seguridad

- **Aspectos organizativos de la seguridad de la información**

Los resultados de forma global para el presente dominio se muestran a continuación: para el SI se tiene el 66.67%, mientras que el resultado para la respuesta NO es el 33.33%, con estos resultados se puede concluir que los aspectos organizativos dentro de la Brigada de Fuerzas Especiales No.9 “Patria”, se está cumpliendo considerablemente.

Si			No	
3	100		3	100
2	**X**		1	**X**
X=	66.67%		**X=**	33.33%

Tabla 3.2.3 Resultados del Dominio: Aspectos Organizativos de la Seguridad de la Información

- **Gestión de activos**

Los resultados de forma global para el presente dominio se muestran a continuación: para el SI se tiene el 57.14%, mientras que el resultado para la respuesta NO es el 42.86%, con estos resultados se puede concluir que la gestión de activos dentro de la Brigada de Fuerzas Especiales No.9 “Patria”, se está cumpliendo de manera regular.

Si			No	
14	100		14	100
8	**X**		6	**X**
X=	57.14%		**X=**	42.86%

Tabla 3.2.4 Resultados del Dominio: Gestión de Activos

- **Seguridad ligada a los recursos humanos**

Los resultados de forma global para el presente dominio se muestran a continuación: para el SI se tiene el 70%, mientras que el resultado para la respuesta NO es el 30%, con estos resultados se puede concluir que la seguridad ligada a los recursos humanos dentro

de la Brigada de Fuerzas Especiales No.9 “Patria”, no se están cumpliendo.

Si			No	
10	100		10	100
7	**X**		3	**X**
X=	70.00%		**X=**	30.00%

Tabla 3.2.5 Resultados del Dominio: Seguridad Ligada a Recursos Humanos

- **Seguridad física y ambiental**

Los resultados de forma global para el presente dominio se muestran a continuación: para el SI se tiene el 47.06%, mientras que el resultado para la respuesta NO es el 52.94%, con estos resultados se puede concluir que la seguridad física y ambiental dentro de la Brigada de Fuerzas Especiales No.9 “Patria”, se están cumpliendo pero no de la manera esperada.

Si			No	
17	100		17	100
8	X		9	X
X=	47.06%		**X=**	52.94%

Tabla 3.2.6 Resultados del Dominio: Seguridad Física y Ambiental

- **Gestión de comunicaciones y operaciones**

Los resultados de forma global para el presente dominio se muestran a continuación: para el SI se tiene el 66.67%, mientras que el

resultado para la respuesta NO es el 33.33%, con estos resultados se puede concluir que la gestión de comunicaciones y operaciones dentro de la Brigada de Fuerzas Especiales No.9 “Patria”, no se están cumpliendo, pero se podría mejorar luego del presente trabajo.

Si			No	
6	100		6	100
4	X		2	X
X=	66.67%		**X=**	33.33%

Tabla 3.2.7 Resultados del Dominio: Gestión de Comunicación de Operaciones

- **Control de acceso**

Los resultados de forma global para el presente dominio se muestran a continuación: para el SI se tiene el 20%, mientras que el resultado para la respuesta NO es el 80%, con estos resultados se puede concluir que el control de acceso al Datacenter dentro de la Brigada de Fuerzas Especiales No.9 “Patria”, no se está cumpliendo.

Si			No	
5	100		5	100
1	X		4	X
X=	20.00%		**X=**	80.00%

Tabla 3.2.8 Resultados del Dominio: Control de Acceso

- **Adquisición, desarrollo y mantenimiento de sistemas de información**

Los resultados de forma global para el presente dominio se muestran a continuación: para el SI se tiene el 60%, mientras que el resultado para la respuesta NO es el 40%, con estos resultados se puede concluir que la adquisición, desarrollo y mantenimiento de los Sistemas de la Información dentro del Datacenter de la Brigada de Fuerzas Especiales No.9 “Patria”, se están cumpliendo de manera regular, pero luego del presente trabajo se podría mejorar.

Si			**No**	
10	100		10	100
6	X		4	X
X=	60.00%		**X=**	40.00%

Tabla 3.2.9 Resultados del Dominio: Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

- **Gestión de incidentes de seguridad en la seguridad de la información**

Los resultados de forma global para el presente dominio se muestran a continuación: para el SI se tiene el 20%, mientras que el resultado para la respuesta NO es el 80%, con estos resultados se puede concluir que la gestión de incidentes de la seguridad de la información dentro del Datacenter de la Brigada de Fuerzas Especiales No.9 “Patria”, no se está cumpliendo de manera adecuada.

Si			No	
5	100		5	100
1	X		4	X
X=	20.00%		**X=**	80.00%

Tabla 3.2.10 Resultados del Dominio: Gestión de Incidentes de Seguridad

- **Gestión de la continuidad del negocio**

Los resultados de forma global para el presente dominio se muestran a continuación: para el SI se tiene el 50%, mientras que el resultado para la respuesta NO es el 50%, con estos resultados se puede concluir que la Gestión de la continuidad del Negocio dentro de la Brigada de Fuerzas Especiales No.9 “Patria”, es neutral.

Si			No	
4	100		4	100
2	X		2	X
X=	50.00%		**X=**	50.00%

Tabla 3.2.11 Resultados del Dominio: Gestión de la Continuidad del Negocio

- **Cumplimiento**

Los resultados de forma global para el presente dominio se muestran a continuación: para el SI se tiene el 57.14%, mientras que el resultado para la respuesta NO es el 42.86%, con estos resultados se

puede concluir que el cumplimiento dentro de la Brigada de Fuerzas Especiales No.9 “Patria”, se están cumpliendo en mínima porción.

Si			No	
7	100		7	100
4	X		3	X
X=	57.14%		**X=**	42.86%

Tabla 3.2.12 Resultados del Dominio: Cumplimiento

3.3 DIAGNÓSTICO GENERAL DE LA SEGURIDAD INFORMÁTICA

Una vez que se analizaron los resultados arrojados por las encuestas, se procedió a formar la matriz de riesgos, para identificar los activos que se encuentran expuestos a riesgos dentro de la Brigada de Fuerzas Especiales No.9 “Patria”.

La matriz de riesgo contiene los activos, definidos en Magerit (activos estándar), las valoraciones que se tendrán son: la magnitud del daño y la probabilidad de la amenaza que luego serán multiplicadas entre si para obtener el nivel de riesgo al que se encuentran sometidos los activos analizados.

La matriz de riesgo se encuentra a detalle en el **ANEXO A**

3.4 DATOS DEL SISTEMA DE SEGURIDAD INFORMÁTICA.

La Metodología MAGERIT, recomienda realizar cinco pasos, en el análisis de riesgos, que indica que los pasos 1, 2, 3,4 y 5 se siguen primero, obviando el paso 3, de forma que las valoraciones del impacto y/o riesgos sean realizadas sin salvaguardas desplegadas, con el objetivo de obtener estimaciones reales del impacto y/o riesgo potencial, para luego proceder a aplicar las salvaguardas

Para la identificación de los activos, se ha tomado los más relevantes para la institución con cada una de sus relaciones, teniendo en cuenta las dimensiones de seguridad y su respectiva valoración.

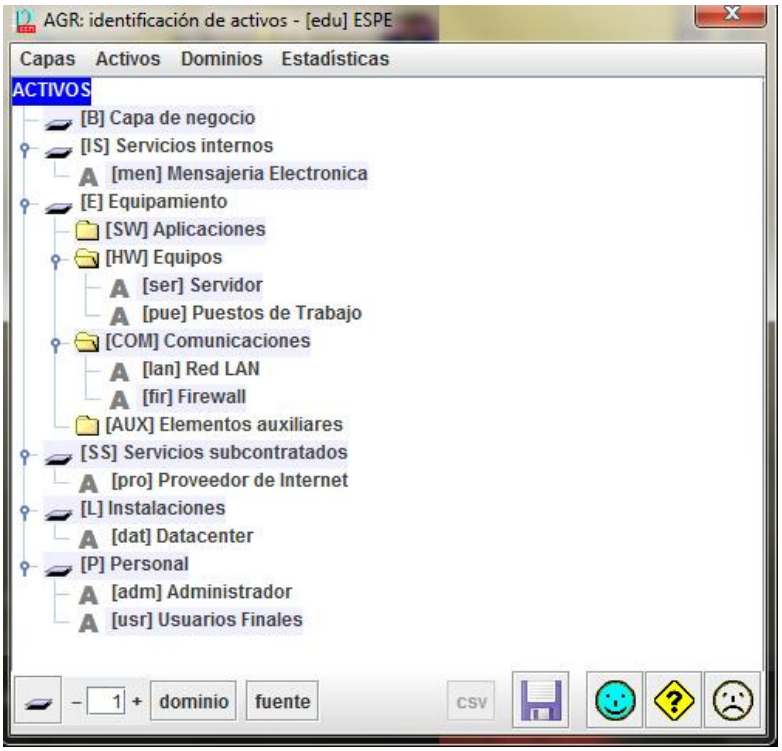

Figura 3.4.1 Identificación de Activos

La dependencia entre activos ayuda a identificar y valorar, tomando en cuenta en que puede ser perjudicado un activo superior por medio de las amenazas que pueda tener un activo inferior.

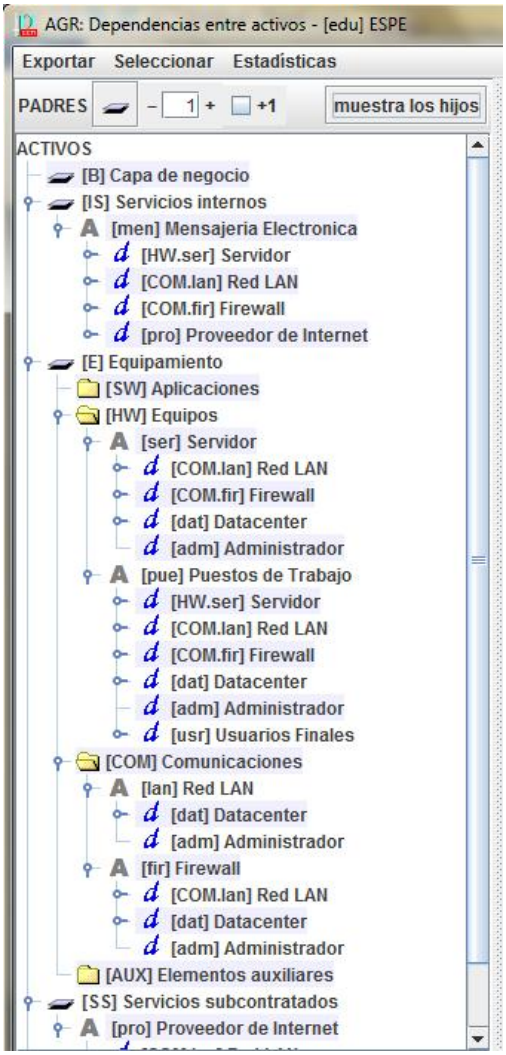

Figura 3.4.2 Creación de la dependencia entre activos

En la valoración de los activos, tiene referencia en identificación de activos y dependencias entre activos, para la valoración se identifica la dimensión en la que un activo es valioso.

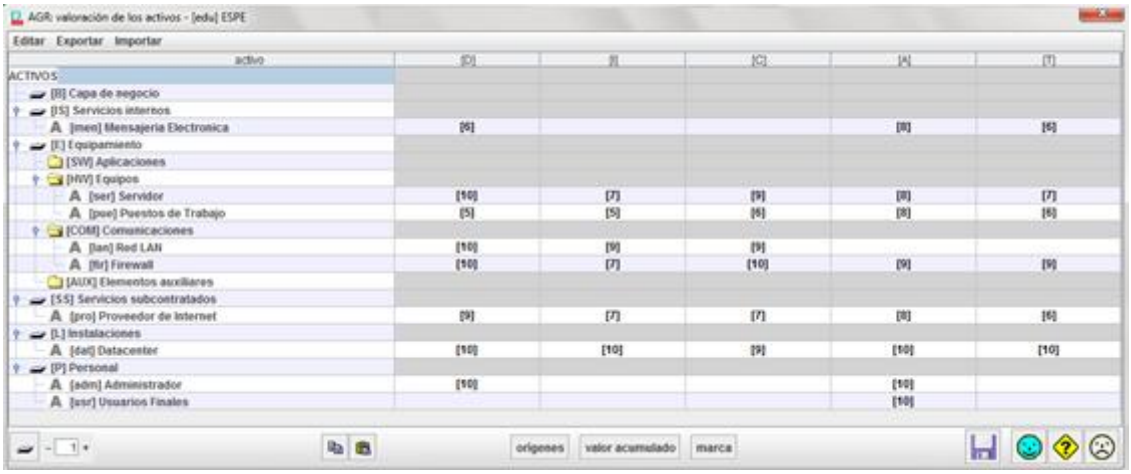

Figura 3.4.3 Valoración de Activos

En la identificación de las amenazas, se identifican las amenazas relevantes sobre cada activo, teniendo en cuenta las relaciones de las posibles amenazas.

A continuación se muestra la identificación de las diferentes amenazas que se encuentran en el centro de datos y dentro de cada capa.

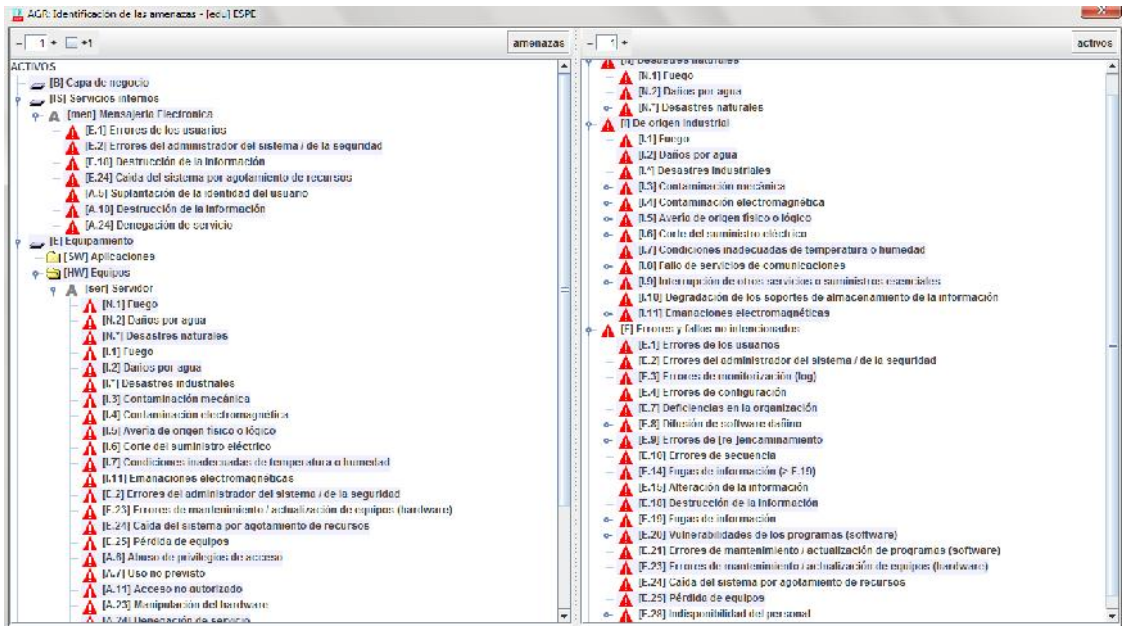

Figura 3.4.4 Identificación de Amenazas

Para la valoración de las amenazas, se estima la frecuencia y la degradación de la materialización de las amenazas sobre cada activo que se está analizando.

La valoración de las diferentes amenazas sobre los activos se tiene 5 rangos: **B:** Bajo, **M:** Medio**, A:** Alto y **MA:** muy Alto que es la degradación por niveles y porcentajes.

Valor		Criterio
4	Muy alto	Daño muy grave a la organización
3	Alto	Daño grave a la organización
2	Medio	Daño importante a la organización
1	Bajo	Daño menor a la organización
0	Despreciable	Irrelevante a efectos prácticos

Cuadro 1.[15] Valoración de los Activos

Para el análisis de riesgos del Datacenter de la Brigada “Patria”, se tomó la frecuencia y degradación en porcentajes.

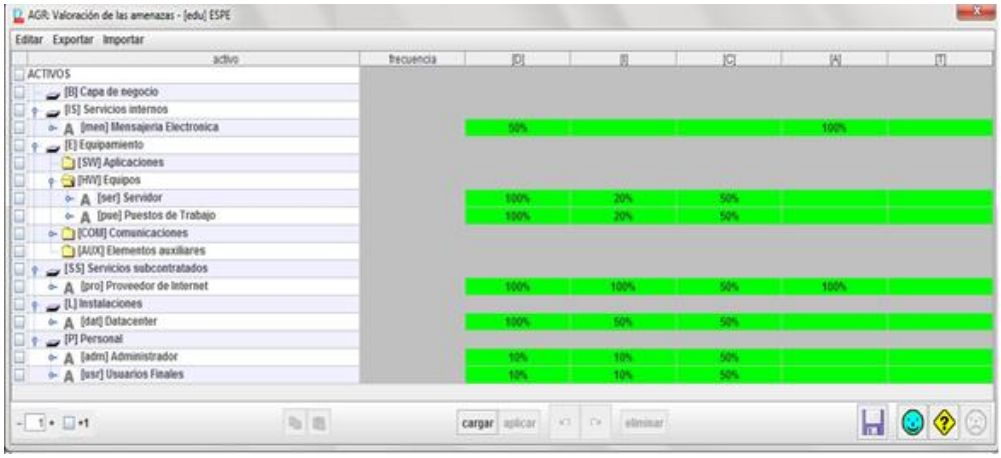

Figura 3.4.5 Valoración de Amenazas

[15] **Fuente**: Metodología Magerit, Administración Española

En la tarea de estimación del impacto se tiene el impacto residual y potencial al que se encuentran sometidos los activos de la Brigada “Patria”.

El resultado de la tarea de valoración de activos se tiene la matriz del impacto acumulado, la misma que se muestra a continuación.

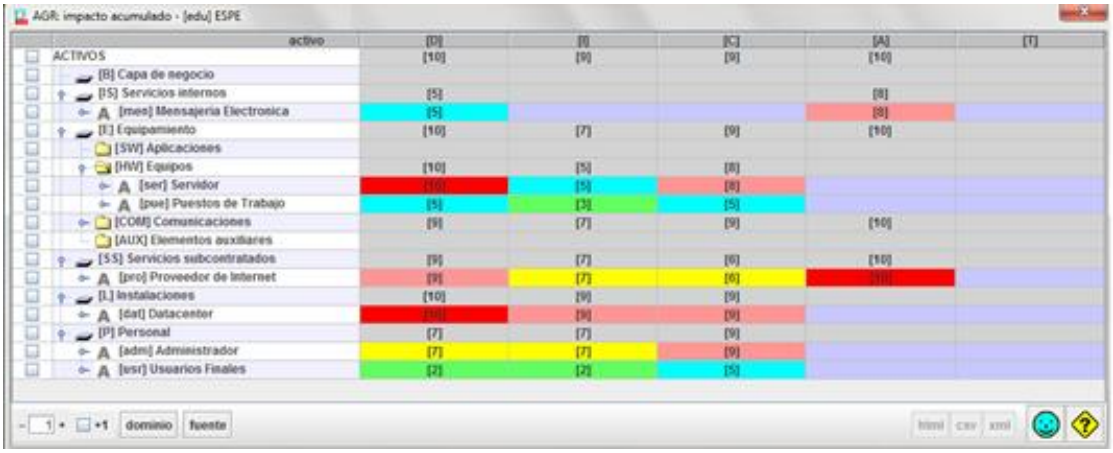

Figura 3.4.6 Matriz del Impacto Acumulado

3.4.1 MEDIOS HUMANOS.

Se tomaron dos activos, para ser sometidos al análisis de riesgos, los activos identificados para la capa de personal son: el Administrador y a los Usuarios Finales.

El administrador no se encuentra dependiendo de ningún otro activo, mientras que el activo de usuarios finales depende de la red LAN, el firewall, el proveedor de Internet el Datacenter y el administrador.

El activo: administrador tiene valoración de 10 en las dimensiones de disponibilidad y autenticidad, ya que es el encargado de gestionar:

permisos, mantenimiento, respaldos, entre otros. Mientras que los usuarios finales tienen valoración de 10 en la dimensión de autenticad.

En la identificación de amenazas se utilizó la biblioteca estándar de PILAR para asociar a los activos tomando en cuenta sus clases y dependencias.

3.4.2 MEDIOS TÉCNICOS.

Se tomaron los siguientes activos: La mensajería electrónica, servidores, puestos de trabajo, la red LAN, el firewall, el proveedor de Internet y el Datacenter, los mismos que serán sometidos al respectivo análisis de riesgos.

Dentro de las dependencias, se especificó la relación entre activos principales padre e hijo, para la obtención del árbol de activos.

Para la valoración de activos, se eligió los niveles de acuerdo a la valoración entre activos sus vulnerabilidades, las mismas que fueron reflejadas en pilares.

En la identificación de amenazas se utilizó la biblioteca estándar de PILAR para asociar a los activos tomando en cuenta sus clases y dependencias.

Para la valoración de amenazas se tomó en cuenta la frecuencia y la probabilidad de que la amenaza se haga efectiva y la misma que ha sido tomada en porcentaje.

Una vez realizado el proceso anterior se procede a la obtención de los resultados.

El análisis del riesgo acumulado se da a partir del riesgo de los activos inferiores.

3.4.3 MEDIDAS Y PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA.

Una vez conocidas las matrices de riesgo y de impacto acumulado se procede a aplicar las salvaguardas dentro del software PILAR que permitirán hacer frente a las amenazas.

- **De protección física:** Este tipo de seguridad se encuentra enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza, y las mismas se analizan para aplicar las salvaguardas necesarias para mantener protegido el Datacenter; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos físicos.
- **A las áreas con tecnologías instaladas:** Para aplicar las salvaguardas se consideraron las áreas vitales y reservadas en correspondencia con el tipo de información que se procesa, intercambia, reproduce o conserva y considerando el impacto que pueda ocasionar para la institución mediante la afectación de los activos o recursos que en ellas se encuentren.

- **A las tecnologías de información:** Se tomó en cuenta la posición de las tecnologías de información destinadas al procesamiento de información con alto grado de confidencialidad o sensibilidad del Datacenter de forma que se evite la visibilidad de la información a distancia, minimice la posibilidad de captación de las emisiones electromagnéticas y garantice un mejor cuidado y conservación de las mismas.

  Las salvaguardas también ayudarán a garantizar el control de las tecnologías de información existentes, durante su explotación, conservación, mantenimiento y traslado.

- **A los soportes de información:** Se implementaron salvaguardas al sistema de control establecido sobre los soportes magnéticos de información refiriéndose entre otros aspectos a:

  Lo relacionado con la identificación de los soportes removibles autorizados a utilizar dentro de la entidad, incluyendo su identificación física y lógica.

  Las condiciones de conservación de los soportes, especificando las medidas que garanticen la integridad y confidencialidad de la información que en ellos se recoge.

  Las salvaguardas que se establecen para garantizar la integridad y confidencialidad de la información clasificada o limitada durante el traslado de los soportes.

- **Técnicas o lógicas:** Se especifican las salvaguardas de seguridad que han sido implementadas a través de software y hardware.
    - **Identificación de usuarios.**

Se aplicaron salvaguardas para la identificación de los usuarios ante los sistemas, servicios y aplicaciones existentes, especificando:

- Como se asignan los identificadores de usuarios.
- Si existe una estructura estándar para la conformación de los identificadores de usuarios.
- Quien asigna los identificadores de usuarios.
- Como se eliminan los identificadores de usuarios una vez que concluya la necesidad de su uso y como se garantiza que estos no sean utilizados nuevamente.
- Proceso de revisión de utilización y vigencia de los identificadores de usuarios asignados.

- **Control de acceso a los activos y recursos.**

Mediante las salvaguardas se trata de asegurar el acceso autorizado a los activos de información y recursos informáticos que requieren restricciones a su empleo, especificando:

- A que activos y recursos se le implementan medidas de control de acceso.
- Métodos de control de acceso utilizados.
- Quien otorga los derechos y privilegios de acceso.
- A quien se otorgan los derechos y privilegios de acceso.

- Como se otorgan y suspenden los derechos y privilegios de acceso.

Las salvaguardas implementadas tratan de llegar a una política de “mínimo privilegio”, en el sentido de otorgar a cada usuario sólo los derechos y privilegios que requiera para el cumplimiento de las funciones que tenga asignadas.

3.5 IDENTIFICACIÓN DE LOS PROCESOS CRÍTICOS DEL DATA CENTER DE LA BRIGADA PATRIA.

Los procesos críticos identificados luego de realizado el análisis con el software PILAR se muestra en la matriz de Riesgo Acumulado.

La Matriz de Riesgos Acumulado muestra los activos con su respectivo riesgo, en cada dimensión de la seguridad como lo son: Disponibilidad, Integridad, Confidencialidad, Autenticidad y trazabilidad.

Para diferenciar cada activo con su dimensión de riesgo, la herramienta muestra en diferentes colores, según la intensidad de daño que estos provoquen a la información, en este caso se tomará como referencia los de color rojo, ya que son riesgos más considerables.

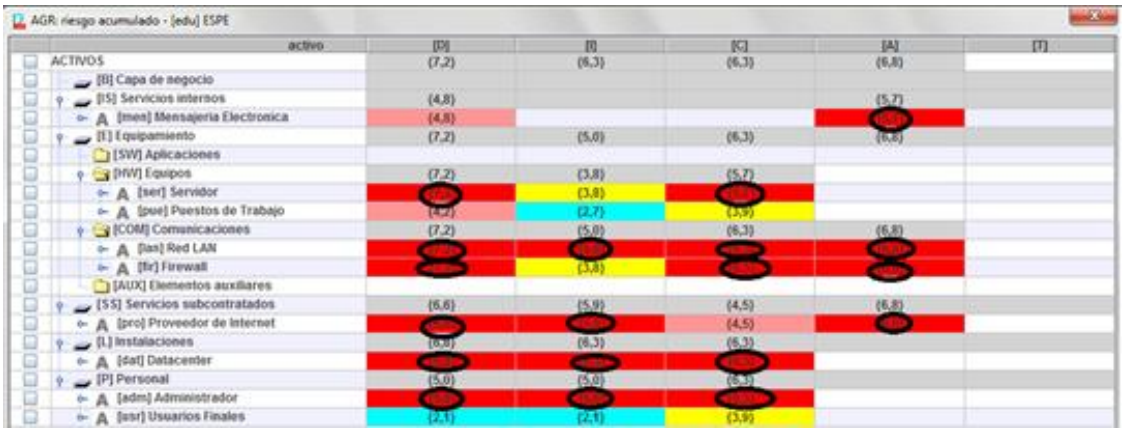

Figura 3.5 Matriz del Riesgo Acumulado

3.6 DESARROLLO DE ANÁLISIS TÉCNICO.

3.6.1 INFORME TÉCNICO DE LAS FALENCIAS ENCONTRADAS.

Nombre del Área: Área Informática

Identificación de la Entidad: Brigada de Fuerzas Especiales No. 9 “Patria”

Introducción.

El presente informe muestra los resultados obtenidos durante el análisis de la Seguridad informática de la Brigada “Patria”, con la utilización de la herramienta PILAR.

El objetivo de analizar los riesgos a los que se encuentra expuesto el Datacenter y para dar una visión a la Brigada de cómo contrarrestarlos y así tome acciones antes de que se tengan sucesos negativos para la información que se maneja dentro de dicha institución.

Para poder identificar de mejor manera las amenazas dentro del centro de datos, se presenta el informe de amenazas que es proporcionado por la

herramienta PILAR, el mismo que se muestra en matrices dando a conocer los procesos críticos de cada activo.

Hallazgos

Una vez verificado el informe de amenazas, se puede verificar cuales son los posibles riesgos a que se hallan expuestos los activos de la Brigada “Patria”.

Dentro de los riesgos encontrados se tienen:

- Caída del sistema por agotamiento de recursos
- Suplantación de la identidad del usuario
- Denegación de servicio
- Fuego
- Daños por agua
- Desastres naturales
- Avería de origen físico o lógico
- Corte del suministro eléctrico
- Condiciones inadecuadas de temperatura o humedad
- Abuso de privilegios de acceso
- Acceso no autorizado
- Manipulación del hardware
- Ataque destructive

Conclusiones:

- Como resultado de la Auditoria se puede manifestar que se ha cumplido con evaluar cada uno de los objetivos de la Norma ISO 27001.
- El Datacenter presenta deficiencias sobre todo en el cumplimiento de Normas de Seguridad, porque no cumple las normas como es debido.

- Se debe destacar que el sistema ofimático no ha sido explotado en su totalidad.

Recomendaciones:

- Elaborar un plan de emergencia que ayudé a contrarrestar de forma rápida y activa la caída del sistema por agotamiento de recursos.
- Realizar un manual de seguridad que permita conocer a los usuarios que información deben proporcionar al momento de ingresar a sitios web.
- Realizar mantenimiento periódico de los Sistemas de Fuego.
- Elaborar un calendario de mantenimiento correctivo y preventivo de rutina periódico.
- Tener usuarios administradores únicamente para los encargados del Datacenter.
- Elaborar toda la documentación técnica correspondiente a los Sistemas implementados y establecer normas y procedimientos para las implementaciones y actualización.
- Asignar un responsable para todos los procesos del Datacenter.
- Tener en mente que la información es el activo más importante de la organización y por eso se debe considerar como un coste necesario.

3.6.2 ANÁLISIS CONFRONTATIVO CON LAS NORMAS ISO 27001 Y 27002

ISO 27001	ISO 27002
Es auditable	Más precisa y detallada
Se obtiene una certificación	No se puede obtener una certificación de esta norma
Define el Sistema de Gestión de Seguridad de la Información (SGSI)	No es una norma de Gestión
	Código de Buenas Practicas
Controla	Ayuda a mejorar la Seguridad de la Información
Establece requisitos	Establece sugerencias
	No distingue entre controles aplicables
Evalúa riesgos cobre cada control	
Está diseñada con un enfoque preciso	Implementa controles

Tabla 3.5.2 Análisis Confrontativo con las Normas ISO 27001 y 27002

En la actualidad se tiene en mente que las normas ISO 27001 e ISO 27002 son equivalentes, pero eso no es verdad, ya que son muy distintas.

Las diferencia principal entre estas dos normas es que la norma (27002) es un código de buenas prácticas y norma (27001) una especificación.

La ISO 27002 es una guía para mejorar la seguridad de la información y posee una serie de apartados a tratar en relación a la seguridad, Los objetivos de seguridad a perseguir, una serie de consideraciones (controles) a tener en cuenta para cada objetivo y un conjunto de "sugerencias" para cada uno de esos controles.

Sin embargo, la propia norma ya indica que no existe ningún tipo de priorización entre controles, y que las "sugerencias" que realiza no tienen por qué ser ni siquiera convenientes, en función del caso en cuestión.

La ISO 27001 habla de los controles de forma residual. El núcleo de la norma anterior queda reducido a un listado de objetivos de control y controles incluidos en un anexo. No aparecen en el cuerpo de la norma, porque en absoluto son la parte más importante. Porque lo que importa en esta norma es la gestión de la seguridad, en forma de Sistema de Gestión.

Lo que importa en la ISO 27001 es que los riesgos se Analicen y se Gestionen, que la seguridad se Planifique, se Implemente y, sobre todo, se revise, corrija y mejore.

También se puede decir que sin la descripción proporcionada por la ISO 27002, los controles definidos en la ISO 27001 no se podrían ser implementados. Sin embargo, sin el marco de gestión de la ISO 27001, la

ISO 27002 sería simplemente un esfuerzo aislado de implementación para la seguridad de la información.

ESPACIO EN BLANCO

INTENCIONAL

CAPITULO 4

4. INFORMES

4.1 INFORME EJECUTIVO

La evaluación técnica de la seguridad informática del Datacenter de las Fuerzas Especiales No. 9 “Patria”, fue elaborada en base a la información provista por el personal encargado.

Para el respectivo análisis se tomaron las normas ISO27001 (Gestión de la Seguridad de la Información) y la ISO 27002 (Código de Buenas Prácticas), además se utiliza la metodología MAGERIT con su respectiva herramienta PILAR, también se realizó la encuesta y las observaciones realizadas durante las visitas al Datacenter.

Con respecto a los dominios y controles que se llevaron a cabo de acuerdo con la siguiente tabla:

ESPACIO EN BLANCO INTENCIONAL

DOMINIO	CONTROLES
A. Política de seguridad	• Documento de política de seguridad de la información
B. Organización de la seguridad	• Organización Interna • Relaciones con Terceros
C. Control y clasificación de los recursos de información	• Previa a la Contratación • Mientras dure la contratación • Fin de la contratación o cambio de puesto de trabajo
D. Seguridad del personal	• Previa a la Contratación • Mientras dure la contratación • Fin de la contratación o cambio de puesto de trabajo
E. Seguridad física y del entorno	• Áreas seguras
F. Manejo de las comunicaciones y las operaciones	• Responsabilidades y procedimientos de operación • Gestión de servicios prestados por terceros • Planificación y aceptación por terceros • Protección frente a código y código descargable • Copias de seguridad • Gestión de seguridad de las redes • Tratamiento de soportes de información

	• Intercambios de información • Servicios de comercio electrónico • Supervisión
G. Control de acceso	• Requisitos de Control de Acceso • Gestión de Usuarios • Responsabilidades de los Usuarios • Control de Acceso a la Red • Control de acceso a sistemas de operación • Control de acceso a datos y a operaciones • Equipos móviles y tele-trabajo
H. Desarrollo y mantenimiento de los sistemas	• Comunicación de incidentes y debilidades • Gestión de incidentes y mejoras
I. Manejo de la continuidad de la empresa	Seguridad de la información en relación a la gestión de la continuidad
J. Cumplimiento o Conformidad	• Satisfacción de requisitos legales • Cumplimiento de políticas, normas y reglamentos técnicos • Consideraciones sobre auditoria de los sistemas de información
K. Cumplimiento	Satisfacción de requisitos legales Cumplimiento de políticas, normas y reglamentos técnicos Consideraciones sobre auditoria de los sistemas de información

Tabla 4.1 Reporte de Dominios

A. **Dominio: Política de Seguridad**

Observación:

- La institución ha llevado una política de seguridad interna de acuerdo con las necesidades de los usuarios.

Riesgo:

- Según las evidencias encontradas sobre los riesgos, se puede llegar a la conclusión que es poco probable que las amenazas se materialicen.

Causa:

- Existe documentación que no está actualizada.

Recomendaciones:

- Se debe actualizar la documentación y el manual de políticas de seguridad,
- El encargado del Datacenter debe verificar que se actualicen de manera periódica las políticas de seguridad.

B. **Dominio: Aspectos Organizativos de la Seguridad de la Información**

Observación:

- Dentro de la Brigada no existen programas o capacitaciones frecuentes de Seguridad.

Riesgo:

- Según las evidencias encontradas sobre los riesgos, se puede llegar a la conclusión que es probable que las amenazas se materialicen en la organización ya que el personal encargado del Datacenter debería estar en capacitación continua.

Causa:

- Se han realizado cursos de seguridad, pero no se los ha implantado de manera correcta.

Recomendación:

- Implementar los conocimientos adquiridos durante los cursos de seguridad informática.

C. Dominio: Gestión de Activos

Observación:

- Se debe designar responsabilidades, si fuera el caso a cada uno de los activos, también se necesita tener un inventario de los activos que se posee actualmente y cuál es el papel que desempeñan dichos activos dentro de la organización

Riesgo:

- En casos de emergencia, el personal podría evadir sus responsabilidades

Causa:

- No se han definido el área específica a la cual corresponde cada activo

Recomendación:

- Designar de manera formal al personal encargado del Datacenter, para que se haga responsable de cada activo.

D. Dominio: Seguridad relacionada con los recursos Humanos

Observación:

- Falta de definición de responsabilidades para el personal encargado.

Riesgo:

- Podrían ocurrir fallas humanas, robo, e incluso fraude dentro de las instalaciones.

Causa:

- Falta de comunicación entre el área informática y las áreas anexas.

Recomendación:

- Designar de manera formal al personal encargado del Datacenter, para que se haga responsable de cada activo.

E. Dominio Seguridad Física y del Entorno

Observación:

- Falta asegurar los equipos del Datacenter.

Riesgos:

- El ingreso de personal no autorizado puede causar que se realicen actividades ilícitas.
- Se puede tener daño de los equipos por falta del suministro eléctrico.

Causa:

- No se tiene un sistema de seguridad en la puerta de ingreso al Datacenter.
- No existe una persona que se encargue de verificar quien entra al área del Centro de datos.

Recomendaciones:

- Supervisar cuales son las personas que tienen permiso de acceder al Datacenter.
- Los proveedores de servicios siempre deben ingresar acompañados de la persona encargada del Datacenter, para supervisar el trabajo realizado.
- Verificar que los dispositivos de alimentación extra se encuentren funcionando correctamente.

F. Dominio: Gestión de Comunicaciones y operaciones

Observación:

- Falta documentar los procedimientos de operación, implementar las copias de seguridad y supervisar con frecuencia.

Riesgos:

- Cambios no autorizados dentro de los sistemas o en la información.
- Uso mal intencionado de los sistemas.
- Perdida de información.
- Fallos en los sistemas.
- Ejecución de código malicioso e inseguro.
- Uso inadecuado de la información, con fines malintencionados.

Causas:

- Daño del sistema a mediano o a largo plazo.
- Daño de los sistemas de información.
- Carga excesiva de procesos.

Recomendaciones:

- Documentar los procesos realizados.
- Implementar procesos para preservar la integridad y la confidencialidad de la información.

G. Dominio: Control de Acceso

Observación:

- A las Políticas de Seguridad de los equipos no se le pone la debida atención.

Riesgos:

- Pérdida de los equipos e incluso de la información.
- Acceso no autorizado de personas externas a la institución.

Causas:

- Perdida de información del personal que se encuentra en la Brigada.
- Espionaje por parte de personal externo,

Recomendaciones:

- Supervisar las actividades del personal que realice lo que su perfil de usuario le permite acceder.
- Monitorear los accesos a la red frecuentemente.

H. Dominio: Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

Observación:

- No se han implantado garantías de procesamiento de información, controles criptográficos y seguridad de los archivos del sistema.

Riesgos:

- Modificación y pérdida de información.
- No se identifican los procesos vulnerables para la información.

Causas:

- Los controles criptográficos no aplican por lo que la información puede perderse.
- El acceso a la red de información sin los perfiles necesarios.

Recomendaciones:

- Se necesita tener políticas de seguridad definidas para que el personal pueda acceder con perfiles de usuario restringidos.
- Se necesita implementar un plan de Contingencia de Seguridad.

I. Dominio: Gestión de incidentes de seguridad de Información

Observación:

- Se cumplen los controles en un 50%

Riesgo:

- Los riesgos se pueden materializar, ya que tiene un 50% de probabilidad que ocurran

Causa:

- Pueden ocurrir incidentes y no se los va a poder solucionar de manera eficiente

Recomendaciones:

- Documentar los incidentes ocurridos, para poder solucionarlos en menor tiempo o realizar el seguimiento de los mismos.

J. Dominio: Gestión de la continuidad del negocio

Observación:

- No aplica este dominio

Riesgo:

- No se pueden aplicar el Plan de Continuidad porque van a fallar en un 100%, ya que no ha sido implementado.

Causa:

- No existe un Plan de Continuidad

Recomendaciones:

- Realizar un Plan de Contingencia, probarlo y actualizarlo

K. Dominio: Cumplimiento

Observación:

- Las revisiones periódicas de las políticas de seguridad no han sido registradas con frecuencia.

Riesgo:

- No tener una visión de las cosas que están afectando a la seguridad de la información.

Causa:

- No tener manuales de reglas actualizados.

Recomendaciones:

- Revisar el regulamiento de las reglas de seguridad y procedimientos apropiados y actualizados periódicamente.

4.2 INFORME DETALLADO

4.2.1 INTRODUCCIÓN

El presente informe se centra en la Evaluación de la Seguridad Informática de la Brigada Fuerzas Especiales No. 9 “Patria”, el mismo que ha sido preparado para informar al personal encargado del Datacenter y a las autoridades de la Brigada sobre el análisis realizado y así ayudar a resguardar los activos de la institución.

4.2.2 METODOLOGÍA

Para realizar el informe se tomó como referencia la norma ISO 27002, la misma que es un estándar para la Seguridad Informática 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 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.

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

El informe que se presenta a continuación muestra los resultados de la evaluación en cada uno de los dominios de la norma ISO27001 que fueron evaluados.

4.2.3 OBJETIVOS

4.2.3.1 Objetivo General

Describir los hallazgos encontrados durante la Evaluación Técnica Informática de las seguridades del Datacenter de la Brigada No.9 “Patria”, considerando como referencia los estándares ISO 27001 e ISO 27002.

4.2.3.2 Objetivo Específicos

- Comunicar los resultados de la Evaluación Técnica a los dirigentes y funcionarios de la Brigada “Patria”.
- Informar los hallazgos encontrados, conclusiones y recomendaciones para determinar acciones correctivas apropiadas para atenuar riesgos.

4.2.4 ALCANCE

El presente informe detallado cubre los dominios y los controles de la norma ISO 27002, con cada uno de las salvaguardas que se han implementado para atenuar los riesgos encontrados.

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 y encargados del Datacenter de la Brigada “Patria”, se encuentren en capacidad de aplicar medidas de seguridad para que la información se mantenga disponible, sea confiable y oportuna.

4.2.5 ANÁLISIS DE LOS RESULTADOS

Los resultados presentados a continuación son los arrojados por la herramienta PILAR.

4.2.5.1 Dominio: Política de Seguridad

Control:

- Documento de Política de Seguridad de la Información.

Objetivo:

- Proporcionar la guía y apoyo de la Dirección para la Seguridad de la Información en relación a los requisitos del negocio y a las leyes y regulaciones relevantes.

Principios:

- La Dirección debería establecer una Política clara y en línea con los objetivos de la Organización y demostrar su apoyo y compromiso con la Seguridad de la Información mediante la publicación y mantenimiento de una Política de Seguridad de la Información.

Condición:

- Disponen de normas, procedimientos y controles de la seguridad que en su mayoría están desactualizados

Evidencia:

Cuestionario de Auditoria Informática y aplicación de la herramienta PILAR para el Datacenter de la Brigada De Fuerzas Especiales No. 9 “Patria”

Gráfico:

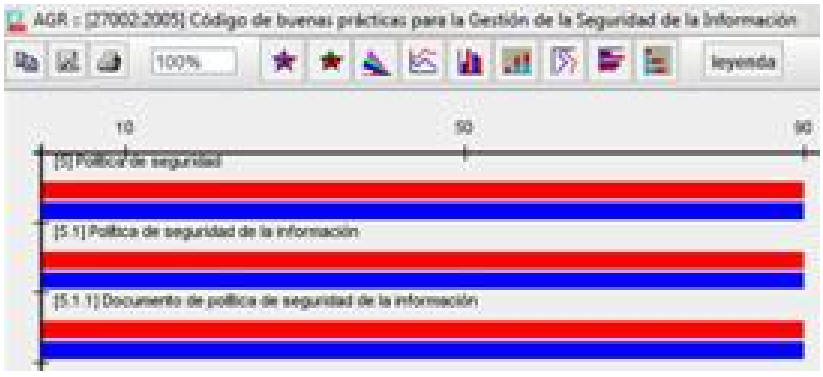

Figura 4.2.5.1 Gráfico de Hallazgos encontrados en PILAR (Política de Seguridad)

Riesgo:

- Según las evidencias encontradas sobre los riesgos, se puede llegar a la conclusión que es probable que las amenazas se materialicen.

Causa:

- Existe documentación que no se actualizado.

Salvaguardas:

Para reducir el riesgo de que las amenazas se materialicen fue necesario aplicar la siguiente salvaguarda:

- **G[321]** Los Documentos de políticas de seguridad deben ser aprobados y respaldados por la dirección y respaldados por la dirección

Gráfico:

Figura 4.2.5.1 Gráfico de Salvaguardas aplicadas en PILAR (Política de Seguridad)

Recomendaciones:

- Se debe actualizar la documentación, el manual de Políticas de Seguridad en el transcurso de tres meses deberá ser actualizado por las personas encargadas del Datacenter.
- El encargado del Datacenter debe verificar que se actualicen de manera periódica las Políticas de Seguridad

4.2.5.2 Dominio: Aspectos Organizativos de la Seguridad de la Información

Controles:

- Organización Interna.
- Relaciones con Terceros.

Objetivo:

- Gestionar la seguridad de la información dentro de la Organización.

Principios:

- Se debería establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la Organización.
- La dirección debería aprobar la Política de Seguridad de la Información, asignar los roles de seguridad, coordinar y revisar la implantación de la Seguridad en toda la Organización.

Condiciones:

- No existen programas o capacitaciones frecuentes de seguridad.
- No se revisa la organización de la seguridad periódicamente con una empresa externa.

Evidencia:

Cuestionario de Auditoria Informática y aplicación de la herramienta PILAR para el Datacenter de la Brigada De Fuerzas Especiales No. 9 “Patria”

Gráfico

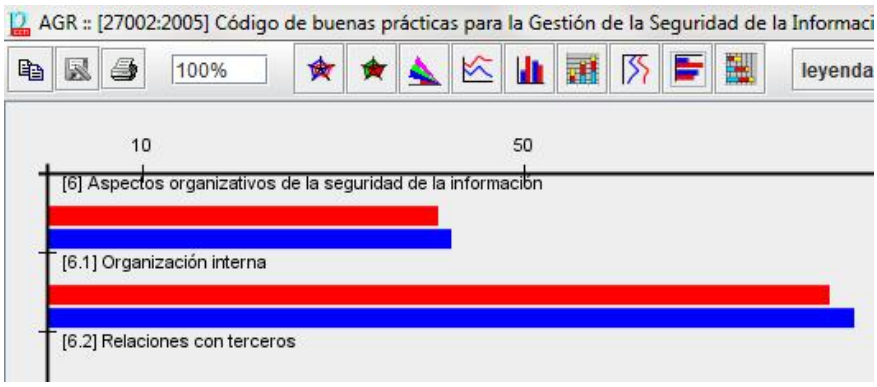

Figura 4.2.5.2 Gráfico de Hallazgos encontrados en PILAR (Aspectos Organizativos de la Seguridad de la Información)

Riesgo:

- Según las evidencias encontradas sobre los riesgos, se puede llegar a la conclusión que es probable que las amenazas se materialicen en la Organización Interna.

Causa:

- Se han realizado cursos de seguridad, pero no se los ha implantado de manera inadecuada.

Salvaguardas:

Asignación de responsabilidades relativas a la seguridad de la Información

- **G[133]** Responsabilidad de la seguridad de la información

Acuerdos de confidencialidad

- **G[P6441]** Inclusión de cláusulas de confidencialidad en los contratos laborales

Recomendaciones:

- Implementar o contratar cursos, para que los conocimientos adquiridos sean puestos en práctica.

Gráfico:

Figura 4.2.5.2 Gráfico de Salvaguardas aplicadas en PILAR (Aspectos Organizativos de la Seguridad de la Información)

4.2.5.3 Dominio: Gestión de Activos

Controles:

- Responsabilidad sobre los activos.
- Clasificación de la Información.

Objetivos:

- Alcanzar y mantener una protección adecuada de los activos de la Organización
- Asegurar que se aplica un nivel de protección adecuado a la información.

Principios:

- Todos los activos deberían ser justificados y tener asignado un propietario.
- Se deberían identificar a los propietarios para todos los activos y asignarles la responsabilidad del mantenimiento de los controles adecuados. La implantación de controles específicos podría ser delegada por el propietario convenientemente. No obstante, el propietario permanece como responsable de la adecuada protección de los activos.
- El término “propietario” identifica a un individuo o entidad responsable, que cuenta con la aprobación del órgano de dirección, para el control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término “propietario” no significa que la persona disponga de los derechos de propiedad reales del activo.

Condición:

- No se ha realizado la clasificación de la información de acuerdo a la criticidad.

Evidencia:

Cuestionario de Auditoria Informática y aplicación de la herramienta PILAR para el Datacenter de la Brigada De Fuerzas Especiales No. 9 “Patria”.

Gráfico:

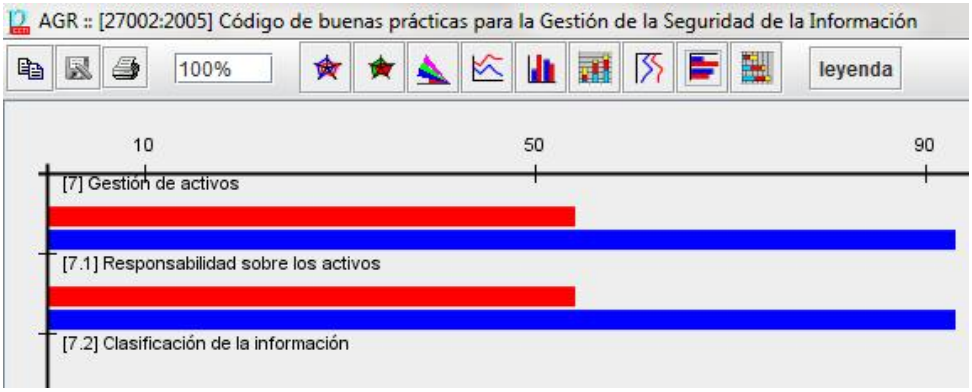

Figura 4.2.5.3 Gráfico de Hallazgos encontrados en PILAR (Gestión de Activos)

Riesgo:

- En casos de emergencia, el personal podría evadir sus responsabilidades.

Causa:

- No se han definido el área específica a la cual corresponde cada activo.

Salvaguardas:

- No aplica, ya que el riesgo es mínimo

Recomendaciones:

- Designar de manera formal al personal encargado del Datacenter, para que se haga responsable de cada activo.

Gráfico:

Figura 4.2.5.3 Gráfico de Salvaguardas Aplicadas en PILAR (Gestión de Activos)

4.2.5.4 Dominio: Seguridad relacionada con los recursos Humanos

Control:

- Previa a la Contratación.
- Mientras dure la contratación.
- Fin de la contratación o cambio de puesto de trabajo.

Objetivo:

- Asegurar que los empleados, contratistas y usuarios de terceras partes entiendan sus responsabilidades y sean aptos para las funciones que desarrollen. Reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.
- Asegurar que los empleados, contratistas y terceras partes son conscientes de las amenazas de seguridad, de sus responsabilidades y obligaciones y que están equipados para cumplir con la política de seguridad de la

organización en el desempeño de sus labores diarias, para reducir el riesgo asociado a los errores humanos.

- Garantizar que los empleados, contratistas y terceras personas abandonan la organización o cambian de empleo de forma organizada.

Principios:

- Las responsabilidades de la seguridad se deberían definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo.
- Se debería definir las responsabilidades de la Dirección para garantizar que la seguridad se aplica en todos los puestos de trabajo de las personas de la organización.
- Se deberían establecer las responsabilidades para asegurar que el abandono de la organización por parte de los empleados, contratistas o terceras personas se controla, que se devuelve todo el equipamiento y se eliminan completamente todos los derechos de acceso.

Condición:

- Se pone poca atención a la Seguridad de la Información y baja del personal.
- No se documentan los incidentes de manera adecuada.

Evidencia:

Cuestionario de Auditoria Informática y aplicación de la herramienta PILAR para el Datacenter de la Brigada De Fuerzas Especiales No. 9 “Patria”.

Gráfico:

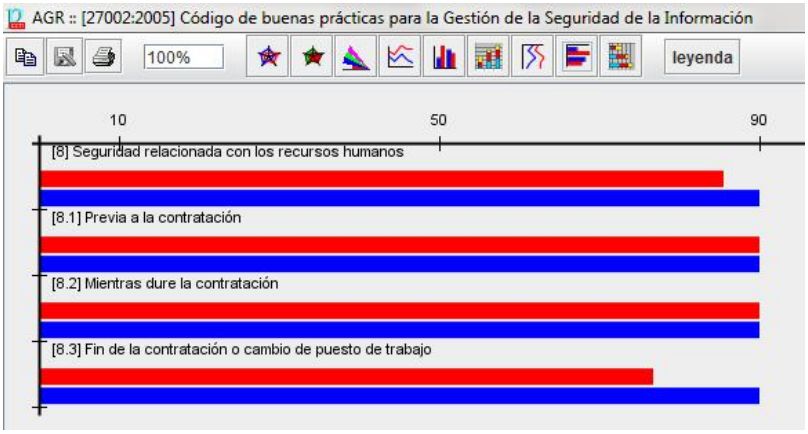

Figura 4.2.5.4 Gráfico de Hallazgos encontrados en PILAR (Seguridad relacionada con los recursos Humanos

Riesgo:

- Podrían ocurrir fallas humanas, robo, e incluso fraude dentro de las instalaciones.

Causa:

- Falta de comunicación entre el área Informática y las áreas anexas.

Salvaguardas:

Funciones y responsabilidades

- [P44] Se tienen en cuenta los requisitos de seguridad de los puestos de trabajo
- [P43]Se han determinado las responsabilidades en materia de seguridad de los puestos de trabajo

Acuerdos de confidencialidad

- [P6441]Inclusión de cláusulas de confidencialidad en los contratos laborales

Procedimiento Disciplinario

- [P6451]Régimen Sancionador por incumplimiento

Finalización de la relación laboral

- [P6462] Recuperación de los elementos se seguridad devolver (llaves, tarjetas, etc.)
- [P6463]Comunicación de la baja a los responsables de seguridad y administradores del sistema

Recomendaciones:

- Designar de manera formal al personal encargado del Datacenter, para que se haga responsable de cada activo.

Gráfico:

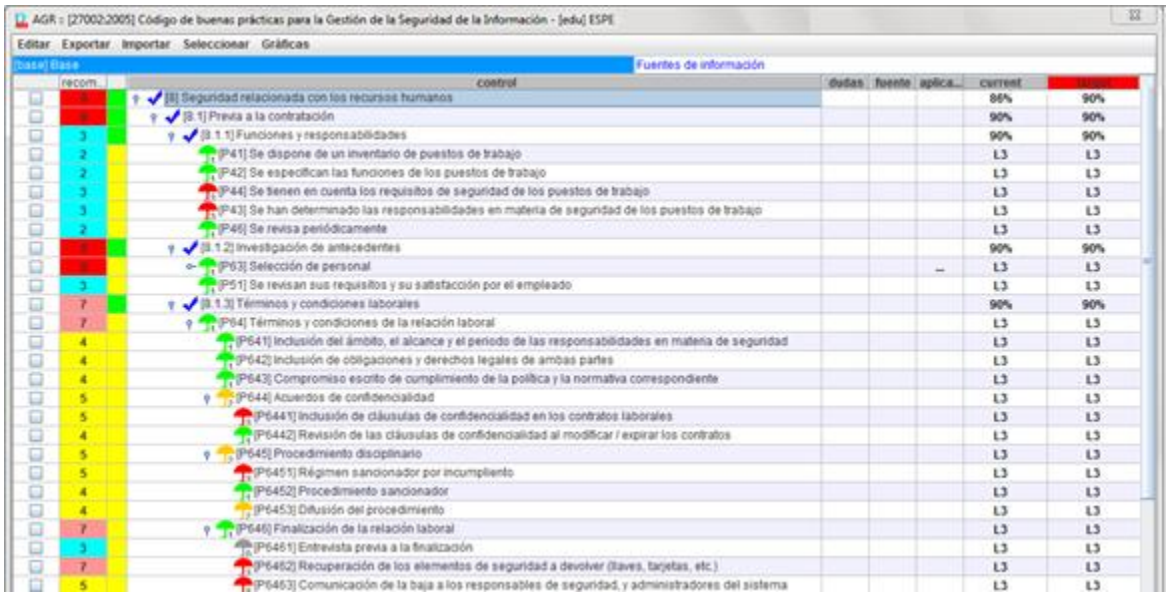

Figura 4.2.5.4 Gráfico de Salvaguardas aplicadas en PILAR (Seguridad relacionada con los recursos Humanos)

4.2.5.5 Dominio: Seguridad Física y del Entorno

Control:

- Áreas seguras.

Objetivo:

- Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de la organización.
- Evitar la pérdida, daño, robo o puesta en peligro de los activos e interrupción de las actividades de la organización.

Principios:

- Los servicios de procesamiento de información sensible deberían ubicarse en áreas seguras y protegidas en un perímetro de seguridad definido por barreras y controles de entrada adecuados. Estas áreas deberían estar protegidas físicamente contra accesos no autorizados, daños e interferencias.
- Deberían protegerse los equipos contra las amenazas físicas y ambientales. La protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo.

Condición:

- Se observó una sola puerta extra de acceso al Datacenter.
- No existen controles adicionales al personal propio y ajeno del Datacenter.
- Aun no se ha implantado procedimientos de seguridades a los equipos que han sido dados de baja.
- No se incluye seguridad en equipos móviles.

Evidencia:

Cuestionario de Auditoria Informática y aplicación de la herramienta PILAR para el Datacenter de la Brigada De Fuerzas Especiales No. 9 “Patria”

Gráfico:

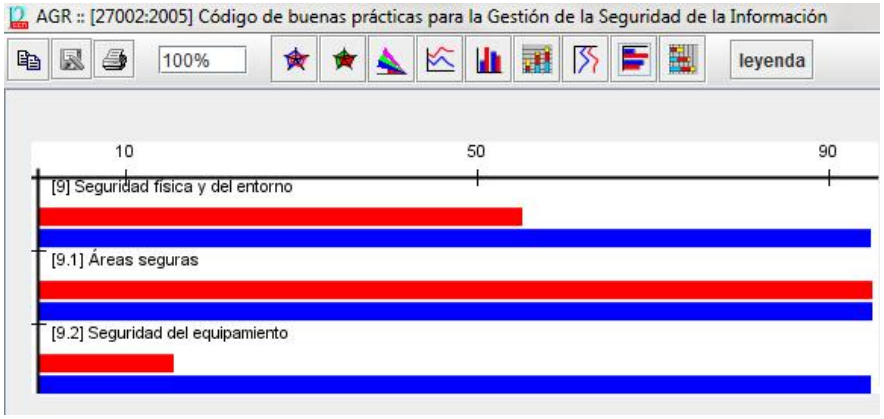

Figura 4.2.5.5 Gráfico de Hallazgos encontrados en PILAR (Seguridad Física y del Entorno)

Riesgo:

- El ingreso de personal no autorizado puede causar que se realicen actividades ilícitas.
- Se puede tener daño de los equipos por falta del suministro eléctrico.

Causa:

- No se tiene un sistema de seguridad en la puerta de ingreso al Datacenter.
- No existe una persona que se encargue de verificar quien entra al Datacenter.

Salvaguardas:

Control de los accesos físicos

- [L54] Los accesos permanecen cerrados fueras de las horas de trabajo

Aseguramiento de salas, instalaciones y oficinas

- [LC] La Seguridad de las instalaciones no es responsabilidad de un único guardia

Protección frente a amenazas externas

Protección frente a incendios

- [L92c]Se dispone de un sistema automático de detección de incendios

Protección frente a inundaciones

- [L933] Se dispone de un sistema de evacuación de agua (canalizaciones, motobomba, etc.)

Protección frente a explosivos

- [L971] El personal recibe información específica (obtención de información, respuesta a la amenaza, etc.)

Suministros

- [AUX51] Se dimensiona el sistema considerado necesidades futuras
- [COM71] Se identifican y evitan "puntos únicos de fallo" (SPF – Single Point on Failure)

Protección del Cableado

- [AUX69] Se controlan todos los accesos al cableado

- [AUX6a]Hay protección prevista contra daños o intercepciones no autorizadas (conductos blindados, cajas o salas cerradas, etc.)
- [AUX6e] El cableado es tolerante a fallos (redundancia de líneas críticas, etc.)

Mantenimiento de Equipos

- [HWb6] Se priorizan las actuaciones encaminadas a corregir riesgos elevados

Seguridad de los equipos fuera de las instalaciones

- [HWa45] El activo se protege técnicamente antes de su salida
- [HWa46] Se proporciona una seguridad equivalente a la de los equipos instalados dentro para el mismo propósito

Recomendaciones:

- Supervisar cuales son las personas que tienen permiso de acceder al Datacenter.
- Los proveedores de servicios siempre deben ingresar acompañados de la persona encargada del Datacenter para supervisar el trabajo realizado.
- Verificar que los dispositivos de alimentación extra se encuentren funcionando de manera correcta.

Gráfico:

Figura 4.2.5.5 Gráfico de Salvaguardas aplicadas en PILAR (Seguridad Física y del Entorno)

4.2.5.6 Dominio: Gestión de Comunicaciones y operaciones

Controles:

- Responsabilidades y procedimientos de operación.
- Gestión de servicios prestados por terceros.
- Planificación y aceptación por terceros.
- Protección frente a código y código descargable.
- Copias de seguridad.
- Gestión de seguridad de las redes.

- Tratamiento de soportes de información.
- Intercambios de información
- Servicios de comercio electrónico
- Supervisión

Objetivos:

- Asegurar la operación correcta y segura de los recursos de tratamiento de información.
- Implementar y mantener un nivel apropiado de seguridad de la información y de la prestación del servicio en línea con los acuerdos de prestación del servicio por terceros.
- Minimizar el riesgo de fallos en los sistemas.
- Proteger la integridad del software y de la información.
- Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación
- Asegurar la protección de la información en las redes y la protección de su infraestructura de apoyo.

Principios:

- Se deberían establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos para el tratamiento de la información.
- La organización debería verificar la implementación de acuerdos, el monitoreo de su cumplimiento y gestión de los cambios con el fin de

asegurar que los servicios que se prestan cumplen con todos los requerimientos acordados con terceros.

- Se requiere una planificación y preparación avanzadas para garantizar la adecuada capacidad y recursos con objeto de mantener la disponibilidad de los sistemas requerida.
- Se requieren ciertas precauciones para prevenir y detectar la introducción de código malicioso y códigos móviles no autorizados
- Se deberían establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo para realizar copias de seguridad y probar su puntual recuperación.
- La gestión de la seguridad de las redes, las cuales pueden cruzar las fronteras de la organización, exige la atención a los flujos de datos, implicaciones legales, monitoreo y la protección.

Condición:

- No se ha encontrado acuerdos para intercambio de hardware y software.
- No se ha implantado medidas de seguridad de los medios que se encuentran en tránsito.
- Los incidentes de seguridad no han sido establecidos para asegurar una respuesta rápida y confiable.

Evidencia:

Cuestionario de Auditoria Informática y aplicación de la herramienta PILAR para el Datacenter de la Brigada De Fuerzas Especiales No. 9 “Patria”

Gráfico:

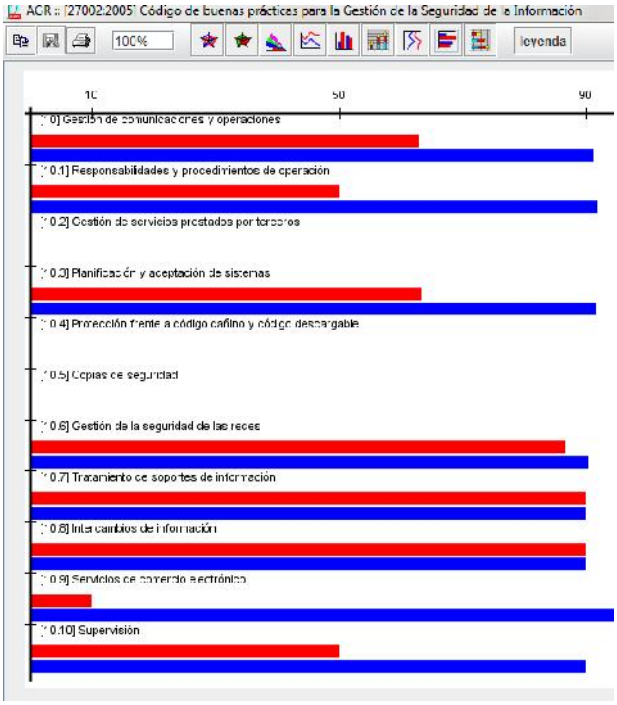

Figura 4.2.5.6 Gráfico de Hallazgos encontrados en PILAR (Gestión de Comunicaciones y operaciones)

Riesgo:

- Cambios no autorizados dentro de los sistemas o en la información.
- Uso mal intencionado de los sistemas.
- Perdida de información.
- Fallos en los sistemas.
- Ejecución de código malicioso e inseguro.
- Uso inadecuado de la información, con fines malintencionados.

Causas:

- Daño del sistema a mediano o largo plazo.
- Daño de los sistemas de información.
- Carga excesiva de procesos.

Salvaguardas:

Gestión de Cambios

- [Swa5] Se priorizan las actuaciones encaminadas a corregir riesgos elevados
- [HWb5] Evaluación del impacto potencial del cambio

Planificación y aceptación de los sistemas

- [G43] Planificación de capacidades

Aceptación de nuevos sistemas

- [S56] Se lleva a cabo una campaña de ejecución de pruebas de regresión (para asegurarse de que no afecte a los demás servicios)

Gestión de las seguridades de las Redes

- [COMa] Protección criptográfica del secreto de los datos intercambiados
- [IP62] Se controla el trafico entrante y saliente

Seguridad de los servicios de Red

- [COM6] Se aplican perfiles de seguridad
- [COMf] Seguridad Wirelless

Recomendaciones:

- Documentar los procesos realizados.
- Implementar procesos para preservar la integridad y la confidencialidad de la información.

Gráfico:

Figura 4.2.5.6 Gráfico de Salvaguardas aplicadas en PILAR (Gestión de Comunicaciones y operaciones)

4.2.5.7 Dominio: Control de Acceso

Controles:

- Requisitos de Control de Acceso.
- Gestión de Usuarios.
- Responsabilidades de los Usuarios.
- Control de Acceso a la Red.
- Control de acceso a sistemas de operación.
- Control de acceso a datos y a operaciones.
- Equipos móviles y tele-trabajo.

Objetivos:

- Controlar los accesos a la información.
- Garantizar el acceso a los usuarios autorizados e impedir los accesos no autorizados a los sistemas de información.
- Impedir el acceso de usuarios no autorizados y el compromiso o robo de información y recursos para el tratamiento de la información.
- Impedir el acceso no autorizado a los servicios en red.
- Impedir el acceso no autorizado al sistema operativo de los sistemas.
- Impedir el acceso no autorizado a la información mantenida por los sistemas de las aplicaciones.
- Garantizar la seguridad de la información en el uso de recursos de informática móvil y teletrabajo.

Principios:

- Se deberían controlar los accesos a la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades de seguridad y de negocio de la Organización.
- Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información.
- La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.
- Se deberían controlar los accesos a servicios internos y externos conectados en red.
- Se deberían utilizar las prestaciones de seguridad del sistema operativo para permitir el acceso exclusivo a los usuarios autorizados.
- Se deberían utilizar dispositivos de seguridad con objeto de restringir el acceso a las aplicaciones y sus contenidos.
- La protección exigible debería estar en relación a los riesgos específicos que ocasionan estas formas específicas de trabajo. En el uso de la informática móvil deberían considerarse los riesgos de trabajar en entornos desprotegidos y aplicar la protección conveniente.

Condición:

- No se protege de la mejor manera a los equipos del área del Datacenter.

Evidencia:

Cuestionario de Auditoria Informática y aplicación de la herramienta PILAR para el Datacenter de la Brigada De Fuerzas Especiales No. 9 “Patria”

Gráfico:

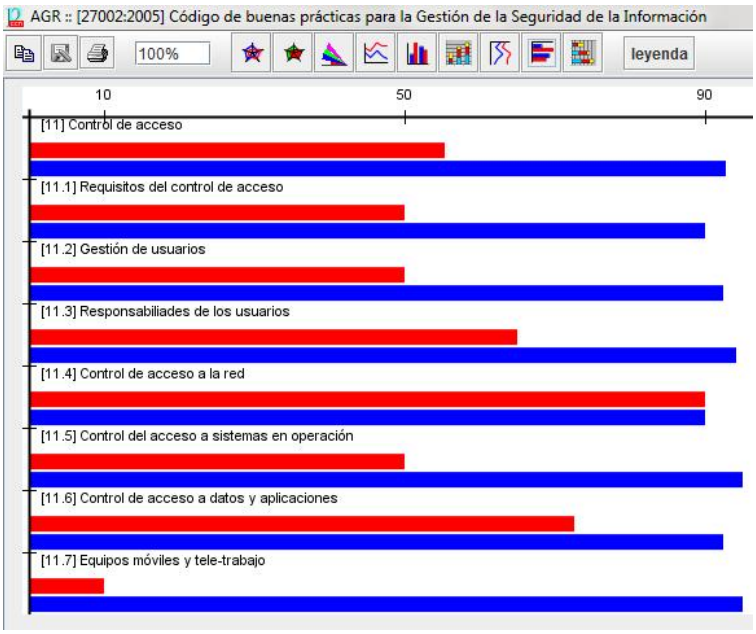

Figura 4.2.5.7 Gráfico de Hallazgos encontrados en PILAR (Control de Acceso)

Riesgo:

- Perdida de los equipos e incluso de la información.
- Acceso no autorizado de personas externas a la institución.

Causas:

- Perdida de información del personal que se encuentra en la Brigada.
- Espionaje por parte de personal externo.

Salvaguardas:

Gestión de Privilegios

- [H28a] Los privilegios se anulan cuando termina la autorización
- [H28b] Los privilegios se revisan cuando el usuario cambia de responsabilidades y de función
- [H28c] Los privilegios se anulan cuando el usuario abandona la organización

Registro de Usuarios

- [H131] Cada usuario recibe un identificador exclusivo (no compartido)
- [H15] Gestión de la identificación y autenticación de usuarios

Uso de Contraseñas

- [H1713] Los usuarios se responsabilizan de la confidencialidad de la contraseñas
- [H171a] Las contraseñas se modifican al ser comprometidas o existir sospecha de ello
- [H1712] Se selecciona contraseñas fáciles de recordar pero de difícil conjetura

Identificación y autenticación de Usuarios

- [H15] Gestión de la identificación y autenticación de usuarios

Aislamiento de Sistemas Críticos

- [L49t] Se evita que el acceso físico para la operación y mantenimiento abra el acceso a otros activos

Recomendaciones:

- Supervisar las actividades del personal, que realicen lo que su perfil de usuario le permite acceder.
- Monitorear los accesos a la red frecuentemente.

Gráfico:

Figura 4.2.5.7 Gráfico de Salvaguardas aplicadas en PILAR (Control de Acceso)

4.2.5.8 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.

Objetivos:

- Garantizar que la seguridad es parte integral de los sistemas de información.
- Evitar errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones.
- Proteger la confidencialidad, autenticidad o integridad de la información con la ayuda de técnicas criptográficas.
- Garantizar la seguridad de los sistemas de ficheros.
- Mantener la seguridad del software del sistema de aplicaciones y la información.
- Reducir los riesgos originados por la explotación de vulnerabilidades técnicas publicadas.

Principios:

- Dentro de los sistemas de información se incluyen los sistemas operativos, infraestructuras, aplicaciones de negocio, aplicaciones estándar o de uso generalizado, servicios y aplicaciones desarrolladas por los usuarios.
- Se deberían diseñar controles apropiados en las propias aplicaciones, incluidas las desarrolladas por los propios usuarios, para asegurar el procesamiento correcto de la información. Estos controles deberían incluir la validación de los datos de entrada, el tratamiento interno y los datos de salida.
- Se debería desarrollar una política de uso de controles criptográficos.
- Se debería controlar el acceso a los sistemas de ficheros y código fuente de los programas.
- Se deberían controlar estrictamente los entornos de desarrollo de proyectos y de soporte.
- Se debería implantar una gestión de la vulnerabilidad técnica siguiendo un método efectivo, sistemático y cíclico, con la toma de medidas que confirmen su efectividad.

Condición:

- No existe ningún tipo de control criptográfico.
- No se aplica seguridad a los archivos.

Evidencia:

Cuestionario de Auditoria Informática y aplicación de la herramienta PILAR para el Datacenter de la Brigada De Fuerzas Especiales No. 9 “Patria”

Gráfico:

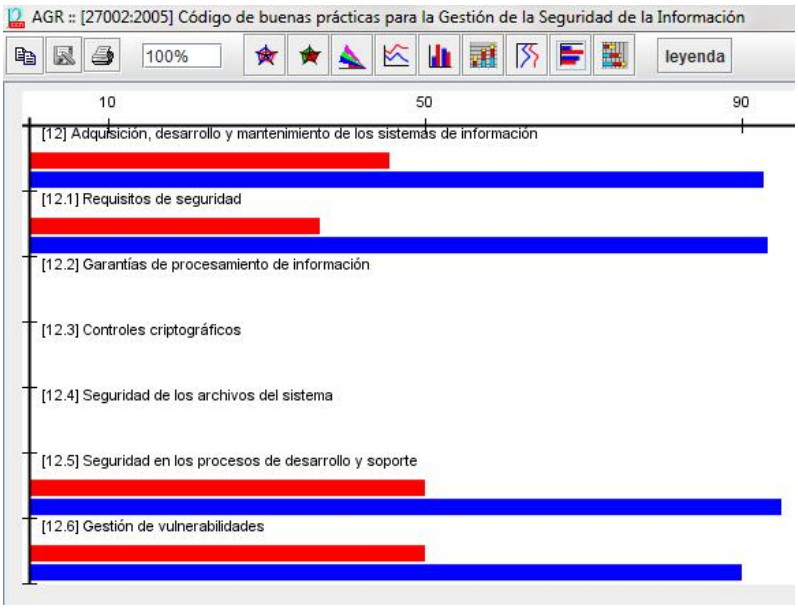

Figura 4.2.5.8 Gráfico de Hallazgos encontrados en PILAR (Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información)

Riesgos:

- Modificación y pérdida de información.
- No se identifican los procesos vulnerables de la información.

Causa:

- Los controles criptográficos no aplican por lo que la información puede perderse.

- Acceso a la red de información sin los perfiles necesarios.

Salvaguardas:

Gestión de Claves

- [K1] Gestión de claves de cifra de información
- [K2] Gestión de claves de cifra de firma de información
- [K3] Gestión de claves para contenedores criptográficos
- [K4] Gestión de claves de comunicación

Control de Vulnerabilidades Técnicas

- [H552] Se actualiza regularmente el conjunto de vulnerabilidades utilizado por el proveedor
- [H553] Se revisa el sistema operativo

Recomendaciones:

- Se necesita tener perfiles de usuarios para que la seguridad este definida y el personal pueda acceder con perfiles restringidos.
- Se necesita implementar un Plan de Contingencia de Seguridad.

Gráfico:

Figura 4.2.5.8 Gráfico de Salvaguardas aplicadas en PILAR (Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información)

4.2.5.9 Dominio: Gestión de incidentes de seguridad de Información

Controles:

- Comunicación de incidentes y debilidades.
- Gestión de incidentes y mejoras.

Objetivo:

- Garantizar que los eventos y debilidades en la seguridad asociados con los sistemas de información se comuniquen de modo que se puedan realizar acciones correctivas oportunas.

- Garantizar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes en la seguridad de información.

Principios:

- Debería establecerse el informe formal de los eventos y de los procedimientos de escalado.
- Deberían establecerse las responsabilidades y procedimientos para manejar los eventos y debilidades en la seguridad de información de una manera efectiva y una vez que hayan sido comunicados.

Condición:

- Se cumplen los controles de dominios de gestión de incidentes en un 50%.

Evidencia:

Cuestionario de Auditoria Informática y aplicación de la herramienta PILAR para el Datacenter de la Brigada De Fuerzas Especiales No. 9 “Patria”

Gráfico:

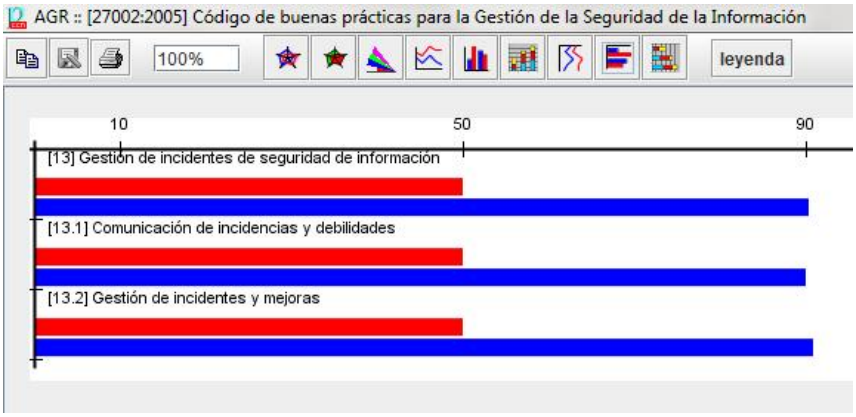

Figura 4.2.5.9 Gráfico de Hallazgos encontrados en PILAR (Gestión de incidentes de seguridad de Información)

Riesgo:

- Los riesgos se pueden materializar, ya que tiene un 50% de probabilidad que ocurran.

Causa:

- Pueden ocurrir incidentes y no se los va a poder solucionar de manera eficiente.

Salvaguardas:

Gestión de Incidencias

- [H481] Se suspenden cautelarmente los trabajos en los sistemas afectados
- [H485] Hay comunicación con los afectados por la incidencia

Recomendaciones:

- Documentar los incidentes ocurridos, para poder solucionarlos en menor tiempo o realizar el seguimiento de los mismos.

Gráfico:

Figura 4.2.5.9 Gráfico de Salvaguardas aplicadas en PILAR (Gestión de incidentes de seguridad de Información)

4.2.5.10 Dominio: Gestión de la continuidad del negocio

Controles:

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

Objetivo:

- Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a desastres o grandes fallos de los sistemas de información.

Principios:

- Se debería implantar un proceso de gestión de continuidad del negocio

  para reducir, a niveles aceptables, la interrupción causada por los desastres y fallos de seguridad (que, por ejemplo, puedan resultar de desastres naturales, accidentes, fallas de equipos o acciones deliberadas) mediante una combinación de controles preventivos y de recuperación.

Condición:

- No existen planes para la continuidad del negocio.

Evidencia:

Cuestionario de Auditoria Informática y aplicación de la herramienta PILAR para el Datacenter de la Brigada de Fuerzas Especiales No. 9 “Patria”.

Gráfico:

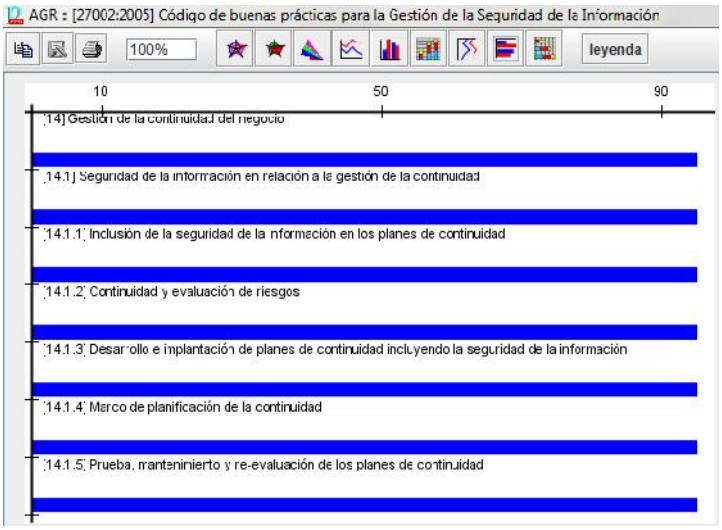

Figura 4.2.5.10 Gráfico de Hallazgos encontrados en PILAR (Gestión de la continuidad del negocio)

Riesgo:

- No se pueden aplicar el plan de continuidad porque van a fallar en un 100%, ya que no ha sido implementado.

Causa:

- No existe un plan de continuidad.

Salvaguardas:

Inclusión de la seguridad de la información en los planes de continuidad

- [BC255] Todas las áreas de la organización están coordinadas

Plan de Continuidad

- [BC259] Los planes se prueban regularmente

Recomendación:

- Realizar un plan de contingencia, probarlo y actualizarlo

Gráfico:

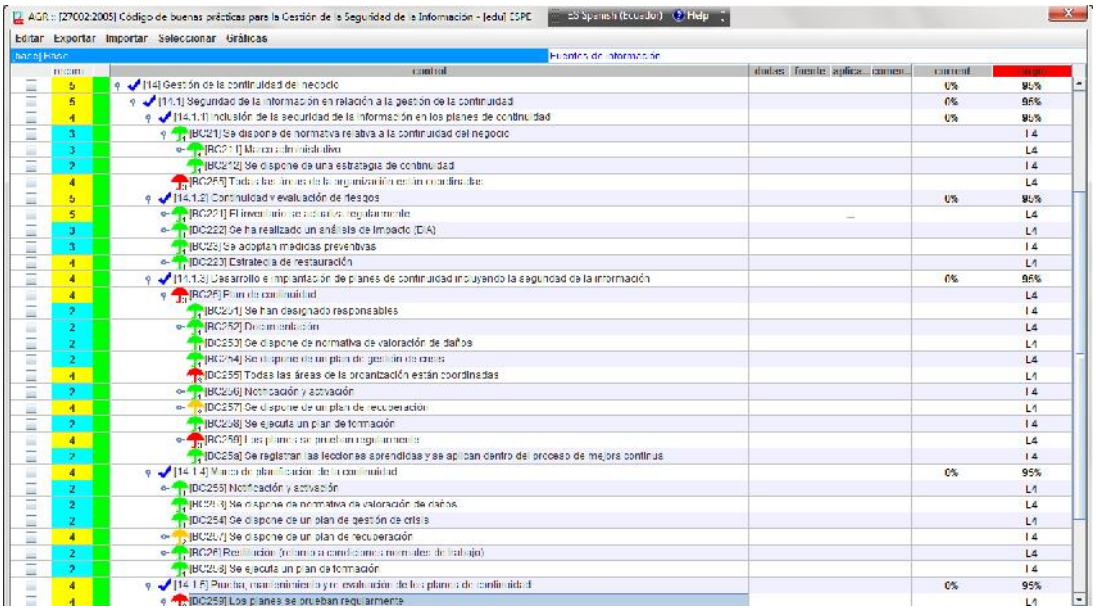

Figura 4.2.5.10 Gráfico de Salvaguardas aplicadas en PILAR (Gestión de la continuidad del negocio)

4.2.5.11 Dominio: Cumplimiento

Controles:

- Satisfacción de requisitos legales.
- Cumplimiento de políticas, normas y reglamentos técnicos.

- Consideraciones sobre auditoria de los sistemas de información.

Objetivos:

- Evitar incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad.
- Garantizar la conformidad de los sistemas con las políticas y estándares de seguridad de la Organización.
- Maximizar la efectividad del proceso de auditoría de los sistemas de información y minimizar las intromisiones a/desde éste proceso.

Principios:

- El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos reguladores y de seguridad contractuales.
- Se deberían realizar revisiones regulares de la seguridad de los sistemas de información.
- Deberían existir controles para proteger los sistemas en activo y las herramientas de auditoría durante el desarrollo de las auditorías de los sistemas de información.

Condición:

- Se han revisado las políticas de seguridad, las normas y reglamento técnico y la satisfacción de requisitos legales

Evidencia:

Cuestionario de Auditoria Informática y aplicación de la herramienta PILAR para el Datacenter de la Brigada De Fuerzas Especiales No. 9 “Patria”.

Gráfico:

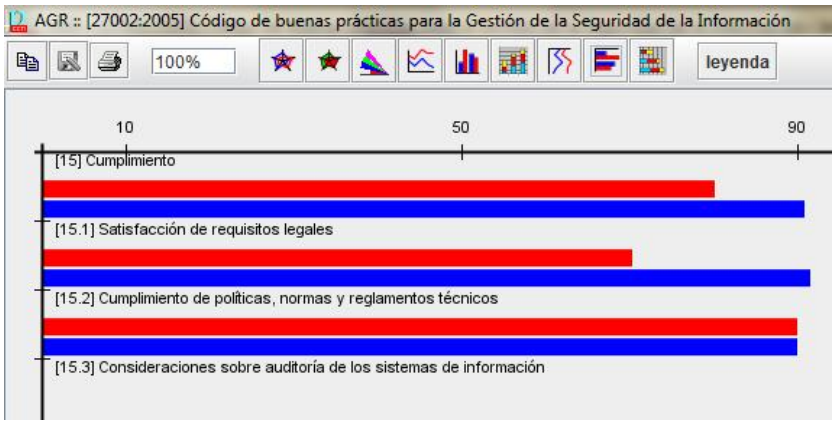

Figura 4.2.5.11 Gráfico de Hallazgos encontrados en PILAR (Cumplimiento)

Riesgo:

- No tener una visión de las cosas que están afectando a la seguridad de la información.

Causa:

- No tener manuales de reglas actualizados.

Salvaguardas:

- No aplican ya que se tiene más del 50% de cumplimiento.

Recomendaciones:

- Revisar el regulamiento de las reglas de seguridad y procedimientos apropiados y actualizados.

Gráfico:

Figura 4.2.5.11 Gráfico de Salvaguardas aplicadas en PILAR (Cumplimiento)

CAPÍTULO 5

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- La presente tesis sirve como aplicación de la metodología MAGERIT y su herramienta PILAR, realizar el análisis de riesgos de cualquier institución pública o privada que tenga activos como por ejemplo la información.

- La seguridad informática permite proteger la infraestructura computacional incluyendo la información que ésta contiene, por lo que debe ser tratado con mucha más responsabilidad dentro del Datacenter.

- Se debe tener en cuenta que la detección y mitigación de riesgos debe ser parte importante de la institución, ya que ayudará a mantener la integridad y la confidencialidad de la información mediante técnicas y métodos.

- Las normas 27000 ayudo a conocer de manera general como se encuentra actualmente la seguridad informática del Datacenter de la Brigada “Patria”, tomando como ayuda la metodología MAGERIT

5.2 RECOMENDACIONES

- Se recomienda utilizar la metodología MAGERIT para el analizar los riesgos dentro de las instituciones privadas o públicas que tengan activos tangibles e intangibles integrando el software PILAR que es una aplicación que utiliza la metodología que trabaja con activos, amenazas y salvaguardas.

- Se debe contratar un servicio externo para analizar más a fondo la seguridad informática, o adquirir una herramienta que permita realizar un análisis completo de los riesgos y sea capaz de prevenir riesgos.

- Registrar y documentar los procesos, las actividades y las tareas del personal encargado del centro de datos para tener un registro y el mismo ayude en un nuevo análisis de riesgos.

- Tener en mente que las salvaguardas deben ser transparentes a los usuarios y deben ayudar a disminuir el riesgo.

- Implementar un manual de procedimientos en caso de que los riesgos se materialicen para poder tratarlos sin que se vea afectados activos que dependen del activo afectado.

6. BIBLIOGRAFÍA

27001, E. P. (2009). *NORMAS ISO 27000.* Recuperado el 15 de 02 de 2012, de Http://www.iso27000.es

Baquero, A. (2005). *Libro de Informática: Glosarios y Términos.* México.: McGrow Hill.

Francisco José Serón Arbolea, N. P. (2007). *"Conceptos Generales de Informática".* Recuperado el 12 de 03 de 2012, de http://osluz.unizar.es/files/presentacion_pdi.pdf

Públicas, M. d. (25 de 01 de 2012). *Herramientas de Análisis y Gestión de Riesgos.* Recuperado el 30 de 04 de 2012, de EAR PILAR: http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=magerit

Públicas, M. d. (2012). *Herramientas de Análisis y Gestión de Riesgos.* Recuperado el 15 de 05 de 2012, de http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=magerit

Públicas, M. d. (20 de 06 de 2006). *MAGERIT v.2 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Recuperado el 30 de 11 de 2011, de http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=magerit

Públicas, M. d. (20 de 06 de 2006). *MAGERIT Versión 2.* Recuperado el 25 de 11 de 2011, de Book 1 - Method: www.ccn-cert.cni.es/publico/herramientas/pilar5/ec/magerit/meth-en-v11.pdf

Públicas, M. d. (20 de 06 de 2006). *MAGERIT Versión 2.* Recuperado el 15 de 02 de 2012, de Book III - Techniques: www.ccn-cert.cni.es/publico/herramientas/pilar5/en/magerit/tech-en-v11.pdf

Públicas, M. d. (20 de 06 de 2006). *MAGERIT Versión 2.* Recuperado el 06 de 01 de 2012, de Book II - Catalogue of Elements: www.ccn-cert.cni.es/publico/herramientas/pilar5/en/magerit/cat-en-v11.pdf

BIOGRAFÍA

Nombres y Apellidos:	Sofía Monserrath Viteri Díaz
Lugar de Nacimiento:	Quito
Fecha de Nacimiento:	22 de Marzo de 1986
Educación Inicial:	Escuela José Amadeo Jácome 1991-1992 Quito
Educación Primaria:	Escuela “Cardenal de la Torre” 1993 - 2000 Quito
Educación Secundaria:	Unidad Educativa Nuestra Señora del Rosario 2001 – 2004 Bachiller en Ciencias, especialización Físico Matemático Quito
Educación Superior:	Escuela Politécnica del Ejército ESPE 2005 - 2010 Ingeniería en Sistemas e Informática
Educación Idiomas:	Escuela Politécnica del Ejército ESPE 2008 - 2010 Certificación Suficiencia en Inglés

HOJA DE LEGALIZACION DE FIRMAS

ELABORADA(O) POR

_____

Srta. Monserrath Viteri

DIRECTOR DE LA CARRERA

_____

Ing. Mauricio Campaña Msc.

Lugar y fecha: Marzo 2013