TESIS

UNIVERSIDAD CIENTÍFICA DEL SUR

UNIVERSIDAD CIENTÍFICA DEL SUR

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN Y GESTIÓN

"MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GESTIÓN DE RIESGOS DE LA FUNDACIÓN PARA EL DESARROLLO SOLIDARIO EN EL 2020"

Tesis para optar el título profesional de:

Ingeniero de Sistemas de Información

Presentado por:

Elmer Ivan Santisteban Avalos (0000-0003-2249-8391)

Asesor:

Manuel Antonio Pereyra Acosta (0000-0002-2593-5772)

Lima – Perú

2021

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS

UNIVERSIDAD CIENTÍFICA DEL SUR

UNIVERSIDAD CIENTÍFICA DEL SUR

ACTA DE SUSTENTACIÓN DE TESIS

Lima, 01 de abril, 2021

Los integrantes del Jurado de tesis:

Presidente	**Mg. Luis Alberto Torres Cabanillas**
Miembro 1	**Mg. Jose Rodriguez Parra Feria**
Miembro 2	**Mg. Carlos Federico Díaz Sánchez**

Se reúnen para evaluar la tesis titulada:
"MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GESTIÓN DE RIESGOS DE LA FUNDACIÓN PARA EL DESARROLLO SOLIDARIO EN EL 2020"

Presentado por el(la) bachiller.
Elmer Ivan Santisteban Avalos

Para optar el Título Profesional de
Ingeniero de Sistemas de Información y Gestión
Asesorado(a) por:
Manuel Antonio Pereyra Acosta

Luego de haber evaluado el informe final de tesis y evaluado el desempeño de(l) (los) estudiantes de la carrera de **Ingeniería de Sistemas de Información y Gestión** en la sustentación, concluyen de manera unánime (X) por mayoría simple ( ) calificar a:

Tesista:	Elmer Ivan Santisteban Avalos		
Nota (en letras):	**14**		
Aprobado (X)	Aprobado - Muy buena ( )	Aprobado - Sobresaliente ( )	Desaprobado ( )

Los miembros del jurado firman en señal de conformidad.



Mg. Luis Alberto Torres Cabanillas
Presidente(a) del Jurado



Manuel Antonio Pereyra Acosta
Asesor(a)



Mg. Jose Rodriguez Parra Feria
Miembro 1



Mg. Carlos Federico Díaz Sánchez
Miembro 2

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

DEDICATORIA

Este trabajo de investigación se lo dedico a mi madre, mis hermanos que me apoyaron y animaron a continuar pese a las dificultades que vive el país.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

AGRADECIMIENTOS

Agradecer a la Universidad Científica del Sur por brindarme la enseñanza necesaria para la realización de este proyecto de investigación. Asimismo, a mi asesor el Ing. Manuel Antonio Pereyra Acosta, que me brindó sus conocimientos y el apoyo necesario hasta el término de este proyecto. A la institución Fundación para el Desarrollo Solidario quien me dio la oportunidad de realizar este proyecto en sus instalaciones y a mis compañeros de trabajo. Finalmente, a los ingenieros que aportaron en la validación de los instrumentos que se usaron.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

ÍNDICE GENERAL

Dedicatoria

Agradecimientos

Índice de figuras

Índice de tablas

Índice de anexos

Resumen

Abstract

Introducción 1

CAPITULO I PLANTEAMIENTO DEL PROBLEMA 2

1.1. Descripción de la realidad problemática 2

1.2. Formulación del problema 4

1.2.1. Problema general 4

1.2.2. Problemas específicos 4

1.3. Justificación de la investigación 5

1.3.1. Justificación teórica 5

1.3.2. Justificación metodológica 5

1.3.3. Justificación práctica 5

1.3.4. Justificación económica 6

1.4. Limitaciones de la investigación 6

1.5. Viabilidad de la investigación 6

CAPITULO II MARCO TEORICO 7

2.1. Antecedentes de la investigación 7

2.1.1. Antecedentes nacionales 7

2.1.2. Antecedentes internacionales 10

2.2. Bases teóricas 13

2.2.1. Seguridad de la información 13

a. Dimensiones de seguridad 14

2.2.2. Gestión de riesgo 15

a. Valor de un activo 16

2.2.3. Análisis de riesgo 16

2.2.4. Tratamiento de riesgo 18

a. Las salvaguardas 19

2.2.5. Declaración de aplicabilidad 20

2.2.6. Metodología Magerit 21

a. Determinación del contexto 23

Tesis publicada con autorización del autor
No olvide citar esta tesis

b. Identificación de los riesgos 23
c. La evaluación de los riesgos 23
d. El tratamiento de riesgo 24
e. Comunicación y consulta 24
f. Seguimiento y control 25
2.2.7. Amenazas 25
a. Identificación de las amenazas 26
2.2.8. La probabilidad de la amenaza 26
2.2.9. Vulnerabilidades 27
2.2.10. Degradación 27
2.2.11. Control 28
2.2.12. Impacto residual 28
2.2.13. Metodología 28
2.2.14. Seguridad 28
2.2.15. Riesgo 28
2.2.16. Riesgo residual 29
2.3. Objetivos de la investigación 29
2.3.1. Objetivo general 29
2.3.2. Objetivos específicos 29
2.4. Formulación de hipótesis 29
2.4.1. Hipótesis general 29
2.4.2. Hipótesis especificas 29
CAPITULO III: DISEÑO METODOLÓGICO 30
3.1. Diseño de la investigación 30
3.2. Tipo.. 30
3.3. Enfoque 30
3.4. Población 31
3.5. Muestra 31
3.6. Operacionalización de variables 31
3.6.1. Variable dependiente: Gestión de riesgo 31
a. Análisis de riesgo 32
b. Tratamiento de riesgo 32
3.6.2. Variable independiente: Seguridad de la información 33
a. Confidencialidad 33
b. Integridad 34
c. Disponibilidad 34

Tesis publicada con autorización del autor
No olvide citar esta tesis

3.7. Técnicas para la recolección de datos 34
3.7.1. Descripción de los instrumentos 35
a. Ficha de observación (Valor de riesgo) 35
b. Ficha de observación (Controles) 36
3.7.2. Validez y confiabilidad de los instrumentos 37
a. Validación 37
b. Confiabilidad 37
3.8. Técnica para el procesamiento y análisis de datos 37
3.9. Aspectos éticos 38
CAPITULO IV: RESULTADOS 38
4.1. Estadística descriptiva 40
4.1.1. Gestión de riesgo 40
4.1.2. Evaluación de riesgo 41
4.1.3. Tratamiento de riesgo 43
4.2. Contraste de hipótesis 44
4.2.1. Prueba de hipótesis general 44
4.2.2. Prueba de Hipótesis específica 45
CAPITULO V: DISCUSION, CONCLUSIONES Y RECOMENDACIONES 48
5.1. Discusión 48
5.2. Conclusiones 50
5.3. Recomendaciones 51
REFERENCIAS BIBLIOGRÁFICAS 53
ABREVIATURAS 58
ANEXOS 59
ANEXO 1: MATRIZ DE CONSISTENCIA 59
ANEXO 2: MATRIZ DE OPERACIONALIZACIÓN 60
ANEXO 3: ENCUESTA/INSTRUMENTO DE EVALUACIÓN 61
ANEXO 4: VALIDEZ DE INSTRUMENTOS POR JUECES EXPERTOS 65
ANEXO 5: CONSTANCIA EMITIDA POR LA INSTITUCIÓN DONDE SE REALIZÓ LA INVESTIGACIÓN 71
ANEXO 6. PROCESO DE GESTIÓN DE RIESGO 72
ANEXO 7: IMPLEMENTACIÓN DE POLÍTICAS DE CONTROL EMPLEANDO ISO 27001 116
ANEXO 8: FICHAS DE OBSERVACIÓN 133

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

ÍNDICE DE FIGURAS

Figura 1. Ciclo PDCA 15
Figura 2. Proceso de riesgo de un activo..... 17
Figura 3. Criterios para el tratamiento de riesgo. 18
Figura 4. Tipos de protección según Magerit. 20
Figura 5. Activos relevantes según Magerit 22
Figura 6. Proceso de tratamiento de riesgo. 24
Figura 7. Proceso de Gestión de Riesgo. 25
Figura 8. Identificación de las amenazas por Magerit. 26
Figura 9. Gráfico de barras de la gestión de riesgo. 41
Figura 10. Gráfico de barras de la evaluación de riesgo 42
Figura 11. Gráfico de barras del tratamiento de riesgo. 43

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

ÍNDICE DE TABLAS

Tabla 1 Probabilidad de la amenaza 27
Tabla 2 Nivel de vulnerabilidad 27
Tabla 3 Degradación del valor 27
Tabla 4 Variable dependiente 34
Tabla 5 Nivel de Riesgo Pre test y Post test 39
Tabla 6 Muestra descriptiva de la tabla cruzada de la Gestión de riesgo. 40
Tabla 7 Muestra descriptiva de la tabla cruzada de la Evaluación de riesgo. 41
Tabla 8 Muestra descriptiva de la tabla cruzada del Tratamiento de riesgo. 43
Tabla 9 Prueba de Wilcoxon para la Gestión de riesgo 44
Tabla 11 Prueba de Wilcoxon para la Evaluación de riesgo 45
Tabla 12 Prueba del p-valor en el pre test y post test 45
Tabla 13 Prueba de Wilcoxon para el Tratamiento de riesgo 46
Tabla 14 Prueba del p-valor en el pre test y post test 46

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

ÍNDICE DE ANEXOS

ANEXO 1: MATRIZ DE CONSISTENCIA 59
ANEXO 2: MATRIZ DE OPERACIONALIZACIÓN 60
ANEXO 3: ENCUESTA/INSTRUMENTO DE EVALUACIÓN 61
ANEXO 4: VALIDEZ DE INSTRUMENTOS POR JUECES EXPERTOS 65
ANEXO 5: CONSTANCIA EMITIDA POR LA INSTITUCIÓN DONDE SE REALIZÓ LA INVESTIGACIÓN 71
ANEXO 6. PROCESO DE GESTIÓN DE RIESGO 72
ANEXO 7: IMPLEMENTACIÓN DE POLÍTICAS DE CONTROL EMPLEANDO ISO 27001 116
ANEXO 8: FICHAS DE OBSERVACIÓN 133

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

RESUMEN

Con el pasar del tiempo vemos un aumento de ataques informáticos, el fácil acceso a la tecnología y el poco conocimiento de algunas personas en seguridad son fuente para causar perjuicio. Por esto, el propósito de la investigación fue implementar una alternativa de solución para el problema de seguridad de la información que existe en la institución Fundación para el Desarrollo Solidario. El objetivo de este estudio es demostrar como la mejora de la seguridad de la información influye en el proceso de gestión de riesgo en la institución. Se propuso la Metodología Magerit con enfoque cualitativo y una población de activos de información para que demuestre como la seguridad mejora con el conocimiento de los riesgos que hay, para esto se dividió en dos fases: pre test y post test. Los resultados que se obtuvieron cuando se propuso las salvaguardas en los activos con riesgo, mostraron que esto tuvo una mejora en seguridad y el riesgo se minimizó; De la misma forma estos resultados se validaron estadísticamente en el SPSS y los instrumentos validados por jueces expertos. De acuerdo con el análisis realizado, se concluye que implementando controles y políticas estas ayudan a mejorar la seguridad de la institución y crear conciencia en cada usuario, manteniendo estable los riesgos y saber cómo actuar frente a cualquier amenaza o incidente, además ellos pueden tomar mejores decisiones en proyectos nuevos y/o actuales en las áreas con respecto a la tecnología.

Palabras clave: Ataques informáticos, seguridad de la información, riesgo, metodología, concientización.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

ABSTRACT

Over time we see an increase in computer attacks, easy access to technology and some people's little knowledge of security are a source of harm. For this, the purpose of the research was to implement an alternative solution for the information security problem that exists in the Fundación para el Desarrollo Solidario institution. The objective of this study is to demonstrate how improving information security influences the risk management process in the institution; The Magerit Methodology was proposed with a qualitative approach and information assets for demonstrate how safety improves with knowledge of the risks that exist, for this it's divided this into two phases: pre test and post test. The results that were obtained when I proposed the safeguards in assets with risk, showed that this had an improvement in security and the risk was minimized; The results that were obtained when I proposed the safeguards in assets with risk, showed that this had an improvement in security and the risk was minimized, in the same way, these results were statistically validated in the SPSS and the instruments validated by expert judges. According to the analysis carried out, It is concluded that implementing controls and policies these help to improve the security of the institution and create awareness in each user, risks remain stable and know how to act in the face of any threat or incident, also they will be able to make better decisions on new and / or current projects in areas with respect to technology.

Key words: Computer attacks, information security, risk, methodology, awareness.

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

INTRODUCCIÓN

En un mundo globalizado las organizaciones y las personas están conectadas de manera simultánea, esto gracias a la tecnología que avanza y se actualiza constantemente. Sin embargo, este avance no está a la par con la seguridad. Diferentes ataques cada día son más sofisticados y los usuarios los perjudicados, muchas veces es por una falta de cultura en seguridad de información. Por esta razón la investigación tiene como objetivo evaluar los riesgos que hay en los activos informáticos de la institución en cuanto a una adecuada seguridad en la información, para esto se propone una metodología que facilite tomar decisiones de seguridad y elegir de acuerdo a los resultados: quedarse con el diseño actual o adoptar este nuevo cambio.

El presente documento está dividido en cinco capítulos; En el primer capítulo encontraremos la descripción y formulación del problema, justificación, limitaciones y la viabilidad del proyecto.

El segundo capítulo se menciona los antecedentes y bases teóricas, donde se describe los conceptos relacionados al riesgo y la metodología Magerit como propuesta de implementación, además de los controles del Anexo A de la ISO 27001.

El tercer capítulo se menciona el diseño metodológico pre experimental como modelo que se usa en esta investigación. También se menciona el tipo, enfoque, población, muestra donde se determina a quien se va a estudiar, la forma como se realiza, las variables dependiente e independiente y sus categorías. Finalmente, se muestra la validación de instrumentos y confiabilidad que representa, así como las técnicas que se emplean para el procesamiento del análisis de datos.

En el cuarto capítulo se describe los resultados que se consiguen haciendo un comparativo del riesgo que hay en el pre test y post test, así como la estadística descriptiva de las dimensiones de esta investigación y el contraste de hipótesis través de la prueba de Wilcoxon.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Por último, en el quinto capítulo la discusión, conclusiones y recomendaciones como parte de los resultados obtenidos, relacionándolos con proyectos anteriores que ayudaron en esta investigación.

CAPITULO I PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

Actualmente las organizaciones a fin de alcanzar los objetivos del negocio dependen de las tecnologías para realizar sus procesos de manera más eficiente y rápida. El constante y vertiginoso avance tecnológico hace que los riesgos y ataques a la información estén en aumento y esto determina que las organizaciones presten mayor atención a una gestión de seguridad adecuada.

Cada día a nivel mundial se crean y difunden diferentes tipos de ataques informáticos que comprometen los servicios de la información, por mencionar algunos: La ingeniería social conocida como las técnicas que emplean los atacantes para persuadir a los usuarios, obteniendo así su información personal y/o de la organización; Así mismo, la explotación de vulnerabilidades, que se originan a raíz de no tener sistemas tecnológicos actualizados, además de una cultura de prevención impartida a los trabajadores.

La información siendo un activo importante en las organizaciones, requiere tener una adecuada gestión para minimizar los riesgos de ataques informáticos.

Acerca de la implementación de tecnologías en las organizaciones; se invierte en moderna infraestructura, pero no se implementan políticas de seguridad que las resguarden, capacitaciones al personal a cargo y a los usuarios finales, siendo ellos la primera línea de riesgo en seguridad.

Tesis publicada con autorización del autor
No olvide citar esta tesis

La función principal de la seguridad de la información trata con problemas complejos que solo se afronta con una adecuada y adaptable organización.

Por otra parte, existen organizaciones que no toman la importancia debida a la seguridad de la información, y solo cuando se ven afectados por algún ataque es cuando aparecen las acciones reactivas; esta falta de importancia, en muchos casos de manera grave; genera pérdida de información, tiempo, producción y costos. Por mencionar un ejemplo, en la actualidad, debido a la pandemia mundial hay diversos ataques informáticos como las noticias falsas, conocidas como "fake news", que unidos a ataques de ingeniería social desinforman a las personas y roban su información personal. Por tal motivo, es importante que las organizaciones tengan presente que toda información que esté en la red siempre estará en riesgo, por lo cual se debe establecer una gestión de riesgo juntamente con normas y políticas para obtener una adecuada seguridad y toma de decisiones proactivas ante alguna amenaza.

A nivel nacional según la Encuesta Global de Seguridad de la Información 2019-2020 realizada por la firma EY Perú en el menciona el 27% de las empresas incluyen un área de seguridad al inicio de operaciones y el 51% relaciona las actividades de seguridad con los procesos de negocio (p.8,10). Tal es el caso de las ONG que tienen ciertas limitaciones al adquirir equipamiento o recursos para controles de seguridad al no contar con un presupuesto estable ya que no generan ingresos y para ello tienen que elaborar proyectos propios o recibir donaciones de otras instituciones.

La ONG "Fundación para el Desarrollo Solidario", cuyo objetivo principal es apoyar a la mejora de calidad de vida de las personas vulnerables, realizando actividades y proyectos sociales en varias áreas, muestra que los procesos que hay en seguridad de la información son insuficientes y no se encuentran bien definidos; En caso haya

Tesis publicada con autorización del autor
No olvide citar esta tesis

incidentes esto crearía vulnerabilidad en los sistemas, en los activos y la información, la cual debe estar segura mediante un control adecuado, resguardado y protegida por el administrador; El mismo quien dará acceso a estos activos mediante políticas de seguridad y generando concientización entre los usuarios. Para hacerlo posible es necesario una evaluación de riesgo adecuada que ayude a verificar qué activos están en riesgos y no generar problemas legales, económicos ni operacionales; además de prevenir, minimizar las amenazas y vulnerabilidades actuales y futuras. Por lo tanto, esta investigación que se realizará en la "Fundación para el Desarrollo Solidario" busca encontrar la manera de mejorar la Gestión de información, con una metodología que se adapte a la institución, para determinar los riesgos que hay en los activos, realizar un tratamiento de riesgo para mitigarlos y finalmente hacer una mejora continua. Además de tener una base en caso de auditorías o certificaciones que se quiera obtener más adelante.

1.2. Formulación del problema

1.2.1. *Problema general*

¿De qué manera la mejora de la seguridad de la información influye en el proceso de gestión de riesgo de la Fundación para el Desarrollo Solidario?

1.2.2. *Problemas específicos*

¿De qué manera la seguridad de la información influye en la evaluación de riesgo de la Fundación para el Desarrollo Solidario?

¿De qué manera la seguridad de la información influye en el tratamiento de riesgo de la Fundación para el Desarrollo Solidario?

Tesis publicada con autorización del autor
No olvide citar esta tesis

1.3. Justificación de la investigación

1.3.1. *Justificación teórica*

La presente investigación se justifica teóricamente porque se usará como modelo para un análisis de riesgo la metodología Magerit que tiene como base la ISO/IEC 27005; La investigación pretende ampliar las teorías que hay de esta variable y su influencia en la seguridad de la información demostrando la eficacia del análisis de riesgo en las Organizaciones, lo cual permite, tener una detección oportuna de los riesgos y amenazas en los activos, siguiendo cada paso de los controles establecidos. Finalmente, se toma mejores decisiones para asegurar la continuidad del negocio.

1.3.2. *Justificación metodológica*

La investigación diseña una propuesta metodológica para medir y prevenir el riesgo de la información, tan válida como cualquier metodología convencional, con la ventaja de usar recursos disponibles de la institución y tener una cultura de información en el usuario. Así mismo se usará instrumentos validados y confiables que contribuirá con la toma de decisiones ante cualquier incidente.

1.3.3. *Justificación práctica*

Debido a las dificultades de las ONG's para implementar y corregir la seguridad de la información, se realiza la investigación para buscar alternativas que puedan minimizar las vulnerabilidades y amenazas en los activos. Igualmente servirá para concientizar al personal sobre ataques informáticos, con la finalidad de prevenir y evitar alguna consecuencia grave que pueda llevar a una pérdida de información y/o económica.

Tesis publicada con autorización del autor
No olvide citar esta tesis

1.3.4. *Justificación económica*

Al realizar el trabajo de investigación, se ha podido observar que es importante considerar el factor económico; ya que, a través del ingreso de dinero se podrá medir el nivel de eficiencia de la fundación.

Uno de los problemas encontrados ha sido el flujo de dinero en la Institución, la distribución de este ha provocado dificultades en cuanto a la adquisición de activos necesarios para el trabajo realizado, ya sean equipos de cómputo, licencias de software, servicios de mantenimiento, entre otros.

Por lo expuesto anteriormente, al realizar el proyecto, se realizará una lista detallada de los activos donde se destaque no solo las cantidades de activos, sino también el estado de estos y el uso dado en la actualidad, para poder disponer de manera ordenada y decidir mejor la forma en la que se invertirá el dinero, destinándolo de este modo a las áreas necesarias, así reducir costos en eventos futuros para la adquisición de materiales imprescindibles.

1.4. Limitaciones de la investigación

El área de sistemas solo cuenta con una persona a cargo; así que el instrumento que se usa son las fichas de observación. Las ONG's no cuentan con un presupuesto estable para adquirir infraestructura moderna, la metodología que se implementará será para ver el estado actual del riesgo en los activos mediante fichas de observación (pre y post); donde se medirá la confidencialidad, integridad y disponibilidad de activos, el impacto, el riesgo para así poder realizar un procedimiento que permita actuar frente a las amenazas.

1.5. Viabilidad de la investigación

Se tiene recursos como la información que se fue recolectando poco a poco en este tiempo, tal es el caso de activos y recursos humanos ya que la gerencia se mostró

Tesis publicada con autorización del autor
No olvide citar esta tesis

interesada al plantearles hacer una investigación de gestión de riesgos y su apoyo en las decisiones que se deberían tomar como resultado.

CAPITULO II MARCO TEORICO

2.1. Antecedentes de la investigación

2.1.1. *Antecedentes nacionales*

Llontop (2018) Gestión de riesgos de Tecnologías de Información de las empresas de Nephila Networks.

El objetivo principal de esta investigación es "Describir el nivel de eficiencia de la gestión de riesgo de tecnologías de información de las empresas comerciales y de servicios de Nephila Networks". El método usado es cuantitativo y diseño descriptivo comparativo, que consideró comparar 2 grupos de encuestados, siendo un total de 21 empresas y utilizó como población al soporte interno. Como resultado se muestra la diferencia que hay entre las empresas comerciales y las de servicio, teniendo las primeras un plan de riesgo más eficiente, mejor proceso de gobernanza, cultura entre los trabajadores y una implantación eficaz de TI. Como aporte se destaca las charlas sobre riesgos que se deben realizar a los trabajadores.

Villegas (2018) Diseño de un Sistema de Gestión de Seguridad de la Información Basado en la Norma ISO/IEC 27001:2013 para la Empresa Agroindustrial Pomalca S.A.A. – 2016.

El objetivo principal es aplicar el PDCA (ciclo de mejora continua) y metodología Magerit "apoyándose en el análisis y vulnerabilidades existentes en los activos involucrados en el mantenimiento y proceso de la información, por su facilidad de comprensión, costo económico y poca duración en la aplicación del diseño".

Tesis publicada con autorización del autor
No olvide citar esta tesis

La investigación es de tipo descriptiva – simple, se analizó el problema y se dio una solución. El investigador citó en sus conclusiones que la "Empresa Agroindustrial Pomalca S.A.A. no cumple con la mayoría de los Dominios, Objetivos de Control y Controles de Seguridad" que establece la norma ISO/IEC 27001:2013 objeto de este estudio. Así mismo; para los sistemas complejos que hay en la empresa, se estableció la "Declaración de Aplicabilidad" que propone procedimientos para controlar los principales riegos y el impacto que se pueda provocar en la empresa.

Podemos adicionar como recomendación del autor concientizar a los usuarios internos y externos de la organización en tema de riesgo que puede haber sobre los activos y como debe ser manejado en caso suceda.

Sandoval (2017) Diseño de un Plan de Seguridad de la Información para el Centro de Informática y Telecomunicaciones de la Universidad Nacional de Piura, Periodo 2015-2018.

En esta investigación nos menciona la importancia de que las empresas grandes o pequeñas tengan un nivel de concienciación permanente para la seguridad de los activos. Como su objetivo principal menciona "Diseñar un plan de seguridad de la información para proteger los activos informáticos que se utilizan y generan en los procesos de la Universidad administrados por el Centro de Informática y Telecomunicaciones". El método empleado es analítico-sintético porque descompone sus partes y después lo relaciona cada parte en una síntesis general de lo estudiado. La población usada es de 38 usuarios administrativos en el área de informática. Dentro de las conclusiones resaltantes se dice: "Como resultado de la aplicación de la metodología Magerit y herramienta Pilar, se concluye que el CIT está

Tesis publicada con autorización del autor
No olvide citar esta tesis

expuesto a una serie de riesgos que son críticos para su funcionamiento mediante amenazas como: difusión de software dañino, acceso no autorizado". La recomendación es que no debe faltar el área de seguridad informática para que monitoree constantemente los riesgos que puede haber.

Bernal y Villar (2017) Dashboard para la gestión de riesgos de TI en cumplimiento de las exigencias de la SBS en la EDPYME ALTERNATIVA– Chiclayo, Lambayeque.

El principal objetivo de esta investigación es "Desarrollar un dashboard para la gestión de riesgos de TI que permita el cumplimiento de las exigencias de la SBS en la EDPYME Alternativa", el cual lo usará como una herramienta para realizar un eficaz y eficiente Sistema de Gestión de Seguridad para tomar mejores decisiones de lo que se quiere resguardar. Esta investigación es de tipo cuasi experimental del tipo G: X O. Se empleó como instrumento la recolección de datos, entrevistas, encuestas y observaciones directas. El autor cita como una de las principales conclusiones: "Se logró implementar un dashboard como soporte del modelo de gestión de los riesgos de TI propuesto y que permite evaluar con efectividad cada uno de los componentes considerados en el modelo para cada etapa: identificación y evaluación de riesgos de TI y el tratamiento de los riesgos en rangos no tolerables".

Valdiviezo (2016) Análisis de Riesgos de los activos de información de la Clínica Internacional – Piura aplicando la metodología MAGERIT.

La presente investigación tiene como objetivo aplicar la Metodología Magerit a fin de saber la situación actual del riesgo que tienen los activos de información. El tipo de investigación es descriptiva porque se determinará los activos que hay y se identificará las amenazas, vulnerabilidades y riesgos, además de proponer

Tesis publicada con autorización del autor
No olvide citar esta tesis

salvaguardas. Se utilizaron distintos instrumentos como cuestionarios, registros y fichas de observación que fueron adaptados a la Organización.

Como muestra usaron 84 activos aplicando la metodología Magerit. Entre las conclusiones se determinó que se tuvo una probabilidad de amenaza alta siendo los errores y fallos no intencionados por parte de los usuarios y "con las salvaguardas implantadas se redujo el impacto y riesgo a nivel medio".

2.1.2. *Antecedentes internacionales*

Tubío, López & Rivas. (2019). Improving information security risk analysis by including threat-occurrence predictive models. DOI: 10.1016/j.cose.2019.101609

La revista científica nos describe que, a lo largo del tiempo, diferentes herramientas han ayudado a resguardar la información incluyendo metodologías para calcular los riesgos. El objetivo principal del trabajo es realizar una predicción de las amenazas con los activos actuales del sistema, a fin de mejorar el cálculo de riesgos, utilizando la Metodología Magerit y mostrando como resultado una precisión mayor del 70%, de esta manera, desarrollar eficientes salvaguardas para reducir pérdidas y mejorar la seguridad de la organización.

Barafort (2018) INTEGRATED RISK MANAGEMENT PROCESS IMPROVEMENT FRAMEWORK IN IT SETTINGS BASED ON ISO STANDARDS

Esta investigación tiene como objetivo principal explorar la gestión de riesgos en entornos de TI desde el ángulo de los siguientes estándares ISO: ISO 31000, ISO 27001, ISO 9001. ISO 21500. La contribución que hará esta investigación lo divide en 3 etapas:

Tesis publicada con autorización del autor
No olvide citar esta tesis

La primera será la identificación de actividades de gestión de riesgo según los estándares mencionados. Una vez identificado estas actividades, se integran las actividades en entornos TI y se obtienen procesos dedicados de sistema de gestión de riesgo. Finalmente, se menciona sobre la mejora de procesos de la gestión de riesgos para la evaluación de procesos. El resultado muestra un marco integrado que mejora la gestión de riesgo en entornos TI en base a estándares ISO.

Ararat (2018) Diseño de un SGSI basado en la norma ISO 27001 para la empresa MA PEÑALOSA CÍA.S.A.S. sede principal Cúcuta.

El objetivo principal de la investigación es proponer una implementación de Sistema de Gestión de la Seguridad de la Información realizada con la Norma ISO 27001 para crear políticas de seguridad y la metodología Magerit para el inventario de activos y verificar las amenazas. Entre las principales conclusiones se muestra: Después de realizar un análisis de riesgo se determina que la empresa requiere de procedimientos para una Gestión de riesgos, igualmente de una falta de capacitación a los usuarios sobre los riesgos informáticos y para finalizar el compromiso de los directivos de la organización ya que ellos deberán ser los principales promotores de las normas implementadas y seguir de ejemplo hacia los demás.

Yañez (2017) Sistema de gestión de seguridad de la información para la Subsecretaría de Economía y empresas de menor tamaño.

El autor menciona como principal objetivo “Definir e implementar un conjunto de sistemas basados en software open source para crear un SGSI de costo asequible, que cumpla con la normativa indicada en la ISO27001:2013”. Para esto seguirá las pautas de la norma ISO para lograr la disponibilidad, integridad

Tesis publicada con autorización del autor
No olvide citar esta tesis

y confidencialidad de la información para la continuidad del negocio. Para esta investigación se realizaron auditorias y utilizaron técnicas de recojo de información y entrevistas al personal de sistemas. Entre las conclusiones el autor señala: “La forma de trabajo, definida en torno a la creación de equipos constituidos por los propios dueños o encargados de los procesos organizacionales, tuvo un alto impacto positivo en la formulación e implantación de políticas y procedimientos de seguridad de la información”.

Molina-Miranda. (2017). Análisis de riesgos de centro de datos basado en la herramienta pilar de Magerit. DOI: 10.31876/re.v1i11.125

En esta investigación de la revista científica identifica que el principal objetivo es “la aportación de este estudio es identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad implementada y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos”. Se indica que tuvo una problemática con la información, no se cuenta con información económica, estadística, financiera ni registros oficiales. Ante esto se menciona que la investigación servirá como guía. Esta investigación es de tipo cualitativa aplicado en los servicios informáticos de la Universidad. Cabe destacar, que se usa la herramienta Pilar que permitirá realizar informes escritos y salvaguardas. Esta herramienta permitió identificar rápidamente la necesidad de implementar procedimientos y normas lo cual permitirá la protección de los recursos e información.

Tesis publicada con autorización del autor
No olvide citar esta tesis

2.2. Bases teóricas

2.2.1. *Seguridad de la información*

Solarte F., Enriquez E., Benavides M. (2015) define la seguridad informática como "las metodologías, procesos y procedimientos para mantener salvaguardada la información y los datos confidenciales de una organización, al interior de los sistemas informáticos", teniendo como principal objetivo proteger la información y los sistemas de la información del acceso, divulgación, uso indebido, interrupción o destrucción sin consentimiento. Así mismo, mencionemos otra definición hecha por INDECOPI (2007) indica que: "La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios" (pag1). Además, INDECOPI (2014) menciona que los objetivos de la seguridad de la información deben:

- Ser consistentes con la política de seguridad de la información.
- Ser medibles (si es práctico).
- Tomar en cuenta requisitos aplicables de seguridad de la información y resultados de la valoración y tratamiento de riesgos.
- Ser comunicados.
- Ser actualizados según sea apropiado (p.8).

La seguridad de la información tiene como finalidad proteger la confidencialidad, disponibilidad e integridad de la información mediante una metodología y unos procesos de control.

Tesis publicada con autorización del autor
No olvide citar esta tesis

a. *Dimensiones de seguridad*

La seguridad de la información tiene tres principales dimensiones de las cuales detallaremos las siguientes:

La confidencialidad según Reiner et al. (2016) afirma que "es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización" (p.15). Es decir, la información solo debe ser vista y tratada por personas autorizadas, si esta es vulnerada se minimiza la confianza de los demás en la organización y puede llevar al incumplimiento de leyes sobre la custodia de la información.

La integridad se refiere según Reiner et al. (2016). "es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados". La información que se envía o recibe debe ser íntegra y solo será modificada por personal autorizado. La información deja de ser íntegra cuando alguna persona, programa o proceso modifica o borra datos de dicha información.

De la misma forma Reiner et al. (2016) menciona que la disponibilidad "es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones" (p.15). El concepto indica que personas autorizadas pueden ingresar a la información en el momento que se requiera.

El valor estimado que se le da a cada activo es el promedio de las tres dimensiones: $VE = (C+I+D) / 3$

Tesis publicada con autorización del autor
No olvide citar esta tesis

2.2.2. *Gestión de riesgo*

Según la ISO27000 define la gestión de riesgos como las "Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo". Así mismo Llontop (2018) indica que "se refiere al tratamiento de las incidencias que comprometan la continuidad de las actividades comunes de la empresa, así como las amenazas que puedan poner en riesgo la información del usuario, siendo estos importantes patrimonios para la empresa" (p.23). Con lo cual ayudará al personal encargado a tomar acciones para disminuir las posibilidades de que un incidente pueda suceder y afecte a la organización.

De la misma forma, la Gestión de riesgo basa su proceso en el PDCA, desde su inicio para una adecuada toma de decisiones.

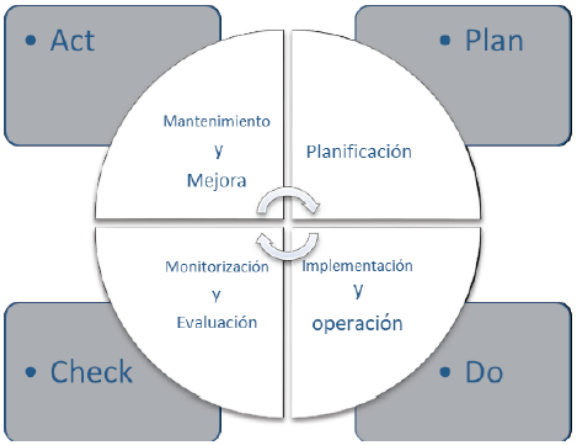


Figura 1. Ciclo PDCA
2017 por Espirales revista multidisciplinaria de investigación

Para empezar a realizar una gestión de riesgos adecuada, se debe elaborar una identificación de activos que serán objeto de estudio e ingresados en el inventario de activos; describiendo su nombre, categoría y propietario. Magerit (2012) menciona sobre los activos: "Componente o funcionalidad de un sistema

Tesis publicada con autorización del autor
No olvide citar esta tesis

de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización" (p.22).

De igual manera Ponce (2011) nos dice: "Un activo es un componente o una parte de un sistema global al que la organización asigna un valor y, por tanto, requiere protección" (p.64).

Cabe destacar que en esta investigación se tomarán de muestra los equipos informáticos, equipos de red, la información almacenada, la infraestructura y servicios.

Guanoluisa Huertas & Maldonado Soliz (2015) divide los activos de la siguiente manera:

Activos primarios: Comprenden los servicios procesos y actividades esenciales para la organización.

Activos de soporte: Son los activos que dependen de los activos primarios.

a. *Valor de un activo*

Los activos informáticos deben valorarse siguiendo una clasificación de acuerdo a su carácter personal o de seguridad (Magerit, 2012). Al valorar los activos se deben tomar en cuenta el CID, determinando la importancia del activo para la organización de acuerdo a una escala de valores establecida.

2.2.3. *Análisis de riesgo*

La ISO27000 lo define como el: "Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo". De la misma forma Molina-Miranda (2017) afirma de manera similar como "el proceso sistemático para

Tesis publicada con autorización del autor
No olvide citar esta tesis

estimar la magnitud de los riesgos a que está expuesta una organización" (p.2). Y en base a los resultados se identifica cuál es su valor y cuanto está protegido siguiendo objetivos y estrategias para generar un plan adecuado.

Podemos agregar que el análisis de riesgo puede agruparse en tres categorías: cuantitativa (cuantificando sus consecuencias), cualitativa (ordenando su importancia) y ambas, esto dependerá de la información que se desee obtener y el nivel de detalle que se analice.

Así mismo Molina-Miranda (2017) indica como objetivos del análisis de riesgo:

- Identificar las amenazas por tipo de activo
- Identificar las vulnerabilidades.
- Identificar el riesgo y cómo afecta las dimensiones de los activos (CID).
- Obtener el nivel de tolerancia al riesgo.

El análisis de riesgo siempre debe estar en constante monitoreo, debido a los cambios que se producen en la tecnología y los nuevos riesgos que aparecen con dichos cambios. Magerit (2012) menciona que al determinar una amenaza que afecta a un activo, se tiene que valorar la influencia de este tomando en cuenta la degradación y la probabilidad.

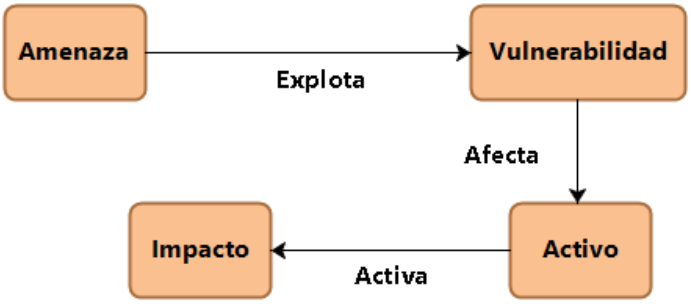


Figura 2. Proceso de riesgo de un activo.
Elaboración propia.

Tesis publicada con autorización del autor
No olvide citar esta tesis

2.2.4. *Tratamiento de riesgo*

Al conocer el estado de riesgo se empieza con la etapa de tratamiento de riesgo, el cuál según Quispe, Pacheco (2018) indica que "consiste en establecer e implementar las acciones correctivas a tomar para poder mitigar los riesgos identificados y poder lograr riesgos residuales aceptados por la empresa según su apetito del riesgo que se haya definido previamente" (p.50). Cabe destacar que para este proyecto se identificará qué control de la norma ISO 27001 se aplicará.

Así mismo Magerit (2012) afirma que en esta fase se va a elaborar un plan que al implementarse y poner en operación cumplirá con los objetivos de minimizar el riesgo a un nivel aceptable. En esta etapa la participación del personal que trabaja con los activos es importante, ya que estarán pendientes de los incidentes y la monitorización de los sistemas a fin de determinar si el tratamiento implantado cumple con los objetivos.

Para el tratamiento de riesgos, existen criterios que se aplicarán en los activos que son afectados, Guanoluisa Huertas & Maldonado Soliz (2015) menciona como principales criterios: reducir, aceptar, evitar, transferir.



Figura 3. Criterios para el tratamiento de riesgo.
2015 por Guanoluisa Huertas & Maldonado Soliz

Tesis publicada con autorización del autor
No olvide citar esta tesis

a. *Las salvaguardas*

Según Magerit (2012), nos dice “son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo” (p.31). Para seleccionar las mejores salvaguardas dependiendo del riesgo, es necesario que se clasifique por lo que verdaderamente sea relevante para la organización, es por eso, que Magerit (2012) menciona priorizar de acuerdo con:

- Tipo de activo a proteger.
- Dimensiones de seguridad que requieren protección.
- Amenazas de las que necesitamos protegernos.
- Si existen salvaguardas alternativas.

Y de acuerdo con la proporcionalidad:

- Mayor o menor valor propio o acumulado sobre un activo.
- La mayor o menor probabilidad de que una amenaza ocurra.
- La cobertura del riesgo que proporcionan salvaguardas alternativas (p.31).

Mencionar que Magerit (2012) menciona diferentes tipos de protección de salvaguardas, las cuales son:

Tesis publicada con autorización del autor
No olvide citar esta tesis

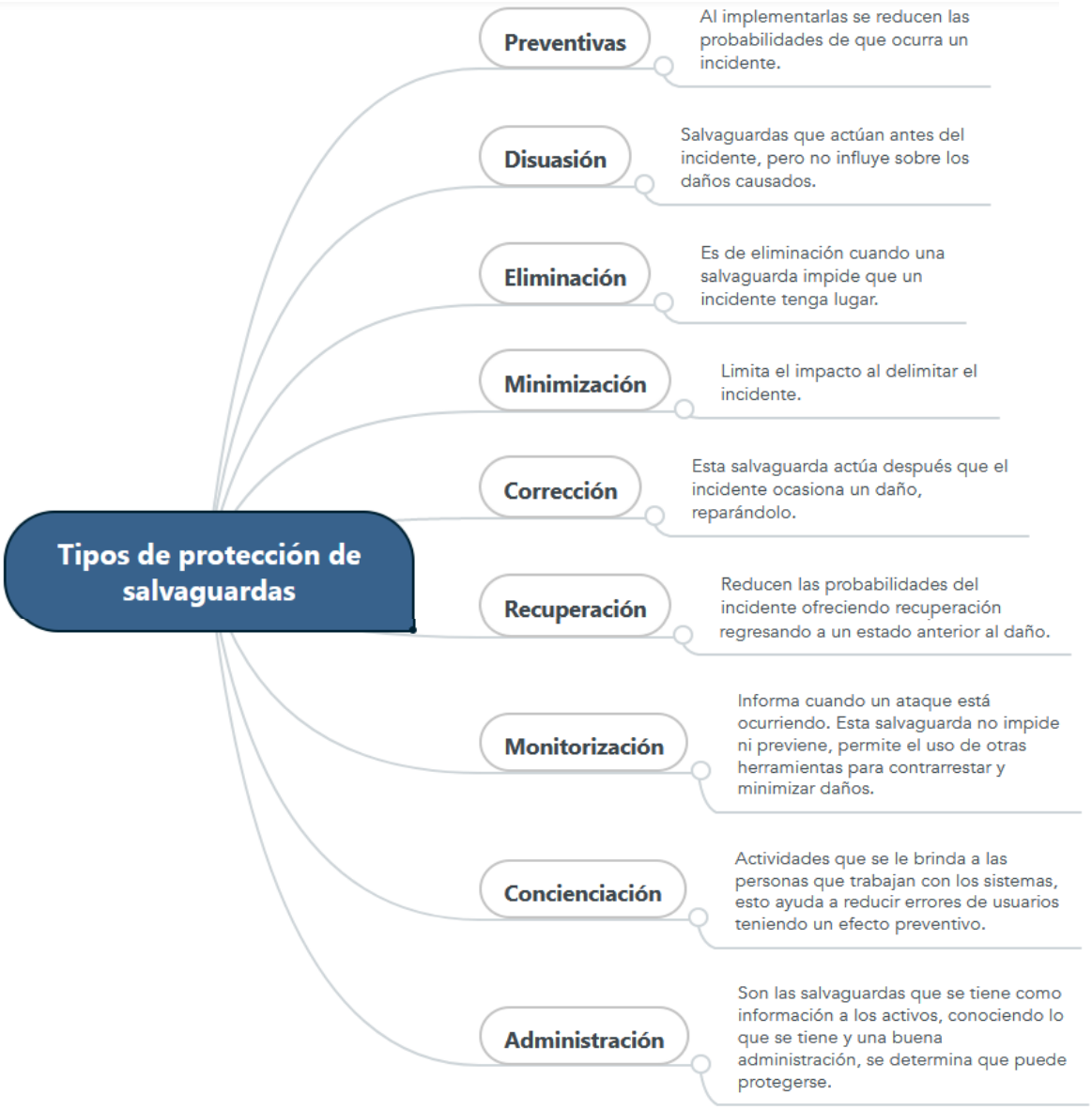


Figura 4. Tipos de protección según Magerit.
Elaboración propia

En este proyecto se implementarán salvaguardas de acuerdo a los riesgos encontrados teniendo como guía a Magerit y controles del anexo A de la ISO 27001.

2.2.5. *Declaración de aplicabilidad (SOA)*

La noma ISO27002 lo define como un documento en el que se establece los riesgos de información y los controles de seguridad necesarios para el SGSI de la organización. Consta de 114 controles, 35 objetivos de control y 14 dominios.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Los indicadores para estas dimensiones serán documentos en los cuales se pondrán para el valor de riesgo (N° de valor) y controles (si/no). Las dimensiones serán medibles con estos criterios:

El valor de riesgo: Jara (2018) dice que el indicador para esta dimensión será el número resultante de riesgo de cada activo, a través de la siguiente fórmula:

$$NR = (P \times I)$$

Tratamiento de riesgo: Jara (2018) dice que el indicador para esta dimensión será la cantidad de controles aplicados mediante la fórmula:

CA = ISO - (CNE + CNA)

CA = N° de controles aplicados.

Ciso = N° de controles ISO 27002

CNE = N° de controles no existentes.

CNA = N° de controles no aplicables.

Este documento permitirá mantener un registro y control de medidas de seguridad aplicadas. Los controles se deberán seleccionar de acuerdo al riesgo en cada activo, con el objetivo de reducir el riesgo a un nivel aceptable. Igualmente puede determinar si un control no se justifica implementarlo (p.61).

2.2.6. *Metodología Magerit*

Es el acrónimo de Metodología de Análisis y Gestión de Riesgo de Sistemas de la Información, fue creada en el año 1997 por el Consejo Superior de Administración Electrónica de España (CSAE). Magerit (2012) afirma que la Gestión de riesgo es “el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización” (p.9).

Tesis publicada con autorización del autor
No olvide citar esta tesis

Esta metodología consta de una serie de pasos como reconocer los activos relevantes que hay, identificar las amenazas, indicar las salvaguardas necesarias según el riesgo, estimar el impacto que puede realizar la amenaza y finalmente medir el riesgo relacionado con el impacto. Todo esto se realiza mediante un plan de seguridad que se establece y la participación del personal que se relaciona con la información.

Magerit (2012) menciona en su libro II, los tipos de activos importantes que hay, como son la información y los servicios que presta. Además, otros activos relevantes como:



Figura 5. Activos relevantes según Magerit
Elaboración propia

Tesis publicada con autorización del autor
No olvide citar esta tesis

Según esta metodología, una vez identificado los activos se les asigna un valor, así Magerit (2012) dice "La valoración se puede ver desde la perspectiva de la 'necesidad de proteger' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes" (p.24). La Gestión de riesgo que sigue Magerit lo realiza mediante este conjunto de fases:

a. *Determinación del contexto*

Magerit (2012) indica que "lleva a una determinación de los parámetros y condicionantes externos e internos que permiten encuadrar la política que se seguirá para gestionar los riesgos" (p.20). Como parámetros internos podemos considerar la situación económica de la organización, características del capital humano y objetivos a mediano y largo plazo. Igualmente, los parámetros externos como el entorno legal, tecnológico, de mercado, a nivel local, nacional o internacional.

b. *Identificación de los riesgos*

La Norma ISO 27000 menciona como "el proceso de encontrar, reconocer y describir riesgos". En el instrumento validado que se aplicará se especifican los activos, amenazas, vulnerabilidades, impacto, probabilidad y riesgo; Todo esto en base a datos históricos, análisis, opiniones de expertos.

c. *La evaluación de los riesgos*

Magerit (2012) nos dice "Aquí entran factores de percepción, de estrategia y de política permitiendo tomar decisiones respecto de qué riesgos se aceptan y cuáles no" (p.20). Se evalúa los más importantes

Tesis publicada con autorización del autor
No olvide citar esta tesis

para priorizar los riesgos a tratar. Se considera los criterios de impacto como son legal, operativo y económico, entre otros.

d. *El tratamiento de riesgo*

En esta etapa se realizan las acciones que se tomarán a fin de minimizar el riesgo, tomando como criterios el de evitar, asumir, eliminar, modificar, compartir y retener. Así mismo, se identifica los controles según la norma ISO 27001 que se aplicará.

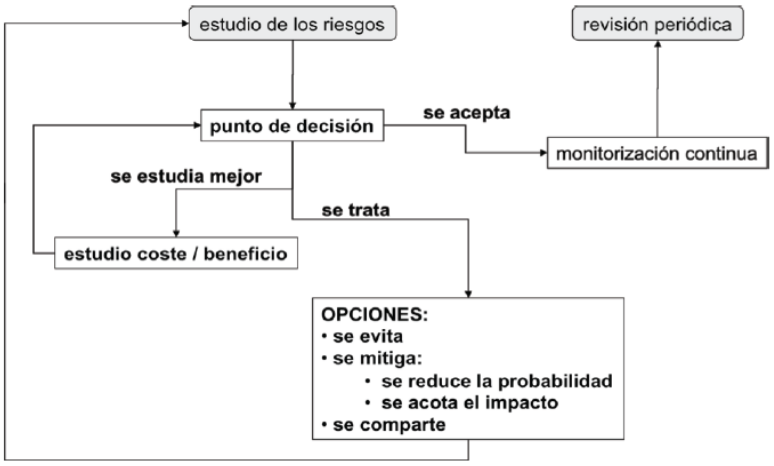


Figura 6. Proceso de tratamiento de riesgo.
2012 MAGERIT – versión 3.0 Libro I

e. *Comunicación y consulta*

En esta penúltima fase, Magerit (2012) indica “Siempre hay que buscar un equilibrio entre seguridad y productividad y en ese equilibrio hay que contar con la colaboración de varios interlocutores” (p.20). Las opiniones de los usuarios se deben escuchar; ya que, son colaboradores activos en las operaciones del sistema. Asimismo, brindar instrucciones a los proveedores para que den un buen servicio y que la gerencia brinde canales de comunicación para consolidar la confianza de los sistemas de información para alcanzar los objetivos.

Tesis publicada con autorización del autor
No olvide citar esta tesis

f. *Seguimiento y control*

Se recopila información de las acciones que se realizaron, lo que ocurrió en cada acción y decisiones que se tomaron, y esto permitirá ir mejorando el conocimiento sobre los sistemas; así como, la mejora del análisis de riesgo que será cambiante en el tiempo.



Figura 7. Proceso de Gestión de Riesgo.
2015. Guía de aproximación para el empresario.

Magerit promueve concientizar a los responsables y personal de la organización del riesgo que hay actualmente en los sistemas de información e identificarlos para tomar las medidas necesarias a tiempo.

2.2.7. *Amenazas*

Ponce (2011) define las amenazas: "consiste en aprovechar las deficiencias o debilidades de un sistema para lanzar un ataque" (p.67). Dicho de otro modo, un sistema vulnerable corre más riesgo a sufrir amenazas; para ello, la solución inmediata es corregir y disminuir estas vulnerabilidades para que los ataques no causen más daño. El análisis de riesgo permite desarrollar medidas para

Tesis publicada con autorización del autor
No olvide citar esta tesis

mitigarlas. Las amenazas son cosas que ocurren y pueden ocurrir a los activos y causar daño (Magerit, 2012).

a. *Identificación de las amenazas*

Magerit (2012) presenta el siguiente grupo de amenazas:

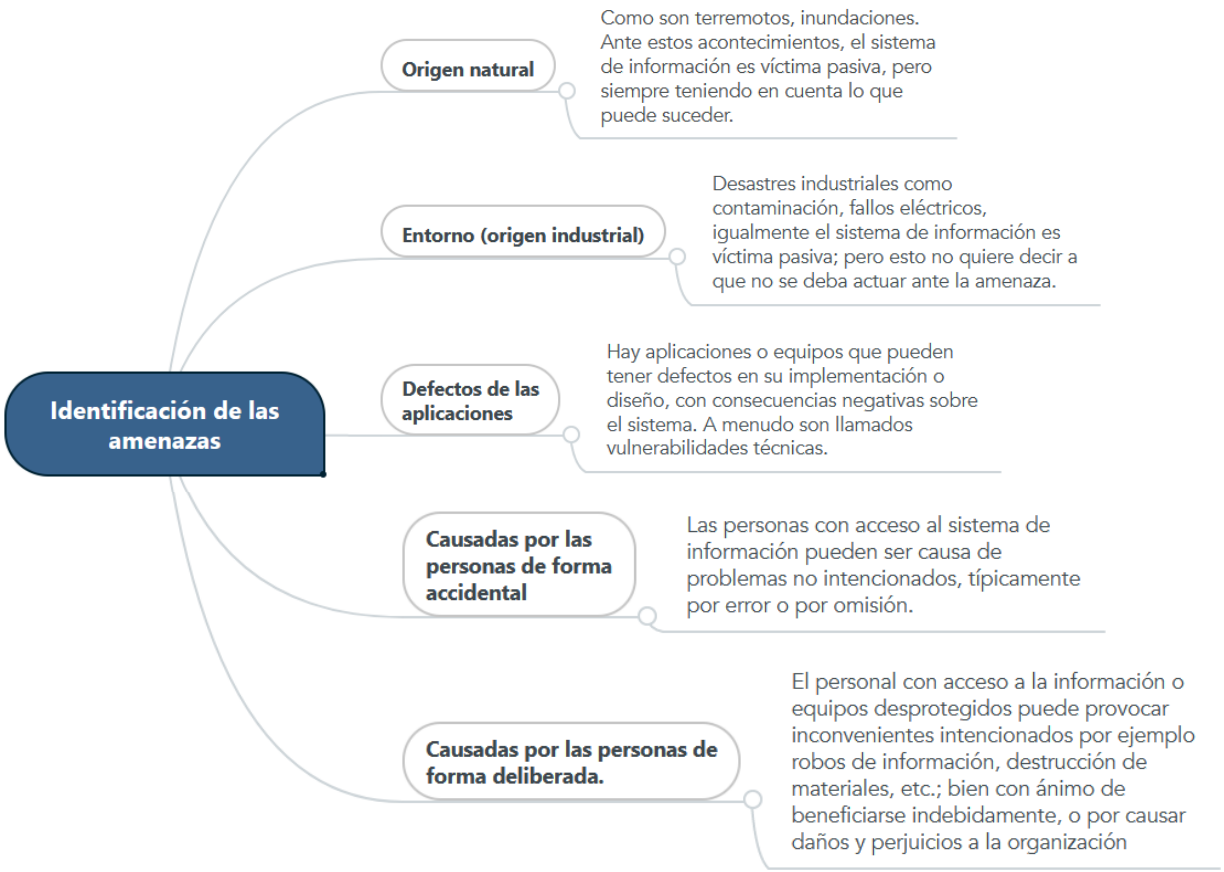


Figura 8. Identificación de las amenazas por Magerit.
Elaboración propia

2.2.8. *La probabilidad de la amenaza*

Magerit (2012) menciona que "cuán probable o improbable es que se materialice la amenaza". Nos ayuda a ver qué tan seguro o no están los activos y la valoración del costo de las pérdidas en caso suceda algún incidente. La probabilidad se mide de acuerdo con la siguiente tabla:

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

Tabla 1
Probabilidad de la amenaza

Clasificación	Descripción
Muy Alto (5)	Diario
Alto (4)	Una vez la semana
Medio (3)	Una vez al mes
Bajo (2)	Una vez cada 6 meses
Muy Bajo (1)	Una vez cada año

Nota: Elaboración propia.

2.2.9. *Vulnerabilidades*

Ararat (2018) define las vulnerabilidades como "el conjunto de debilidades que establecen que tan susceptible puede ser la empresa a la hora de recibir una amenaza informática o circunstancial" (p.29). De la misma manera Magerit (2012) dice que es "toda vulnerabilidad que puede ser aprovechada por una amenaza" (p.35).

Tabla 2
Nivel de vulnerabilidad

Clasificación	Descripción
Muy Alto (5)	No hay controles para contener la amenaza
Alto (4)	Hay controles, pero no se documentan.
Medio (3)	Hay controles documentados, pero no son medibles
Bajo (2)	Hay controles medibles, pero no son mejorados
Muy Bajo (1)	Existen controles continuamente mejorados

Nota: Elaboración propia.

2.2.10. *Degradación*

Magerit (2012) menciona la degradación como "cuán perjudicado resultaría el valor del activo". Indica que mide el daño que causaría a un activo si ocurriera un incidente. Y el resultado nos mostraría qué activos requieren mayor atención.

Tabla 3
Degradación del valor

Abreviatura	Descripción
MA	Muy alta
A	Alta
M	Media
B	Baja
MB	Muy baja

Nota: Valor de degradación a un activo.
Recuperado de MAGERIT– versión 3.0 Libro I Método 2012.

Tesis publicada con autorización del autor
No olvide citar esta tesis

2.2.11. *Control*

Es la medida por la cual va a modificar el riesgo de un activo mediante políticas, procesos, prácticas, entre otros que se implementen en la Institución. Para esto se usará el instrumento de control del anexo A de la ISO 27002, se eligen dependiendo del resultado para aquellos activos que requieran reducir su riesgo a un nivel aceptable.

2.2.12. *Impacto residual*

Magerit (2012) indica que es el impacto resultante después de implementar las salvaguardas.

2.2.13. *Metodología*

"Una metodología se materializa por un conjunto de métodos, técnicas y herramientas. No contiene métodos específicos; sin embargo, lo especifica por procesos que conforman el marco de gestión de riesgo" (Molina-Miranda, 2017, p.3).

2.2.14. *Seguridad*

Magerit (2012) lo define como la "capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas" (p.8). Es decir, protege las propiedades de los activos, redes, procesos (confidencialidad, integridad y disponibilidad).

2.2.15. *Riesgo*

Ararat (2018) indica que el riesgo es la "probabilidad de que la amenaza que se pueda presentar en la empresa se convierta en un desastre" (p.29). Si la vulnerabilidad que hay en un activo de información es alta, el riesgo es alto, ocasionando pérdida a la organización si no se controla con tiempo.

Tesis publicada con autorización del autor
No olvide citar esta tesis

2.2.16. *Riesgo residual*

Magerit (2012) indica que es el valor de riesgo resultante después de implementar las salvaguardas y controles necesarios. En esta nueva medición solo cambian la magnitud de la probabilidad residual. (p. 35)

2.3. Objetivos de la investigación

2.3.1. *Objetivo general*

Demostrar como la mejora de la seguridad de la información influye en el proceso de gestión de riesgo en la Fundación para el desarrollo solidario.

2.3.2. *Objetivos específicos*

Demostrar como la mejora de la seguridad de la información influye en la evaluación de riesgo de la Fundación para el Desarrollo Solidario.

Demostrar como la mejora de la seguridad de la información influye en el tratamiento de riesgo de la Fundación para el Desarrollo Solidario.

2.4. Formulación de hipótesis

2.4.1. *Hipótesis general*

La mejora de la seguridad de la información influye significativamente en el proceso de gestión de riesgo en la Fundación para el Desarrollo Solidario.

2.4.2. *Hipótesis especificas*

La mejora de la seguridad de la información influye significativamente en la evaluación de riesgo de la Fundación para el Desarrollo Solidario.

La mejora de la seguridad de la información influye significativamente en el Tratamiento de riesgo de la Fundación para el Desarrollo Solidario.

Tesis publicada con autorización del autor
No olvide citar esta tesis

CAPITULO III: DISEÑO METODOLÓGICO

3.1. Diseño de la investigación

La presente investigación utilizará un diseño de investigación pre experimental permitiendo usar a un grupo de activos que recibirán una manipulación, aplicando causa efecto entre las variables. Se realizará una identificación actual del contexto (pre test), se aplicará la metodología Magerit y se obtendrá un resultado (post test).

G: Grupo experimental que recibirá la metodología.

O1: Resultado Pre test

O2: Resultado Post test

X: Variable aplicativo

G = O1 x O2

3.2. Tipo

El tipo estudio de investigación que se realiza es aplicada de corte longitudinal. Será longitudinal porque se va a estudiar y evaluar a una variable obteniendo dos resultados (antes y después). Además, se podrá actualizar constantemente los datos ya que la tecnología tiene cambios constantes, como indica Delgado y Llorca (2004) "El análisis debe tener en cuenta las medidas repetidas y esto es lo que confiere finalmente a un estudio su carácter longitudinal" (p.141).

3.3. Enfoque

El tipo de enfoque que se usará es cuantitativo, ya que se empezará describiendo la situación actual de los activos y riesgos que hay, aplicando una metodología.

Tesis publicada con autorización del autor
No olvide citar esta tesis

3.4. Población

La Fundación para el Desarrollo Solidario ubicado en el distrito de Barranco con el objetivo de ayudar a mejorar la condición de vida de las personas con problemas de discapacidad cuenta con 123 activos que comprende personal, información, servicios hardware y software, que se agruparán de acuerdo a su importancia y estos serán objeto de estudio en la metodología aplicada. Magerit permitió reducir a 58 activos importantes en la institución que serán objeto de estudio.

3.5. Muestra

En la investigación se tomará como muestra el tipo no probabilístico y el criterio de selección será por conveniencia porque se tomará a un grupo de activos que se identificarán de acuerdo a la información que se recolecte en base a inventarios, documentación y consultas a personal.

3.6. Operacionalización de variables

3.6.1. *Variable dependiente: Gestión de riesgo*

Jara (2018) menciona al Proceso de gestión de riesgo como el "conjunto de fases sucesivas, que implican evaluar el riesgo y tratar el riesgo en el contexto de la organización, estas acciones involucran llevar el nivel de riesgo a un grado aceptable y determinar el número de controles aplicados para su reducir el riesgo" (p.60). Magerit (2012) complementa el concepto como "El proceso de gestión de riesgos debe identificar y tratar urgentemente los riesgos críticos, pudiendo ir tratando progresivamente riesgos de menor criticidad" (p.13). Mediante estas actividades determinarán que acciones se deben tomar con los activos en riesgo y gestionarlos hasta llegar a un riesgo aceptable. Según Magerit (2012) la gestión de riesgo posee las siguientes dimensiones: Análisis de riesgo y Tratamiento de riesgo.

Tesis publicada con autorización del autor
No olvide citar esta tesis

a. *Análisis de riesgo*

Magerit (2012) indica que "El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema. Proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas" (p.10). Esto se realiza a través de un procedimiento documentado donde detalla cómo se identifica, analizan, evalúan, y priorizan los riesgos relacionados a los activos más relevantes. Los pasos que determina Magerit (2012) a seguir son:

- Seleccionar activos
- Mostrar las amenazas en que los activos están comprometidos.
- Determinar las salvaguardas.
- Evaluar el impacto

b. *Tratamiento de riesgo*

Magerit (2012) dice: "En coordinación con los objetivos, estrategia y política de la Organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la Dirección" (p.10). Igualmente, Jara (2018) indica la forma de tratar y/o modificar el riesgo es:

- Prevenir las situaciones que lo provocan.
- Minimizar la probabilidad del impacto.
- Compartir el riesgo
- Asumiendo o aceptando.

Durante el desarrollo del tratamiento se "determina el número de controles aplicados para reducir el riesgo". Y para realizarlo se aplicará a través de la ficha de observación usando el modelo de la ISO 27001 anexo A.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Jara (2018) dice que para evaluar y tratar el riesgo dentro de la organización y llevarlos a un nivel aceptable se debe medir o valorar el riesgo y determinar los controles a través del instrumento como la ficha de observación. Para este proyecto se usará ambos indicadores a fin de determinar el grado de riesgo que hay en los activos.

3.6.2. *Variable independiente: Seguridad de la información*

La ISO/IEC 27000 (2009) indica que "La seguridad de la información implica la aplicación y gestión de medidas de seguridad adecuadas que implican la consideración de una amplia gama de amenazas. Incluye tres dimensiones principales: confidencialidad, disponibilidad e integridad". Son medidas tanto preventivas como reactivas que se adaptan a las organizaciones para permitir resguardar y proteger la información que se encuentran en diferentes medios, además de impedir la ejecución de operaciones no autorizadas en un sistema permitiendo mantener la confidencialidad. integridad y disponibilidad de los datos. Además, Magerit (2012) indica que sus dimensiones son las siguientes:

- Confidencialidad
- Integridad
- Disponibilidad

a. *Confidencialidad*

Magerit (2012) "que la información llegue solamente a las personas autorizadas "(p9). Propiedad de la información por la cual solo será accesible mediante una comprobada y debida autorización y esta no deberá ser mostrada por personas o sistemas que no estén autorizados.

Tesis publicada con autorización del autor
No olvide citar esta tesis

b. *Integridad*

Magerit (2012) “mantenimiento de las características de completitud y corrección de los datos” (p.9). Es una cualidad de la información en la cual no debe ser modificada, manteniendo sus datos íntegros como fueron generados, sin alteraciones de ningún tipo.

c. *Disponibilidad*

Acerca de la disponibilidad Magerit (2012) dice que es la “disposición de los servicios a ser usados cuando sea necesario” (p.9). Los servicios y los activos deben estar aptos los trabajos en la organización cuando se requiera, para ello deben estar en buenas condiciones y en constante monitoreo en caso de algún incidente.

Tabla 4
Variable dependiente

Variable	Dimensión	Indicador
Gestión de riesgo	Evaluación de riesgo	Nivel de riesgo
	Tratamiento de riesgo	Número de controles aplicados

Nota: Elaboración propia.

3.7. Técnicas para la recolección de datos

La técnica empleada en esta investigación para medir las variables es la observación directa. De acuerdo con Bernal (2010) “permite conocer de forma directa el objeto de estudio para luego describir y analizar situaciones sobre la realidad estudiada”, Esta técnica nos ayuda a determinar los activos que hay en la organización y lo que se tratará en los instrumentos establecidos.

Tesis publicada con autorización del autor
No olvide citar esta tesis

3.7.1. *Descripción de los instrumentos*

En el presente proyecto se tendrá en cuenta realizar dos fichas de observación.

a. *Ficha de observación (Valor de riesgo)*

En la primera ficha de observación nos permitirá saber cómo está actualmente la institución, se describirá los activos más importantes para la institución, se mencionará las amenazas, el impacto que ocasionará estas amenazas y se calculará el riesgo. Con el resultado se determinará cuales tienen mayor riesgo según el rango establecido para este proyecto y se decidirá las salvaguardas adecuadas.

A continuación, se describen los campos que tendrá la ficha valor de riesgo:

- Evaluación de riesgo: Proceso por el cual se identifica, se analiza y se estima un nivel de riesgo.
- Código del activo: Se le da una identificación al activo objeto de estudio.
- Nombre del activo: Descripción del activo.
- Confidencialidad: Valor que se le dará al activo según el acceso que tiene por parte del usuario o proceso autorizado.
- Integridad: Valor que se le dará al activo según su integridad.
- Disponibilidad: Valor que se le da al activo según su disponibilidad.
- Amenaza: Descripción las amenazas que afectan al activo.
- Nivel: Se le da un nivel de amenaza de acuerdo al rango establecido.
- Vulnerabilidad: Descripción de las vulnerabilidades que afectan al activo.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Nivel: Se le da un nivel de vulnerabilidad de acuerdo al rango establecido.
- Legal: Se le da un nivel de impacto legal que afectaría a la institución.
- Operativo: Se le da un nivel de impacto operativo que afectaría a la institución.
- Económico: Se le da un nivel de impacto económico que afectaría a la institución.

b. *Ficha de observación (Controles)*

La segunda ficha de observación (controles) se enumerará los controles de seguridad que se implementarán en la institución, luego de los resultados de la evaluación y tratamiento de riesgos. Estos controles se adaptarán de acuerdo a las necesidades de la institución, permitirá saber el estado actual de los controles y una valoración de lo que hay actualmente y como estará al aplicarlo. A continuación, se detalla los campos que tendrá la ficha controles:

- Control de riesgo: Instrumento que indica los controles que hay y los que necesitan implementarse.
- Sección: Código de cada control establecido por la ISO27001.
- Control: Descripción de los controles establecidos por la ISO27001.
- Estado actual: Es el estado que determina si el control está implementado en la institución.
- Valoración: Es el resultado de saber si un control esta implementado o no en la organización.

Tesis publicada con autorización del autor
No olvide citar esta tesis

3.7.2. *Validez y confiabilidad de los instrumentos*

a. Validación

El concepto de validación como lo menciona Hernández, Fernández y Baptista, (2014) indica que un instrumento mostrara un resultado de la variable que mide. Para este proyecto de investigación la validación estará a cargo de un juicio de expertos quienes calificaron y categorizaron cada instrumento que medirá la variable.

b. Confiabilidad

Es el resultado de una aplicación de forma repetida que se hace al mismo objeto de estudio produciendo resultados iguales (Hernández, Fernández y Baptista, 2014). El instrumento aplicará la prueba estadística del Test y Retest. Tomándose la información anterior al pre test y post test, de manera que se correlacionan ambos grupos de datos.

3.8. Técnica para el procesamiento y análisis de datos

A través de las fichas de observación de las dimensiones de riesgo y controles, se construye una base de datos utilizando la herramienta SPSS, expresados en porcentajes.

Para el análisis de los datos que corresponde a la estadística descriptiva, se utilizará en el procesamiento de datos cualitativo, para variables de tipo nominal y ordinal, la distribución de frecuencias por cada grupo de información. Asimismo, se mostrarán los gráficos de barras para la comparación de grupos del pre y post test. Para Inferencia estadística, respecto a las pruebas de hipótesis, considerando que las variables son cualitativas, por lo tanto, no tienen normalidad, para la comparación de los grupos, se utilizará la prueba de Wilcoxon.

Tesis publicada con autorización del autor
No olvide citar esta tesis

3.9. Aspectos éticos

Para esta investigación se recolectará información sobre los activos informáticos que será el grupo investigado, procesos y controles. Los resultados mostrarán si será necesario o no concientizar al personal. La institución tiene conocimiento de esta recolección mediante una constancia de consentimiento informado firmada por el representante legal donde se detalla lo que se realizará. El investigador solicitará el consentimiento informado a los participantes y se compromete a no revelar información confidencial de los mismos.

CAPITULO IV: RESULTADOS

En este capítulo se presenta el análisis de las causas que detalla el riesgo en los activos informáticos en la Fundación para el Desarrollo Solidario mediante la evaluación de riesgo, el cual, a través de un inventario de activos nos ayuda a identificar los problemas que hay en seguridad. Del mismo modo, se describe como la seguridad de la información influye en el tratamiento de riesgo mediante la implementación de políticas que contribuirá a minimizar los riesgos informáticos en la institución.

Datos obtenidos de la revista de investigaciones aplicadas de la Universidad de Trujillo (Poma, Vargas, 2019) muestra una tabla de los principales ataques de seguridad que en Perú se generó, siendo el medio de ataque principales las amenazas web (43.60%) y el correo electrónico (22.32%), medios que son usados frecuentemente en las oficinas. De acuerdo a esta información recopilada, los ataques de información (amenazas) se dan en su mayoría a los usuarios quienes por desconocimiento son los que causan en su mayoría este problema (vulnerabilidad).

Es por esto que en la institución se realiza este proyecto para mejorar el sistema de información, ya que, las medidas actuales no son las adecuadas. Asimismo, posterior a los resultados del análisis se tendrá una visión más amplia de los riesgos mostrados a través de los instrumentos aplicados y validados estadísticamente.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Tabla 5
Nivel de Riesgo Pre test y Post test

N°	Activos	Pre test	Post test
1	Datos públicos	20	10
2	Registros de la organización	20	10
3	Datos de carácter personal	20	10
4	Datos clasificados	20	10
5	Usuarios externos (asociadas)	20	8
6	Usuarios internos	20	8
7	Internet	12	9
8	Acceso remoto	16	8
9	Correo electrónico	16	8
10	Almacenamiento de datos	20	8
11	Claves de autenticación	20	8
12	Transferencia de datos	16	8
13	Gestión de identidades	20	8
14	Gestión de privilegios	20	8
15	Software CONCAR	20	8
16	Cliente de correo electrónico	9	9
17	Antivirus	20	8
18	Sistema Operativo	16	8
19	Sistema de backups	20	8
20	Servidor	20	8
21	Desktop	20	8
22	Laptop	20	8
23	Marcador digital	6	6
24	Router de internet	16	8
25	Router de telefonía	16	8
26	Switch de datos - Internet	16	8
27	Switch de datos - Telefonía	16	8
28	Switch de datos inalámbrico	16	8
29	Convertidor a fibra óptica	10	6
30	Firewall de datos	16	8
31	Central telefónica	16	8
32	Teléfonos IP	4	4
33	Access point 1	4	4
34	Access point 2	4	4
35	Access point 3	4	4
36	Medios de impresión	4	4
37	Equipos de respaldo	20	8
38	Red de internet	12	8
39	Red telefónica	9	9
40	Red inalámbrica	6	6
41	Discos externos	15	6
42	Almacenamiento en red	20	8
43	Material impreso	16	12
44	CD-ROM	16	12
45	Fuentes de alimentación	10	4
46	UPS	6	6

Tesis publicada con autorización del autor
No olvide citar esta tesis

47	Equipos de aclimatación	9	9
48	Cableado estructurado	6	9
49	Fibra óptica	6	9
50	Mobiliario: armarios, racks.	25	10
51	Edificio	12	8
52	Oficina	12	8
53	Almacén	9	9
54	Cuarto de servidor	12	8
55	Canalización	6	4
56	Usuarios finales	16	8
57	Administrador de Sistemas	20	8
58	Usuarios externos (Proveedores)	15	9
	Nivel de riesgo	**14.33**	**7.79**

Nota: Resultados en detalle del nivel de riesgo en la fase pre test y post test.

La tabla anterior muestra un nivel de riesgo promedio de 14.33 en la etapa pre test, al aplicar los controles y políticas de las salvaguardas el nivel tiene como resultado un 7.79 en promedio en la etapa post test. A este nuevo resultado se le llama riesgo residual.

Mediante la estadística descriptiva e inferencial se muestra los resultados que obtuvieron en el software SPSS usándose la prueba de Wilcoxon para la inferencia estadística y el gráfico de barras para la estadística descriptiva.

4.1. Estadística descriptiva

4.1.1. *Gestión de riesgo*

Tabla 6
Muestra descriptiva de la tabla cruzada de la Gestión de riesgo.

		Criterio			
		Bajo	Medio	Alto	Total
Pre test	Recuento	41	15	2	58
	% dentro de Prueba	70,7%	25,9%	3,4%	100,0%
Post test	Recuento	2	52	4	58
	% dentro de Prueba	3,4%	89,7%	6,9%	100,0%

Nota: Tabla realizada en el SPSS.

Tesis publicada con autorización del autor
No olvide citar esta tesis

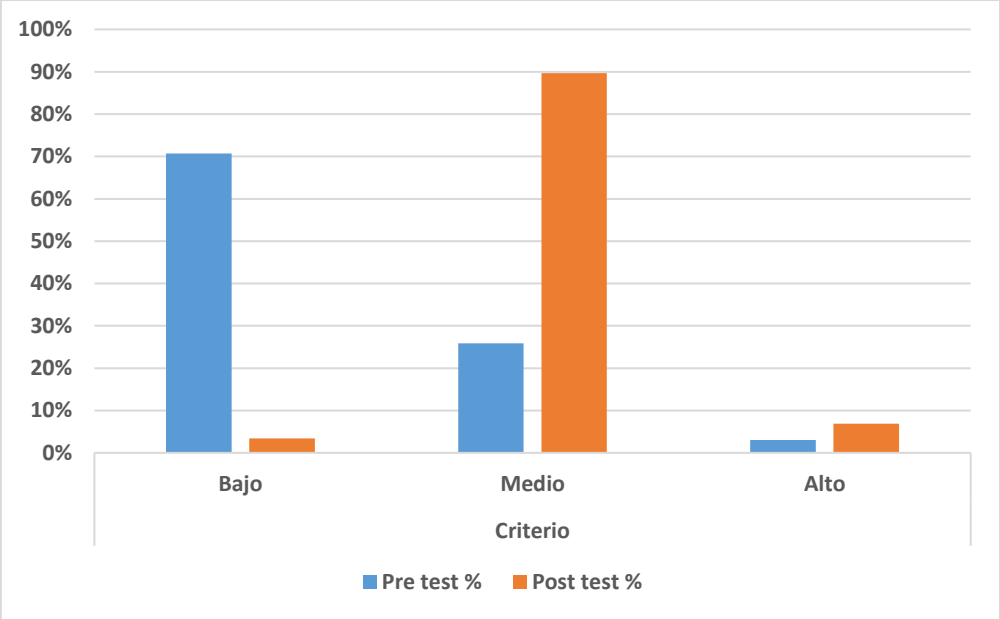


Figura 9. Gráfico de barras de la gestión de riesgo.
Hay una tendencia a la gestión de riesgo moderada de la que antes había con los cambios aplicados.
Elaboración propia.

a. Interpretación

La tabla 6 muestra el recuento y el porcentaje de la gestión de riesgo en la etapa pre y post test, mediante una escala de alto, moderado, bajo. La gestión de riesgo en el pre test tiene un recuento de 41 activos equivalente al 70.7% (bajo), 15 activos equivalente al 25.9% (medio) y 2 activos equivalente al 3.4% (alto). En el post test al aplicar las salvaguardas, muestra un recuento de 2 activos equivalente al 3.4% (bajo), 52 activos equivalente al 89.7% (medio) y 4 activos equivalente al 6.9% (alto).

4.1.2. *Evaluación de riesgo*

Tabla 7
Muestra descriptiva de la tabla cruzada de la Evaluación de riesgo.

		Criterio				
		Crítico	Alto	Moderado	Bajo	Total
Pre test	Recuento	34	7	12	5	58
	% dentro de Prueba	58,6%	12,1%	20,7%	8,6%	100,0%
Post test	Recuento	0	2	41	15	58
	% dentro de Prueba	0,0%	3,4%	70,7%	25,9%	100,0%

Nota: Tabla realizada en el SPSS.

Tesis publicada con autorización del autor
No olvide citar esta tesis

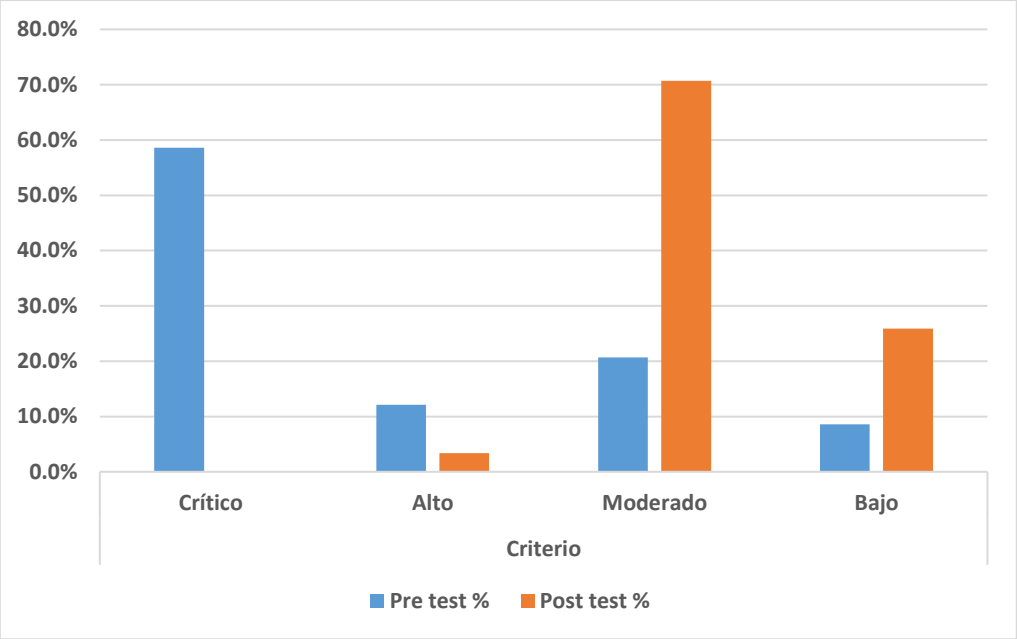


Figura 10. Gráfico de barras de la evaluación de riesgo.
Los activos en estado crítico y alto pasan al riesgo moderado con los cambios aplicados.
Elaboración propia.

a. Interpretación

La tabla 7 muestra el recuento y el porcentaje en nivel crítico, alto, moderado, bajo en que se encuentran los activos. En el pre test, la evaluación de riesgo tiene un total de 58 en el cual hay 34 activos equivalente al 58.6% (crítico), 7 activos equivalente al 12,1% (alto), 12 activos equivalente al 20.7% (Moderado) y 5 activos equivalente al 8.6% (Bajo). Dando un total de 58 activos

En el post test al aplicar las salvaguardas, muestra un recuento de 0 activos equivalente al 0.0% (crítico), 2 activos equivalente al 3,4% (alto), 41 activos equivalente al 70.7% (Moderado) y 15 activos equivalente al 25,9% (Bajo).

Tesis publicada con autorización del autor
No olvide citar esta tesis

4.1.3. *Tratamiento de riesgo*

Tabla 8
Muestra descriptiva de la tabla cruzada del Tratamiento de riesgo.

			Criterio		
			No existe	Existe	Total
Prueba	Pre test	Recuento	107	7	114
		% dentro de Prueba	93,9%	6,1%	100,0%
	Post test	Recuento	12	102	114
		% dentro de Prueba	10,5%	89,5%	100,0%

Nota: Tabla realizada en el SPSS.

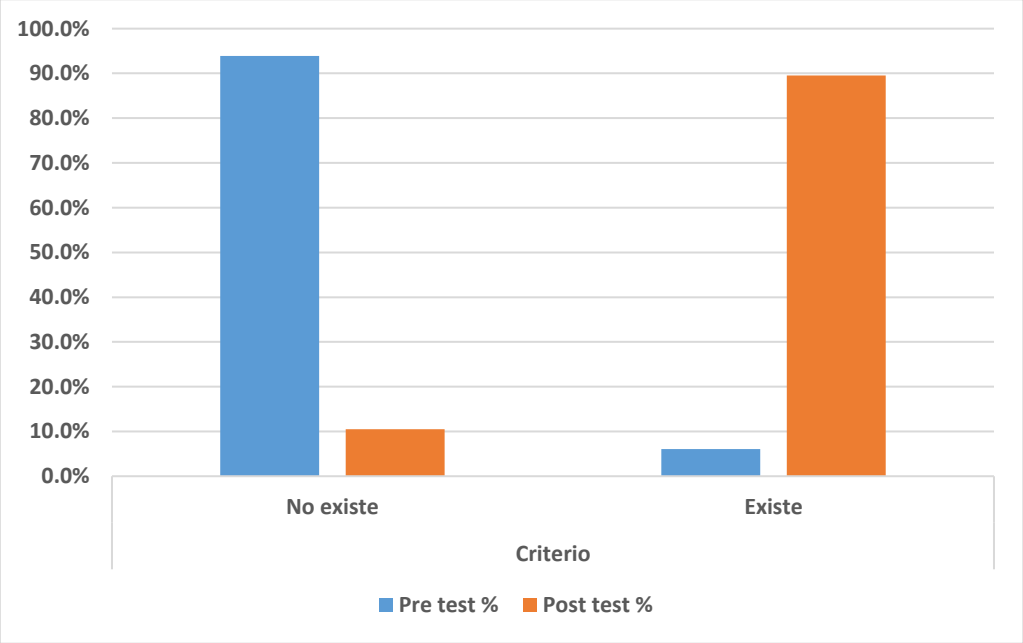


Figura 11. Gráfico de barras del tratamiento de riesgo.
En el post test hay más controles aplicados (102) y por ende una mejor seguridad de información.

a. Interpretación

La tabla 8 muestra el recuento y el porcentaje de los controles que existen y no existen en la institución. En el pre test, el tratamiento de riesgo muestra un total de 114 controles los cuales 107 (93.9%) de controles no existentes y 7(6.1%) de controles existentes; Para el post test, los controles no existentes son 12(10.5%) y 102(89.5%) de controles existentes.

Tesis publicada con autorización del autor
No olvide citar esta tesis

4.2. Contraste de hipótesis

4.2.1. *Prueba de hipótesis general*

Considerando que las variables son ordinales sin normalidad, aplicamos la prueba de comparación de grupos para muestras relacionadas, es decir, la prueba de Wilcoxon.

H_0: La seguridad de la información no influye significativamente en el proceso de gestión de riesgo de la Fundación para el Desarrollo Solidario.

H_1: La seguridad de la información influye significativamente en el proceso de gestión de riesgo de la Fundación para el Desarrollo Solidario

Medida de significación: Será de 0.05

Criterio de decisión: Si el p. < 0.05, la H_0 es rechazada; Si el p. > 0.05 la H_0 se acepta.

Tabla 9
Prueba de Wilcoxon para la Gestión de riesgo

		N	Rango promedio	Suma de rangos
Proceso de gestión de riesgo (Post test) - Proceso de gestión de riesgo (Pre test)	Rangos negativos	0[a]	,00	,00
	Rangos positivos	58[b]	29,50	1711,00
	Empates	0[c]		
	Total	58		

Tabla 10
Prueba del p-valor en el pre test y post test

Z	-7,441[b]
Sig. asintótica(bilateral)	,000

a. Resultado estadístico:

Considerando que las variables son ordinales sin normalidad, aplicamos la prueba de comparación de grupos para muestras relacionadas (Wilcoxon).

Tesis publicada con autorización del autor
No olvide citar esta tesis

La prueba estadística de Wilcoxon muestra una medida de significación = 0,00 siendo menor al criterio de decisión establecido ($p < 0.05$) resultando la H_0 rechazada y asegurando que la seguridad de la información influye significativamente en la gestión de riesgo en la Fundación para el Desarrollo Solidario.

4.2.2. *Prueba de Hipótesis específica*

H_0: La seguridad de la información no influye significativamente en la evaluación de riesgo de la Fundación para el Desarrollo Solidario.

H_1: La seguridad de la información influye significativamente en la evaluación de riesgo de la Fundación para el Desarrollo Solidario.

Medida de significación: Será de 0.05

Criterio de decisión: Si el p. < 0.05, la H_0 es rechazada; Si el p. > 0.05 la H_0 se acepta.

Tabla 11
Prueba de Wilcoxon para la Evaluación de riesgo

		N	Rango promedio	Suma de rangos
Evaluación de riesgo (Post Test) - Evaluación de riesgo (Pre test)	Rangos negativos	0[a]	,00	,00
	Rangos positivos	42[b]	21,50	903,00
	Empates	16[c]		
	Total	58		

Tabla 12
Prueba del p-valor en el pre test y post test

Z	-5,808[b]
Sig. asintótica(bilateral)	,000

Tesis publicada con autorización del autor
No olvide citar esta tesis

a. Resultado estadístico

Considerando que las variables son ordinales sin normalidad, aplicamos la prueba de comparación de grupos para muestras relacionadas (Wilcoxon). La prueba estadística de Wilcoxon muestra una medida de significación = 0,00 siendo menor al criterio de decisión establecido ($p < 0.05$) resultando la H_0 rechazada y asegurando que la seguridad de la información influye significativamente en la evaluación de riesgo en la Fundación para el Desarrollo Solidario.

H_0: La seguridad de la información no influye significativamente en el tratamiento de riesgo de la Fundación para el Desarrollo Solidario.

H_1: La seguridad de la información influye significativamente en el tratamiento de riesgo de la Fundación para el Desarrollo Solidario.

Medida de significación: Será de 0.05

Criterio de decisión: Si el p. < 0.05, la H_0 es rechazada; Si el p. > 0.05 la H_0 se acepta.

Tabla 13
Prueba de Wilcoxon para el Tratamiento de riesgo

		N	Rango promedio	Suma de rangos
Tratamiento de riesgo (Post test) - Tratamiento de riesgo (Pre test)	Rangos negativos	0[a]	,00	,00
	Rangos positivos	95[b]	48,00	4560,00
	Empates	19[c]		
	Total	114		

Tabla 14
Prueba del p-valor en el pre test y post test

Z	-9,747[b]
Sig. asintótica(bilateral)	,000

Tesis publicada con autorización del autor
No olvide citar esta tesis

a. Resultado estadístico

Considerando que las variables son ordinales sin normalidad, aplicamos la prueba de comparación de grupos para muestras relacionadas (Wilcoxon). La prueba estadística de Wilcoxon muestra una medida de significación = 0,00 siendo menor al criterio de decisión establecido ($p < 0.05$) resultando la H_0 rechazada y asegurando que la seguridad de la información influye significativamente en el tratamiento de riesgo en la Fundación para el Desarrollo Solidario.

Tesis publicada con autorización del autor
No olvide citar esta tesis

CAPITULO V: DISCUSION, CONCLUSIONES Y RECOMENDACIONES

5.1. Discusión

Lo encontrado en esta investigación demuestran que hay una mejora de seguridad en la institución y por eso aceptamos la hipótesis general en la cual establece que hay una influencia de la seguridad de la información en el proceso de gestión de riesgo, gracias a la evaluación y tratamiento que se implementa y la metodología usada para realizar el proyecto en la institución.

En base a la hipótesis especifica plateada N°1 “La mejora de la seguridad de la información influye significativamente en la evaluación de riesgo de la Fundación para el Desarrollo Solidario” se puede evidenciar a través de los datos que resultaron del instrumento evaluación de riesgo que hay una mejora en la seguridad de la información desde el pre test hasta la aplicación de las salvaguardas en la etapa post test. Al igual que Jara (2018) los resultados se relacionan porque demuestra que existe una mejora en la gestión de riesgo a través de la evaluación y tratamiento, lo cual es importante para esta investigación. Las comparaciones de nivel de riesgo en dos etapas distintas demostraron que en la etapa pre test tuvo un nivel de riesgo de 11 (en promedio) y al aplicar los controles obtuvo un mejor resultado de 5.67 (en promedio) de riesgo.

En base a la hipótesis especifica plateada N°2 “La mejora de la seguridad de la información influye significativamente en el tratamiento de riesgo de la Fundación para el Desarrollo Solidario” se puede evidenciar a través de los datos obtenidos por el instrumento del tratamiento de riesgo que políticas implementadas en diversos sectores influyeron en la mejora de la seguridad. Asimismo, los resultados guardan relación con lo que menciona Barafort (2018) que en su investigación explora la gestión de riesgos en entornos TI a través de los estándares ISO 31000 27001, 90001, obteniendo como resultado una integración de procesos entre distintas áreas. De

Tesis publicada con autorización del autor
No olvide citar esta tesis

igual forma Villegas (2018) en su investigación analiza el problema interno que hay con respecto a la seguridad, el desconocimiento de los directivos y no tener una seguridad adecuada; Asimismo, permite saber que activos necesitan de cuidados, así como las políticas que necesitan ser implementados para su funcionamiento adecuado, puntos que son relevante para esta investigación.

Finalmente, Olaza (2017) realiza en su proyecto de tesis la implementación de NTP ISO 27001 para el Ministerio de Educación, en el cual realiza comparativos (antes y después) sobre las dimensiones de los datos (confidencialidad, integridad y disponibilidad) obteniendo como resultados una mejora en la propiedad de los datos. La información y proceso sirvió como base para esta investigación.

Tesis publicada con autorización del autor
No olvide citar esta tesis

5.2. Conclusiones

Como conclusión general, el contenido de la tesis y sus complementos originados en el contexto de la investigación, se afirma que se ha alcanzado los objetivos presentados en el capítulo II de esta tesis.

1. Se demostró como la implementación de la seguridad de la información influye en el proceso de gestión de riesgo en la Fundación para el Desarrollo Solidario. Los resultados presentados estadísticamente muestran que la gestión de riesgo cambia de un estado bajo (25.9%) a uno moderado (89.7%) y alto (6.9%) por las medidas que se implementaron.
2. En base al objetivo específico N°1: La implementación de la seguridad de la información influyó en la evaluación de riesgo de la Fundación para el Desarrollo Solidario. Se logró determinar mediante análisis estadístico como se redujo el nivel de riesgo en las fases crítica (58.6%) y alto (12.1%) pasando a una fase alta (3.4%), moderada (70.7%) y baja (25.9%). Encontrándose que las medidas adoptadas mejoraron la seguridad de la información.
3. Asimismo, en base al objetivo específico N°2: La implementación de la seguridad de la información influyó en el tratamiento de riesgo de la Fundación para el Desarrollo Solidario. Se logró determina mediante análisis estadístico que los controles de seguridad solo estaban implementados en un 6.1% y luego pasó a tener un 89.5% encontrándose que al aplicarse los controles y políticas mejoró la seguridad de la información.
4. Las organizaciones para un mejor control de sus activos, su valoración y minimizar las amenazas requieren del uso de una metodología de análisis de riesgo ayudando a seleccionar las medidas, controles, mejorando sus procesos y ser reconocidos en el sector que se desempeñan.

Tesis publicada con autorización del autor
No olvide citar esta tesis

5.3. Recomendaciones

1. En base a la conclusión N° 1 se recomienda que instituciones como ONG y en general tengas establecidos una gestión de riesgo en base a estándares, por ejemplo, se puede emplear ISO 27000 o la NTP-ISO/IEC 27001 que son guías de buenas prácticas para seguridad de la información, ayudan a tener mejores decisiones y se puede emplear en diferentes áreas. Con el tiempo el gobierno podría sugerir y/o hacerlo ley que se cumplan estas buenas prácticas según los recursos y objetivos de cada empresa.
2. En base a la conclusión N° 2 la evaluación de riesgo debe ser realizado cada cierto tiempo e impuesto como una norma interna en cada empresa, asimismo una auditoria interna y externa ayuda a verificar el nivel de riesgo, siempre y cuando se tengan los recursos y alcanzar alguna certificación internacional si es requerido.
3. En base a la conclusión N° 3 el personal interno y externo de cada empresa, deben seguir lo controles y políticas establecidos, los responsables de seguridad deben formular planes de acción ante incidentes y concientizar al personal mediante publicidad, acciones recreativas, charlas, etc. Sobre los ataques que cada vez son más constantes.
4. Las instituciones con pocos recursos pueden implementar este tipo de modelos, ya que se demuestra tener una idea más clara de lo que se tiene, juntamente con una metodología que sea acorde a los requerimientos de cada institución. Los resultados serán expuestos a cada persona que tome las decisiones.
5. Muchas veces la seguridad no es tomada en cuenta por los usuarios y empresas, el Congreso y el Estado Peruano deberían fortalecer, sugerir e implementar acciones en temas de ciberseguridad y usar la tecnología como

Tesis publicada con autorización del autor
No olvide citar esta tesis

herramienta para el transporte, banca, en contra de la delincuencia, etc. a fin de incentivar a las generaciones desde temprana edad y llegar con un conocimiento amplio en una posterior etapa.

Tesis publicada con autorización del autor
No olvide citar esta tesis

REFERENCIAS BIBLIOGRÁFICAS

Agroindustrial Pomalca S.A.A. – 2016 (Tesis de pregrado). Recuperado de http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/2440/BC-TES-TMP1311.pdf?sequence=1&isAllowed=y.

Ararat, J. (2018). Diseño de un SGSI basado en la Norma ISO 27001 para la empresa MA PEÑALOSA CÍA. S.A.S. sede principal Cúcuta (Tesis de pregrado). Recuperado de https://repository.unad.edu.co/bitstream/handle/10596/21259/27604094.pdf?sequence=1&isAllowed=y.

Barafort, B. (2018) INTEGRATED RISK MANAGEMENT PROCESS IMPROVEMENT FRAMEWORK IN IT SETTINGS BASED ON ISO STANDARDS (Tesis Doctoral). Recuperado de https://dialnet.unirioja.es/servlet/tesis?codigo=260427

Behar, D. (2008). Metodología de la Investigación. Recuperado de http://rdigital.unicv.edu.cv/bitstream/123456789/106/3/Libro%20metodologia%20investigacion%20este.pdf

Bernal, H. y Villar, J. (2017) DASHBOARD PARA LA GESTIÓN DE RIESGOS DE TI EN CUMPLIMIENTO DE LAS EXIGENCIAS DE LA SBS EN LA EDPYME ALTERNATIVA – CHICLAYO, LAMBAYEQUE (Tesis de pregrado). Recuperado de http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/5054/BC-TES-%203856%20BERNAL%20VALLEJOS%20%20VILLAR%20SOBERON.pdf?sequence=1&isAllowed=y.

Bernal Torres, César (2010) Metodología de la investigación administración, economía, humanidades y ciencias sociales (3ª edición).

ISBN: 978-958-699 128-5

Hernández R., Fernández C. y Baptista.P, (2014). Metodología de la Investigación (3ª edición) [archivo PDF]. Mexico. Recuperado de ISBN: 978-1-4562-2396-0.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Delgado, M. y Llorca, J. (2004). Estudios longitudinales: concepto y particularidades. *Revista Española de Salud Pública*, 78(2), 141-148. Recuperado de http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1135-57272004000200002&lng=es&tlng=es

Dirección general de modernización Administrativa, procedimientos e impulso de la administración electrónica. (2012). Magerit – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Recuperado de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

Domínguez, J. (2015). Seguridad Informática Personal y Corporativa (Segunda parte). Recuperado de https://www.academia.edu/19595640/Seguridad_Inform%C3%A1tica_Personaly_Corporativa_Segunda_parte_

Encuesta Global de Seguridad de la Información de EY (2020). Recuperado de https://assets.ey.com/content/dam/ey-sites/ey-com/es_pe/topics/cybersecurity/ey-giss-como-pasar-seguridad-aislada-integrada.pdf

Garcia, J. y Huamani S (2019) Modelo de gestión de riesgos de seguridad de la información para pymes en el Perú. Recuperado de https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/625905/garcia_pj.pdf?sequence=3&isAllowed=y

Guanoluisa Huertas, J. E., & Maldonado Soliz, I. F. (2015). Análisis de Riesgos y Diseño de un Plan de Seguridad de la Información para el Consejo Nacional de Igualdad de Discapacidades "CONADIS" (Proyecto previo a la obtención del título de Ingeniero en Sistemas Informáticos y de Computación). Quito. Recuperado de https://bibdigital.epn.edu.ec/bitstream/15000/10499/1/CD-__6217.pdf

INDECOPI. (2014). Norma Técnica Peruana ntp-ISO-IEC-27001 (2da ed.)

Tesis publicada con autorización del autor
No olvide citar esta tesis

ISO/IEC 27000. (2005). Definición Gestión de riesgo. Recuperado de http://www.iso27000.es/glosario.html#section10p

Jara, O. (2018) Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018 (Tesis de maestría). Recuperado de http://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/31209/Jara_MOY.pdf?sequence=1&isAllowed=y

Llontop, G. (2018) Gestión de riesgos de Tecnologías de Información de las empresas de Nephila Networks (Tesis de maestría). Recuperado de http://repositorio.ucv.edu.pe/handle/UCV/17596.

Molina-Miranda, M. F. (2017). Análisis de riesgos de centro de datos basado en la herramienta Pilar de Magerit. DOI: 10.31876/re.v1i11.125

Olaza, H. (2017). "Implementación de NTP ISO/IEC 27001 para la Seguridad de Información en el Área de Configuración y Activos del Ministerio de Educación – Sede Centromin". Recuperado de https://repositorio.ucv.edu.pe/handle/20.500.12692/9927

Olaza, C. y Aquino J. (2018) Diseño de un Sistema de Gestión de Seguridad de la Información Basado en la Norma Iso/Iec 27001:2013 para la Empresa Agroindustrial Pomalca S.A.A. – 2016. Recuperado de http://repositorio.unprg.edu.pe/handle/UNPRG/2440

Ponce, D. (2011). Análisis y gestión de riesgos de seguridad de la información (Tesis de pregrado). Recuperado de http://dspace.unitru.edu.pe/bitstream/handle/UNITRU/11435/PONCE%20PAJUELO%2C%20Dante%20Jacob.pdf?sequence=1&isAllowed=y.

Quispe Loarte, J. E. & Pacheco Pedemonte, D. L. (2018). Modelo de evaluación de riesgos de seguridad de la información basado en la ISO/IEC 2705 para analizar la viabilidad de adoptar un servicio en la nube. Universidad Peruana de Ciencias Aplicadas (UPC), Lima, Perú, 2018. Recuperado de https://repositorioacademico.upc.edu.pe/handle/10757/625879

Tesis publicada con autorización del autor
No olvide citar esta tesis

Poma, V. y Vargas, V. (2017). Problemática en Ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el Mundo. DOI: http://dx.doi.org/10.17268/sciendo.2019.034

Sandoval, J. (2017) Diseño de un Plan de Seguridad de la Información para el Centro de Informática y Telecomunicaciones de la Universidad Nacional de Piura, Periodo 2015-2018 (Tesis de pregrado). Recuperado de http://repositorio.unp.edu.pe/bitstream/handle/UNP/1165/IND-SAN-QUI-17.pdf?sequence=1&isAllowed=y.

Seguridad de la información. (n.d.). Glosario Terminología Informática. Recuperado de: http://www.tugurium.com/gti/termino.php?Tr=information%20security&Tp=T &Or=0

Solarte, F., Enriquez E., y Benavides M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL – RTE, Vol. 28, N. 5, 492-507.* Recuperado de http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

Tubío, P., López, C., y Rivas, J. (2019). Improving information security risk analysis by including threat-occurrence predictive models. Computers & Security. 88. 101609, 1-10. DOI: 10.1016/j.cose.2019.101609.

Universidad Peruana de Ciencias Aplicadas (UPC), Lima, Perú, 2018. Recuperado de https://repositorioacademico.upc.edu.pe/handle/10757/625879

Valdiviezo, Y. (2016) Análisis de Riesgos de los activos de información de la Clínica Internacional – Piura aplicando la metodología MAGERIT (Tesis de pregrado). Recuperado de http://repositorio.ucv.edu.pe/handle/UCV/11924.

Villegas, C. y Aquino J. (2018) Diseño de un Sistema de Gestión de Seguridad de la Información Basado en la Norma Iso/Iec 27001:2013 para la Empresa Agroindustrial Pomalca S.A.A. – 2016. Recuperado de http://repositorio.unprg.edu.pe/handle/UNPRG/2440

Tesis publicada con autorización del autor
No olvide citar esta tesis

Wikipedians, & Creutzburg, Reiner & Briseño, Editor & Oyervides, Editor & Carranco, Editor & Ricalde, Editor. (2016). Seguridad Informática y Análisis Forense Digital. 10.13140/RG.2.1.4578.2641. (Bases teóricas, disponibilidad, etc). Recuperado de https://www.researchgate.net/publication/303974058_Seguridad_Informatica_y_Analisis_Forense_Digital

Tesis publicada con autorización del autor
No olvide citar esta tesis

ABREVIATURAS

CID: Confidencialidad, integridad, disponibilidad.

ISO: Organización Internacional de Normalización.

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

NTP: Norma Técnica Peruana.

ONG: Organización no Gubernamental.

P: p-valor

SOA: Statement of Applicability (Declaración de aplicabilidad)

SPSS: Statistical Package for the Social Sciences.

Tesis publicada con autorización del autor
No olvide citar esta tesis

ANEXOS

ANEXO 1: MATRIZ DE CONSISTENCIA

Problema general	Objetivo general	Hipótesis general	METODO
¿De qué manera la mejora de la seguridad de la información influye en el proceso de gestión de riesgo de la Fundación para el Desarrollo Solidario?	Demostrar como la mejora de la seguridad de la información influye en el proceso de gestión de riesgo en la Fundación para el Desarrollo Solidario.	La seguridad de la información influye significativamente en el proceso de gestión de riesgo en la Fundación para el Desarrollo Solidario.	Metodología: Hipotético deductivo Tipo: Aplicada Enfoque: Cuantitativa Población: Activos críticos de información. Muestra: No probabilístico. Instrumento de recolección de datos: Fichas de observación. Técnica de procesamiento de datos: Análisis estadístico a través del SPSS tablas y gráficos.
Problema Especifico	**Objetivo Especifico**	**Hipótesis Específicos**	
¿De qué manera la seguridad de la información influye en la evaluación de riesgo de la Fundación para el Desarrollo Solidario?	Demostrar como la seguridad de la información influye en la evaluación de riesgo de la Fundación para el Desarrollo Solidario.	La seguridad de la información influye significativamente en la evaluación de riesgo de la Fundación para el Desarrollo Solidario.	
¿De qué manera la seguridad de la informática influye en el tratamiento de riesgo de la Fundación para el Desarrollo Solidario?	Demostrar como la seguridad de la información influye en el tratamiento de riesgo de la Fundación para el Desarrollo Solidario.	La mejora de la seguridad de la información influye significativamente en el tratamiento de riesgo de la Fundación para el Desarrollo Solidario.	

Tesis publicada con autorización del autor
No olvide citar esta tesis

ANEXO 2: MATRIZ DE OPERACIONALIZACIÓN

VARIABLES	DEFINICIÓN	DIMENSIÓN	INDICADOR	ESCALA	INSTRUMENTO
SEGURIDAD DE LA INFORMACIÓN	La ISO/IEC 27000 (2009) indica que "La seguridad de la información implica la aplicación y gestión de medidas de seguridad adecuadas que implican la consideración de una amplia gama de amenazas. Incluye tres dimensiones principales: confidencialidad, disponibilidad e integridad"	Confidencialidad			
		Integridad			
		Disponibilidad			
GESTIÓN DE RIESGO	Jara (2018) menciona al Proceso de gestión de riesgo como el "conjunto de fases sucesivas, que implican evaluar el riesgo y tratar el riesgo en el contexto de la organización, estas acciones involucran llevar el nivel de riesgo a un grado aceptable y determinar el número de controles aplicados para su reducir el riesgo"	Evaluación de riesgo	Nivel de riesgo	Ordinal	Ficha de observación
		Tratamiento de riesgo	Número de controles aplicados	Nominal	Ficha de observación

Tesis publicada con autorización del autor
No olvide citar esta tesis

ANEXO 3: ENCUESTA/INSTRUMENTO DE EVALUACIÓN

FICHA DE OBSERVACIÓN 1 (pre test)

Empresa: Fundación para el Desarrollo Solidario
Fecha //al //
Responsable Elmer Santisteban Avalos
Formato: Nivel de riesgo

GRUPO FUNDADES
Mejorando vidas

CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	C	I	D	AMENAZA	NIVEL	VULNERABILIDAD	NIVEL	LEGAL	OPERATIVO	ECONOMICO

Tesis publicada con autorización del autor
No olvide citar esta tesis

FICHA DE OBSERVACIÓN 2 (pre test)

Empresa: Fundación para el Desarrollo Solidario
Fecha: //al //
Responsable: Elmer Santisteban Avalos
Formato: Número de controles aplicados

GRUPO FUNDADES
Mejorando vidas

SECCIÓN	CONTROL	ESTADO ACTUAL	OBSERVACIONES
A.5 Políticas de seguridad de la información			
A.5.1	**Dirección de la gerencia para la seguridad de la información**		
A.5.1.1	Políticas para la seguridad de la información	No tiene	
A.5.1.2	Revisión de las políticas para la seguridad de la información	No tiene	
A.6 Organización de la seguridad de la información			
A.6.1	**Organización interna**		
A.6.1.1	Roles y responsabilidades para la seguridad de la información	No tiene	
A.6.1.2	Segregación de funciones	No tiene	
A.6.1.3	Contacto con autoridades	No tiene	
A.6.1.4	Contacto con grupos especiales de interés	No tiene	
A.6.1.5	Seguridad de la información en la gestión de proyectos	No tiene	
A.6.2 Dispositivos móviles y teletrabajo			
A.6.2.1	Política de dispositivos móviles	No tiene	
A..6.2.2	Teletrabajo	No tiene	
A.7 Seguridad de los recursos humanos			
A.7.1 Antes del empleo			
A.7.1.1	Investigación de antecedentes	Si tiene	
A.7.1.2	Términos y condiciones del empleo	Si tiene	
A.7.2 Durante el empleo			
A.7.2.1	Responsabilidades de la gerencia	No tiene	
A.7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	No tiene	
A.7.2.3	Proceso disciplinario	No tiene	
A.7.3 Terminación y cambio de empleo			
A7.3.1	Terminación o cambio de responsabilidades del empleo.	No tiene	
A.8 Gestión de activos			
A.8.1 Responsabilidad por los activos			
A.8.1.1	Inventario de activos	No tiene	
A.8.1.2	Propiedad de los activos	No tiene	
A.8.1.3	Uso aceptable de los activos	Si tiene	
A.8.1.4	Retorno de activos	Si tiene	

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

A.8.2 Clasificación de la información				
A.8.2.1	Clasificación de la información			
A.8.2.2	Eliminación de soportes			
A.8.2.3	Manejo de activos			
A.8.3 Manejo de los medios				
A.8.3.1	Gestión de medios removibles			
A.8.3.2	Disposición de medios			
A.8.3.3	Transferencia de medios física			
A.9 Control de acceso				
A.9.1 Requisitos de la empresa para el control de acceso				
A.9.1.1	Política de control de acceso			
A.9.1.2	Acceso a redes y servicios de red			
A.9.2 Gestión de acceso de usuario				
A.9.2.1	Registro y baja de usuarios			
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios			
A.9.2.3	Gestión de los derechos de acceso con privilegios especiales			
A.9.2.4	Gestión de información de autentificación secreta de usuarios			
A.9.2.5	Revisión de derecho de acceso de usuarios			
A.9.2.6	Remoción o ajuste de derechos de acceso			
A.9.3 Responsabilidades de los usuarios				
A9.3.1	Uso de información de autentificación secreta			
A.9.4 Control de acceso a sistemas y aplicaciones				
A.9.4.1	Restricción de acceso a la información			
A.9.4.2	Procedimientos de ingreso seguro			
A.9.4.3	Sistema de gestión de contraseñas			
A.9.4.4	Uso de programas utilitarios privilegiados			
A.9.4.5	Control de acceso al código fuente de los programas			
A.10 Criptografía				
A.10.1 Controles criptográficos				
A.10.1.1	Politica sobre el uso de controles criptográficos			
A.10.1.2	Gestión de claves			
A.11 Seguridad física y ambiental				
A.11.1 Áreas seguras				
A.11.1.1	Perímetro de seguridad física			
A.11.1.2	Controles de ingreso físico			
A.11.1.3	Asegurar oficinas, áreas e instalaciones			
A.11.1.4	Protección contra amenazas externas y ambientales			
A.11.1.5	Trabajo en áreas seguras			
A.11.1.6	Areas de despacho y carga			
A.11.2 Seguridad de los equipos				
A.11.2.1	Emplazamiento y protección de los equipos			
A.11.2.2	Servicios de suministro			
A.11.2.3	Seguridad del cableado			
A.11.2.4	Mantenimiento de equipos			
A.11.2.5	Salida de activos fuera de las dependencias de la empresa			
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones			
A.11.2.7	Retirada o reutilización segura de dispositivos de almacenamiento			
A.11.2.8	Equipos de usuario desatendidos			
A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla			
A.12 Seguridad de las operaciones				
A.12.1 Procedimientos y responsabilidades operativas				
A.12.1.1	Documentación de procedimientos de operación			
A.12.1.2	Gestión del cambio			
A.12.1.3	Gestión de la capacidad			
A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones			
A.12.2 Protección contra códigos maliciosos				
A.12.2.1	Controles contra códigos maliciosos			
A.12.3 Copias de seguridad				
A.12.3.1	Respaldo de la información			
A.12.4 Registros y monitoreo				
A.12.4.1	Registro de eventos			
A.12.4.2	Protección de información de registros			
A.12.4.3	Registros del administrador y del operador			
A.12.4.4	Sicronización de reloj			
A.12.5 Control del software operacional				
A.12.5.1	Instalación de software en sistemas operacionales			
A.12.6 Gestión de vulnerabilidlad técnica				
A12.6.1	Gestión de vulnerabilidades técnicas			
A12.6.2	Restricciones sobre la instalación de softw are			
A.12.7 Consideraciones para la auditoría de los sistemas de información				
A.12.7.1	Controles de auditoría de sistemas de información			
A.13 Seguridad de las comunicaciones				
A.13.1 Gestión de seguridad de la red				
A.13.1.I	Controles de la red			
A.13.1.2	Seguridad de servicios de red			
A.13.1.3	Segregación en redes			
A.13.2 Transferencia de información				
A.13.2.1	Politicas y procedimientos de transferencia de la información			
A.13.2.2	Acuerdo sobre transferencia de información			
A.13.2.3	Mensajes electrónicos			

Tesis publicada con autorización del autor
No olvide citar esta tesis

A.13.2.4	Acuerdos de confidencialidad o no divulgación		
A.14 Adquisición, desarrollo y mantenimiento de sistemas			
A.14.1 Requisitos de seeuridad de los sistemas de información			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la inforrmación		
A.14.1.2	Seguridad de las comunicaciones en servicios accesibles sobre redes públicas		
A.14.1.3	Protección de transacciones en servicios de aplicación		
A.14.2 Seguridad en los procesos de desarrollo y soporte			
A.14.2.1	Política de desarrollo seguro		
A.14.2.2	Procedimientos de control de cambio del sistema		
A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa		
A.14.2.4	Restricciones sobre cambios a los paquetes de software		
A14.2.5	Principios de ingeniería de sisternas seguros		
A.14.2.6	Ambiente de desarrollo seguro		
A.14.2.7	Desarrollo contratado externamente		
A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas		
A.14.2.9	Pruebas de aceptación del sistema		
A.14.3 Datos de prueba			
A.14.3.1	Protección de datos de de prueba		
A.15 Relaciones con los proveedores			
A.15.1 Seguridad de la información en las relaciones con los proveedores			
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores		
A.15.1.2	Tratamiento de riesgo dentro de los acuerdos con proveedores		
A.15.1.3	Cadena de suninistro de tecnología de infromación y comunicación		
A.15.2 Gestión de entrega de servicios del proveedor			
A.15.2.1	Monitoreo y revisión de servicios de los proveedores		
A15.2.2	Gestión de cambios a los servicios de proveedores		
A.16 Gestión de incidentes de seguridad de la información			
A.16.1 Gestión de incidentes de seguridad de la información y mejoras			
A.16.1.1	Responsabilidades y procedimientos		
A.16.1.2	Reporte de eventos de seguridad de la infonnación		
A.16.1.3	Reporte de debilidades de seguridad de la infonnación		
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información		
A.16.1.5	Respuesta a incidentes de seguridad de la infonnación		
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información		
A.16.1.7	Recolección de evidencia		
A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio			
A.17.1 Continuidad de seguridad de la información			
A.17.1..1	Planificación de continuidad de seguridad de la información		
A.17.1.2	Implementación de continuidad de seguridad de la información		
A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información		
A.17.2 Redundancias			
A.17.2.1	Instalaciones de procesamiento de la información		
A.18 Cumplimiento			
A.18.1 Cumplimiento con requisitos legales y contractuales			
A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables		
A.18.1.2	Derechos de propiedad intelectual		
A.18.1.3	Protección de registros de la organización		
A.18.1.4	Privacidad y protección de datos personales		
A.18.1.5	Regulación de controles criptográficos		
A.18.2 Revisiones de seguridad de la información			
A.18.2.1	Revisión independiente de la seguridad de la información		
A.18.2.2	Cumplimiento de políticas y normas de seguridad		
A.18.2.3	Revisión del cumplimiento técnico		

DESCRIPCION	CANTIDAD	%
Controles ISO		
Controles no existentes		
Controles aplicados		
Controles no aplicables		
Total de controles		

Tesis publicada con autorización del autor
No olvide citar esta tesis

ANEXO 4: VALIDEZ DE INSTRUMENTOS POR JUECES EXPERTOS

Facultad de Ciencias Empresariales

UNIVERSIDAD CIENTÍFICA DEL SUR

ANEXO 18

FORMATO DE SOLICITUD DE JUICIO DE EXPERTO

Lima 20 de junio del 2020

Señor,
Luis Torres Cabanillas
Presente. -

De mi consideración,
Siendo conocedor de su trayectoria académica y profesional, me he tomado la libertad de elegirlo como **JUEZ EXPERTO** para revisar el contenido del instrumento que pretendo utilizar para mi investigación. Para ello, adjunto la matriz de consistencia y matriz de operacionalización

A continuación, estos son los criterios de evaluación:

Categoría	Calificación		Indicador
SUFICIENCIA Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta	1	No cumple con el criterio	Los ítems no son suficientes para medir la dimensión
	2	Bajo nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total
	3	Nivel moderado	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4	Alto nivel	Los ítems son suficientes
CLARIDAD Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta	1	No cumple con el criterio	El ítem no es claro
	2	Bajo nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3	Nivel moderado	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4	Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1	No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
	2	Bajo nivel	El ítem tiene una relación tangencial con la dimensión
	3	Nivel moderado	El ítem tiene una relación moderada con la dimensión que está midiendo
	4	Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1	No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2	Bajo nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste
	3	Nivel moderado	El ítem es relativamente importante
	4	Alto nivel	El ítem es muy relevante y debe ser incluido

Los resultados de esta evaluación, servirá para determinar los coeficientes de validez de contenido del presente cuestionario. De ante mano le agradezco su cooperación.

Apellido y Nombre	Elmer Ivan Santisteban Avalos
Código	100032451
Carrera profesional	INGENIERIA DE SISTEMAS DE INFORMACIÓN Y GESTIÓN

Tesis publicada con autorización del autor
No olvide citar esta tesis

Facultad de Ciencias Empresariales

UNIVERSIDAD CIENTÍFICA DEL SUR

ANEXO 18 - A

INFORME DE VALIDEZ DE CONTENIDO Y JUEZ DE EXPERTO

Lima 20 de junio del 2020

Estimado Coordinador de Investigación de la Facultad de Ciencias Empresariales de la Universidad Cientifica del Sur.

A solicitud del tesista, se procedió a revisar la matriz de consistencia, matriz de operacionalización y el instrumento que empleará para su investigación. Según detalle:

Título de la tesis	MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GESTIÓN DE RIESGOS DE LA FUNDACIÓN PARA EL DESARROLLO SOLIDARIO EN EL 2020.
Grado o título que aspira	Ingeniería de Sistemas
Apellidos y Nombre del (los) tesista (s)	Santisteban Avalos Elmer Ivan

Al respecto y de acuerdo con los indicadores mencionados se califica cada uno de los ítems:

Dimensión 1	Ítems (Pregunta)	Suficiencia	Claridad	Coherencia	Relevancia
Evaluación de riesgo	1. Código del activo	4	4	4	4
	2. Nombre del Activo	4	4	4	4
	3. Confidencialidad	4	4	4	4
	4. Integridad	4	4	4	4
	5. Disponibilidad	4	4	4	4
	6. Amenazas	4	4	4	4
	7. Nivel	4	4	4	4
	8. Vulnerabilidades	4	4	4	4
	9. Nivel	4	4	4	4
	10. Legal	4	4	4	4
	11. Operativo	4	4	4	4
	12. Económico	4	4	4	4

Dimensión 2	Ítems (Pregunta)	Suficiencia	Claridad	Coherencia	Relevancia
Control de riesgo	13. Cláusula	4	4	4	4
	14. Sección	4	4	4	4
	15. Control	4	4	4	4
	16. Estado actual	4	4	4	4
	17. Valoraciones	4	4	4	4
	18. Observaciones	4	4	4	4



Firma del Juez Experto

Apellidos y Nombre del experto	Cabanillas Luis Torres
Especialidad del experto	Ingeniero Estadístico – Maestro en Ingeniería de Sistemas
Código de colegiatura	49863
Ficha CTI Vitae (*)	https://ctivitae.concytec.gob.pe/appDirectorioCTI/DirectorioCTI.do?tipo=datosinvestigador

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

Facultad de Ciencias Empresariales

UNIVERSIDAD CIENTÍFICA DEL SUR

ANEXO 18

FORMATO DE SOLICITUD DE JUICIO DE EXPERTO

Lima 23 de junio del 2020

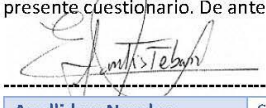
Señora,
Evelyn Gonzales Zuñiga
Presente. -

De mi consideración,
Siendo conocedor de su trayectoria académica y profesional, me he tomado la libertad de elegirlo como **JUEZ EXPERTO** para revisar el contenido del instrumento que pretendo utilizar para mi investigación. Para ello, adjunto la matriz de consistencia y matriz de operacionalización

A continuación, estos son los criterios de evaluación:

Categoría	Calificación		Indicador
SUFICIENCIA Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta	1	No cumple con el criterio	Los ítems no son suficientes para medir la dimensión
	2	Bajo nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total
	3	Nivel moderado	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4	Alto nivel	Los ítems son suficientes
CLARIDAD Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta	1	No cumple con el criterio	El ítem no es claro
	2	Bajo nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3	Nivel moderado	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4	Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1	No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
	2	Bajo nivel	El ítem tiene una relación tangencial con la dimensión
	3	Nivel moderado	El ítem tiene una relación moderada con la dimensión que está midiendo
	4	Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1	No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2	Bajo nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste
	3	Nivel moderado	El ítem es relativamente importante
	4	Alto nivel	El ítem es muy relevante y debe ser incluido

Los resultados de esta evaluación, servirá para determinar los coeficientes de validez de contenido del presente cuestionario. De ante mano le agradezco su cooperación.



Apellido y Nombre	SANTISTEBAN AVALOS ELMER IVAN
Código	100032451
Carrera profesional	INGENIERIA DE SISTEMAS DE INFORMACIÓN Y GESTIÓN

Tesis publicada con autorización del autor
No olvide citar esta tesis

Facultad de Ciencias Empresariales

UNIVERSIDAD CIENTÍFICA DEL SUR

ANEXO 18 - A

INFORME DE VALIDEZ DE CONTENIDO Y JUEZ DE EXPERTO

Lima 23 de junio del 2020

Estimado Coordinador de Investigación de la Facultad de Ciencias Empresariales de la Universidad Cientifica del Sur.

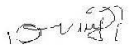
A solicitud del tesista, se procedió a revisar la matriz de consistencia, matriz de operacionalización y el instrumento que empleará para su investigación. Según detalle:

Título de la tesis	MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GESTIÓN DE RIESGOS DE LA FUNDACIÓN PARA EL DESARROLLO SOLIDARIO EN EL 2020.
Grado o título que aspira	Ingeniería de Sistemas
Apellidos y Nombre del (los) tesista (s)	Santisteban Avalos Elmer Ivan

Al respecto y de acuerdo con los indicadores mencionados se califica cada uno de los ítems:

Dimensión 1	Ítems (Pregunta)	Suficiencia	Claridad	Coherencia	Relevancia
Evaluación de riesgo	1. Código del activo	4	4	4	4
	2. Nombre del Activo	4	4	4	4
	3. Confidencialidad	4	4	4	4
	4. Integridad	4	4	4	4
	5. Disponibilidad	4	4	4	4
	6. Amenazas	4	4	4	4
	7. Nivel	4	4	4	4
	8. Vulnerabilidades	4	4	4	4
	9. Nivel	4	4	4	4
	10. Legal	4	4	4	4
	11. Operativo	4	4	4	4
	12. Económico	4	4	4	4

Dimensión 2	Ítems (Pregunta)	Suficiencia	Claridad	Coherencia	Relevancia
Control de riesgo	13. Cláusula	4	4	4	4
	14. Sección	4	4	4	4
	15. Control	4	4	4	4
	16. Estado actual	4	4	4	4
	17. Valoraciones	4	4	4	4
	18. Observaciones	4	4	4	4



Firma del Juez Experto

Apellidos y Nombre del experto	**Gonzales Zuñiga Evelyn**
Especialidad del experto	Ing. De Sistemas
Código de colegiatura	134442
Ficha CTI Vitae (*)	Consignar link https://dina.concytec.gob.pe/appDirectorioCTI/

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

Facultad de Ciencias Empresariales

UNIVERSIDAD CIENTÍFICA DEL SUR

ANEXO 18

FORMATO DE SOLICITUD DE JUICIO DE EXPERTO

Lima 09 de julio del 2020

Señor,
Alexander Abad Madalangoita
Presente. -

De mi consideración,
Siendo conocedor de su trayectoria académica y profesional, me he tomado la libertad de elegirlo como **JUEZ EXPERTO** para revisar el contenido del instrumento que pretendo utilizar para mi investigación. Para ello, adjunto la matriz de consistencia y matriz de operacionalización

A continuación, estos son los criterios de evaluación:

Categoría	Calificación		Indicador
SUFICIENCIA Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta	1	No cumple con el criterio	Los ítems no son suficientes para medir la dimensión
	2	Bajo nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total
	3	Nivel moderado	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4	Alto nivel	Los ítems son suficientes
CLARIDAD Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta	1	No cumple con el criterio	El ítem no es claro
	2	Bajo nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3	Nivel moderado	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4	Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1	No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
	2	Bajo nivel	El ítem tiene una relación tangencial con la dimensión
	3	Nivel moderado	El ítem tiene una relación moderada con la dimensión que está midiendo
	4	Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1	No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2	Bajo nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste
	3	Nivel moderado	El ítem es relativamente importante
	4	Alto nivel	El ítem es muy relevante y debe ser incluido

Los resultados de esta evaluación, servirá para determinar los coeficientes de validez de contenido del presente cuestionario. De ante mano le agradezco su cooperación.

Apellido y Nombre	Elmer Ivan Santisteban Avalos
Código	100032451
Carrera profesional	INGENIERIA DE SISTEMAS DE INFORMACIÓN Y GESTIÓN

Tesis publicada con autorización del autor
No olvide citar esta tesis

Facultad de Ciencias Empresariales

UNIVERSIDAD CIENTÍFICA DEL SUR

ANEXO 18 - A

INFORME DE VALIDEZ DE CONTENIDO Y JUEZ DE EXPERTO

Lima 09 de julio del 2020

Estimado Coordinador de Investigación de la Facultad de Ciencias Empresariales de la Universidad Cientifica del Sur.

A solicitud del tesista, se procedió a revisar la matriz de consistencia, matriz de operacionalización y el instrumento que empleará para su investigación. Según detalle:

Título de la tesis	MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GESTIÓN DE RIESGOS DE LA FUNDACIÓN PARA EL DESARROLLO SOLIDARIO EN EL 2020.
Grado o título que aspira	Ingeniería de Sistemas
Apellidos y Nombre del (los) tesista (s)	Santisteban Avalos Elmer Ivan

Al respecto y de acuerdo con los indicadores mencionados se califica cada uno de los ítems:

Dimensión 1	Ítems (Pregunta)	Suficiencia	Claridad	Coherencia	Relevancia
Evaluación de riesgo	1. Código del activo	4	4	4	4
	2. Nombre del Activo	4	4	4	4
	3. Confidencialidad	4	4	4	4
	4. Integridad	4	4	4	4
	5. Disponibilidad	4	4	4	4
	6. Amenazas	4	4	4	4
	7. Nivel	4	4	4	4
	8. Vulnerabilidades	4	4	4	4
	9. Nivel	4	4	4	4
	10. Legal	4	4	4	4
	11. Operativo	4	4	4	4
	12. Económico	4	4	4	4

Dimensión 2	Ítems (Pregunta)	Suficiencia	Claridad	Coherencia	Relevancia
Control de riesgo	13. Cláusula	4	4	4	4
	14. Sección	4	4	4	4
	15. Control	4	4	4	4
	16. Estado actual	4	4	4	4
	17. Valoración	4	4	4	4
	18. Observaciones	4	4	4	4

ALEXANDER EDUARDO ABAD MADALANGOITA
INGENIERO ELECTRONICO
REG. CIP Nº 228948
Firma del Juez Experto

Apellidos y Nombre del experto	**Abad Madalangoita, Alexander Eduardo**
Especialidad del experto	Ingeniería Electrónica
Código de colegiatura	228948
Ficha CTI Vitae (*)	Título registrado en Sunedu

Tesis publicada con autorización del autor
No olvide citar esta tesis

ANEXO 5: CONSTANCIA EMITIDA POR LA INSTITUCIÓN DONDE SE REALIZÓ LA INVESTIGACIÓN

Facultad de Ciencias Empresariales

UNIVERSIDAD CIENTÍFICA DEL SUR

ANEXO 19

FORMATO DE CONSTANCIA DE CONSENTIMIENTO INFORMADO DE ACCESO PÚBLICO (Empresa)

Por medio de la presente, informamos que la empresa FUNDACIÓN PARA EL DESARROLLO SOLIDARIO autoriza al tesista Elmer Ivan Santisteban Avalos con código de matrícula 100032451 de la carrera profesional de Ingeniería de Sistemas de Información y Gestión de la Universidad Científica del Sur, hacer uso de la información que a continuación se detalla, con el consentimiento de la institución, para el desarrollo de su tesis de grado, la cual lleva por título: MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN EL PROCESO DE GESTIÓN DE RIESGOS DE LA FUNDACIÓN PARA EL DESARROLLO SOLIDARIO EN EL 2020

Información y/o permiso solicitado y a emplear en la tesis:

1. Descripción de la empresa.
2. Descripción de los activos informáticos y su valor.
3. Permiso del lugar de trabajo para realizar las pruebas requeridas.
4. Autorización para consultar y/o capacitar a personal de la empresa.

Dicha información, se recopilará en el Trabajo de Campo para posteriormente ser registrada en su investigación con fines netamente pedagógicos.

Se expide la presente CONSTANCIA DE CONSENTIMIENTO INFORMADO, a solicitud del interesado (a) para los fines que estime conveniente.

Lima, 29 de noviembre de 2019



Firma del Tesista
DNI: 43612489

Firma y sello de la Empresa
Razón Social de la Empresa: FUNDACIÓN PARA EL DESARROLLO SOLIDARIO
RUC: 20162685181
Sitio web: www.fundades.org

Tesis publicada con autorización del autor
No olvide citar esta tesis

ANEXO 6. PROCESO DE GESTIÓN DE RIESGO

Las actividades que se realizaron para aplicar la metodología a fin de mejorar la seguridad de la información, inicia desde evaluar el riesgo tomando como referencia la metodología Magerit y el tratamiento mediante la declaración de aplicabilidad de la ISO 270001 anexo A. También se aplicarán las políticas que ayudarán a un mejor uso, adquisición de los activos y seguridad.

1. Objetivo

- Saber los problemas actuales en seguridad que hay en la institución.
- Averiguar el nivel de riesgo en los activos.
- Implementar las políticas de seguridad.
- Mejorar continuamente.

2. Alcance

Los procedimientos realizados se aplicarán a las actividades y activos de la institución.

3. Organización

La Fundación para el Desarrollo Solidario cuenta con las siguientes áreas:

- Gerencia General
- Administración y Finanzas
- Contabilidad
- Imagen y Comunicaciones
- Sistemas.

4. Metodología de la evaluación de riesgo

Para este proyecto se empleó la metodología Magerit y se aplicó controles como indica la norma ISO 27001. Magerit permite clasificar de manera ordena los activos y darles un valor a cada uno para saber el nivel de importancia que tiene. La ISO 27001 nos permite saber que controles se puede aplicar para tener una mejor seguridad de información, esto abarca a los equipos de cómputo, usuarios, proveedores y toma de decisiones para la gerencia.

Magerit clasifica el proceso de la siguiente manera:

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Inventario de activos
- Amenazas y vulnerabilidades
- Salvaguardas

4.1. Inventario de activos

Se realiza un inventario de activos para conocer qué es lo que se tiene, es decir, cuantos equipos informáticos hay, en qué estado de se encuentran y quienes lo usan. En la institución se verifica que hay un inventario desactualizado y de forma básica, para solucionar esto se actualizará el mismo mediante Magerit que clasifica los activos siguiente manera:

- Activos esenciales
- Servicios
- Software
- Equipos hardware
- Medios de comunicación
- Dispositivos de almacenamiento
- Equipos informáticos adicionales
- Infraestructura
- Usuarios

El inventario de activos está formado así:

- Código del activo (Magerit)
- Código del activo (Institución)
- Nombre del activo
- Descripción
- Ubicación
- Valor

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

ACTIVOS CRÍTICOS									
CÓDIGO (Magerit)	CODIGO	NOMBRE	DESCRIPCIÓN	UBICACIÓN (física o lógica)	CUSTODIO DEL ACTIVO	VALOR DEL ACTIVO			
						C	I	D	V
(essential) Activos esenciales									
(adm)	FU_A_DP	Datos públicos	Data confidencial de la institución.	Sede Barranco	TI	5	5	5	5
(vr)	FU_A_RO	Registros de la organización	Data confidencial de la institución.	Sede Barranco	TI	5	5	5	5
(per)	FU_A_CP	Datos de carácter personal	Data confidencial de la institución.	Sede Barranco	TI	5	5	5	5
(classified)	FU_A_DC	Datos clasificados	Data confidencial de la institución.	Sede Barranco	TI	5	5	5	5
(D) DATOS / INFORMACIÓN				Sede Barranco	TI	5	5	5	5
(backups)	FU_D_CR	Copias de respaldo	Información de equipos de cómputo, servidores, etc.	Sede Barranco	TI	5	5	5	5
(conf)	FU_D_CO	Datos de configuración	Datos críticos para mantener la funcionalidad de las partes del sistema de información.	Sede Barranco	TI	5	5	5	5
(int)	FU_D_GI	Datos de gestión interna	Base de datos del software contable (Concar).	Sede Barranco	TI	5	5	5	5
(password)	FU_D_CR	Credenciales (contraseñas)	Base de datos de contaseñas de correo y equipo administrador.	Sede Barranco	TI	5	5	5	5
(acl)	FU_D_CA	Datos de control de acceso	Información del marcador digital y acceso a carpetas compartidas.	Sede Barranco	TI	5	5	5	5
(S) SERVICIOS				Sede Barranco	TI				
(int)	FU_SR_EX	Usuarios externos	Prestación de servicios externos (asociadas)	Sede Barranco	TI	4	4	4	4
(ext)	FU_SR_IN	Usuarios internos	Usuarios de la propia institución.	Sede Barranco	TI	4	4	4	4
(www)	FU_SR_TR	Internet	Uso de paginas web.	Sede Barranco	TI	3	3	3	3
(telnet)	FU_SR_AR	Acceso remoto	Trabajos remotos de usuarios.	Sede Barranco	TI	2	2	2	2
(email)	FU_SR_CE	Correo electrónico	Correo por aplicación y web.	Sede Barranco	TI	3	3	3	3
(file)	FU_SR_AD	Almacenamiento de datos	Servidor de archivos	Sede Barranco	TI	4	4	4	4
(passw)	FU_SR_CA	Claves de autenticación	Claves de acceso a usuarios internos y externos.	Sede Barranco	TI	4	4	4	4
(ftp)	FU_SR_TR	Transferencia de datos	Conexiones VPN.	Sede Barranco	TI	3	3	3	3
(idm)	FU_SR_GI	Gestión de identidades	Alta y baja a usuarios en el sistema.	Sede Barranco	TI	4	4	4	4
(ipm)	FU_SR_GP	Gestión de privilegios	Acceso a la información.	Sede Barranco	TI	4	4	4	4
(SW) SOFTWARE - APLICACIONES INFORMÁTICAS									
(prp)	FU_SW_CN	Software CONCAR	Software contable para usuarios internos.	Sede Barranco	TI	5	5	5	5
(email -	FU_SW_CE	Cliente de correo electrónico	Correo por la web (office 365).	Sede Barranco	TI	4	4	4	4
(av)	FU_SW_AN	Antivirus	Software de seguridad en las computadoras.	Sede Barranco	TI	4	4	4	4
(os)	FU_SW_SO	Sistema Operativo	Software licenciado para las computadoras.	Sede Barranco	TI	4	4	4	4
(backup)	FU_SW_SB	Sistema de backups	Software para copias de información de las computadoras y servidor	Sede Barranco	TI	5	5	5	5

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

ACTIVOS CRÍTICOS									
CÓDIGO (Magerit)	CODIGO	NOMBRE	DESCRIPCIÓN	UBICACIÓN (física o lógica)	CUSTODIO DEL ACTIVO	VALOR DEL ACTIVO			
						C	I	D	V
(HW) EQUIPAMIENTO INFORMÁTICO (HARDWARE)									
(host)	FU_HW_SV	Servidor	Servidor principal de dominio.	Sede Barranco	TI	5	5	5	5
(pc)	FU_HW_DP	Desktop	Equipos de usuarios finales.	Sede Barranco	TI	4	4	4	4
(lpt)	FU_HW_LP	Laptop	Equipos de usuarios finales.	Sede Barranco	TI	4	4	4	4
(md)	FU_HW_MD	Marcador digital	Marcador de hora de entrada y salida de personal.	Sede Barranco	TI	3	3	3	3
(router - in)	FU_HW_RI	Router de internet	Equipo principal de internet.	Sede Barranco	TI	5	5	5	5
(router -	FU_HW_RT	Router de telefonia	Equipo principal de telefonia.	Sede Barranco	TI	5	5	5	5
(switch)	FU_HW_SI	Switch de datos - Internet	Enlace entre router y puntos de red.	Sede Barranco	TI	5	5	5	5
(switch)	FU_HW_ST	Switch de datos - Telefonia	Enlace entre router y lineas telefónicas.	Sede Barranco	TI	5	5	5	5
(switch)	FU_HW_SD	Switch de datos inalámbrico	Equipo de comuicación entre los access point.	Sede Barranco	TI	5	5	5	5
(fo)	FU_HW_CF	Convertidor a fibra óptica	Enlace entre la central del proveedor y el router.	Sede Barranco	TI	5	5	5	5
(firewall)	FU_HW_FW	Firewall de datos	Equipo de protección.	Sede Barranco	TI	5	5	5	5
(pabx)	FU_HW_CT	Central telefónica	Equipo de comunicación telefónica.	Sede Barranco	TI	5	5	5	5
(ipphone)	FU_HW_TP	Teléfonos IP	Anexos.	Sede Barranco	TI	5	5	5	5
(ap)	FU_HW_AC	Access point 1	AP principal	Sede Barranco	TI	3	3	3	3
(ap)		Access point 2	AP repetidor 1	Sede Barranco	TI	3	3	3	3
(ap)		Access point 3	AP repetidor 2	Sede Barranco	TI	3	3	3	3
(print)	FU_HW_MI	Medios de impresión	Impresoras.	Sede Barranco	TI	2	2	2	2
(svr-backup)	FU_HW_ER	Equipos de respaldo	Servidor de respaldo.	Sede Barranco	TI	5	5	5	5
(COM) REDES DE COMUNICACIÓN									
(internet)	FU_COM_I	Red de internet	Servicio interno (web) y externo (VPN).	Sede Barranco	TI	5	5	5	5
(pstn)	FU_COM_R	Red telefónica	Servicio telefónico.	Sede Barranco	TI	5	5	5	5
(wifi)	FU_COM_RI	Red inalámbirca	Servicio inalámbrico.	Sede Barranco	TI	4	4	4	4
(MEDIA) SOPORTE DE INFORMACIÓN									
(disk)	FU_MEDIA_	Discos externos	Unidades para respaldo de infromación.	Sede Barranco	TI	5	5	5	5
(san)	FU_MEDIA_	Almacenamiento en red	Unidades para respaldo de infromación.	Sede Barranco	TI	5	5	5	5
(printed)	FU_MEDIA_	Material impreso	Almacenaje de información.	Sede Barranco	TI	3	3	3	3
(cd)	FU_MEDIA_	CD-ROM	Almacenaje de información.	Sede Barranco	TI	3	3	3	3

Tesis publicada con autorización del autor
No olvide citar esta tesis

ACTIVOS CRÍTICOS									
CÓDIGO (Magerit)	CODIGO	NOMBRE	DESCRIPCIÓN	UBICACIÓN (física o lógica)	CUSTODIO DEL ACTIVO	VALOR DEL ACTIVO			
						C	I	D	V
(AUX) EQUIPAMIENTO AUXILIAR									
(power)	FU_AU_FA	Fuentes de alimentación	Equipos de soporte.	Sede Barranco	TI	2	2	2	2
(power)	FU_AU_UP	UPS	Equipos de soporte.	Sede Barranco	TI	3	3	3	3
(ac)	FU_AU_EC	Equipos de aclimatación	Equipos de soporte.	Sede Barranco	TI	3	3	3	3
(cabling)	FU_AU_CE	Cableado esttructurado	Equipos de soporte.	Sede Barranco	TI	4	4	4	4
(fiber)	FU_AU_FO	Fibra óptica	Equipos de soporte.	Sede Barranco	TI	4	4	4	4
(furniture)	FU_AU_MB	Mobiliario: armarios, racks.	Equipos de soporte.	Sede Barranco	TI	4	4	4	4
(L) INSTALACIONES									
(building)	FU_L_ED	Edificio	Almacenaje de los sistemas de información y comunicaciones	Sede Barranco	TI	4	4	4	4
(site)	FU_L_OF	Oficina	Almacenaje de los sistemas de información y comunicaciones	Sede Barranco	TI	4	4	4	4
(shelter)	FU_L_AL	Almacén	Almacenaje de los sistemas de información y comunicaciones	Sede Barranco	TI	4	4	4	4
(local)	FU_L_CS	Cuarto de servidor	Almacenaje de los sistemas de información y comunicaciones	Sede Barranco	TI	5	5	5	5
(channel)	FU_L_CN	Canalización	Almacenaje de los sistemas de información y comunicaciones	Sede Barranco	TI	4	4	4	4
(P) PERSONAL									
(ui)	FU_P_UF	Usuarios finales	Personal	Sede Barranco	TI	3	3	3	3
(adm)	FU_P_AS	Administrador de Sistemas	Personal	Sede Barranco	TI	3	3	3	3
(ue)	FU_P_UE	Usuarios externos (Proveedore	Personal	Sede Barranco	TI	4	4	4	4

Para esta investigación se trabajó con 58 activos como principales, obteniendo el valor de cada uno mediante las propiedades de cada activo: la confidencialidad, integridad y disponibilidad.

Tesis publicada con autorización del autor
No olvide citar esta tesis

4.2. Valoración de los activos

Todos los activos de la institución no tienen la misma importancia y en caso surja algún incidente va a generar un impacto distinto, para ello, en este proyecto al valorar los activos se sigue una clasificación de 5 valores determinando que activos tienen un valor más importante que otros y la necesidad de ser protegidos.

ESCALA	VALOR	CRITERIO
Muy alto	5	Afecta irreversiblemente
Alto	4	Impacta gravemente
Medio	3	Impacta considerablemente
Bajo	2	Impacta parcialmente
Muy Bajo	1	No impacta

Esta clasificación se elabora para determinar el impacto que tendrá la amenaza en el activo, como la divulgación no autorizada (confidencialidad), la exactitud y completa información (integridad), la disposición y accesibilidad de la información (disponibilidad). Al establecer el valor de cada activo por su dimensión, se extrae el promedio y el resultado determinará la importancia del activo para la institución.

4.3. Identificación de las amenazas y vulnerabilidades

4.3.1. Identificación de las amenazas

La amenaza causa un efecto dañino en el activo y crear un impacto para la institución. En el inventario de activos realizado, se identifica el valor de los activos según su importancia; El siguiente paso es detectar las amenazas que se encuentran afectando a los activos. La probabilidad de ocurrencia va a indicar la frecuencia con que la amenaza puede atacar, para hallarlo se usa un rango de valores de probabilidad en que puede ocurrir y se muestra en la siguiente tabla:

CLASIFICACIÓN	DESCRIPCIÓN
Muy Alto (5)	Diario
Alto (4)	Una vez por semana
Medio (3)	Una vez al mes
Bajo (2)	Una vez cada 6 meses
Muy Bajo (1)	Una vez cada año

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (AMENAZAS)

ACTIVOS CRÍTICOS				AMENAZAS	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN	PROBABILIDAD DE OCURRENCIA
(essential) ACTIVOS ESENCIALES					
(adm)	FU_A_DP	Datos públicos	Data confidencial de la institución.	Fugas de información	4
				Alteración accidental de la información	4
(vr)	FU_A_RO	Registros de la organización	Data confidencial de la institución.	Fugas de información	4
				Alteración accidental de la información	4
(per)	FU_A_CP	Datos de carácter personal	Data confidencial de la institución.	Fugas de información	4
				Alteración accidental de la información	4
(classified)	FU_A_DC	Datos clasificados	Data confidencial de la institución.	Fugas de información	4
				Alteración accidental de la información	4
(S) SERVICIOS					
(int)	FU_SR_EX	Usuarios externos (asociadas)	Prestación de servicios externos (asociadas)	Alteración accidental de la información	5
(ext)	FU_SR_IN	Usuarios internos	Usuarios de la propia institución.	Alteración accidental de la información	5
(www)	FU_SR_TR	Internet	Uso de paginas web.	Errores de re-encaminamiento	4
				Fugas de información	4
				Errores del administrador	4
(telnet)	FU_SR_AR	Acceso remoto	Trabajos remotos de usuarios.	Errores de configuración	4
(email)	FU_SR_CE	Correo electrónico	Correo por aplicación y web.	Fugas de información	4
(file)	FU_SR_AD	Almacenamiento de datos	Servidor de archivos	Errores del administrador	5
				Errores de monitorización	5
				Errores de configuración	5
(passw)	FU_SR_CA	Claves de autenticación	Claves de acceso a usuarios internos y externos.	Errores del administrador	5
				Errores de los usuarios	5
				Fugas de información	5
(ftp)	FU_SR_TR	Transferencia de datos	Conexiones VPN.	Fugas de información	4
				Errores de re-encaminamiento	4
(idm)	FU_SR_GI	Gestión de identidades	Alta y baja a usuarios en el sistema.	Errores de monitorización	5

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (AMENAZAS)

ACTIVOS CRÍTICOS				AMENAZAS	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN	PROBABILIDAD DE OCURRENCIA
(ipm)	FU_SR_GP	Gestión de privilegios	Acceso a la información.	Errores de configuración	5
				Errores del administrador	5
(SW) SOFTWARE - APLICACIONES INFORMÁTICAS					
(prp)	FU_SW_CN	Software CONCAR	Software contable para usuarios internos.	Errores de los usuarios	5
				Errores del administrador	4
(email - client)	FU_SW_CE	Cliente de correo electrónico	Correo por la web (office 365).	Errores de los usuarios	3
(av)	FU_SW_AN	Antivirus	Software de seguridad en las computadoras.	Errores de mantenimiento / actualización de programas (software)	5
(os)	FU_SW_SO	Sistema Operativo	Software licenciado para las computadoras.	Errores de mantenimiento / actualización de programas (software)	4
(backup)	FU_SW_SB	Sistema de backups	Software para copias de información de las computadoras y servidor	Errores de mantenimiento / actualización de programas (software)	5
				Fugas de información	5
(HW) EQUIPAMIENTO INFORMÁTICO (HARDWARE)					
(host)	FU_HW_SV	Servidor	Servidor principal de dominio.	Denegación de servicio	5
				Errores de mantenimiento / actualización de programas (software)	5
				Pérdida de equipos	5
(pc)	FU_HW_DP	Desktop	Equipos de usuarios finales.	Contaminación mecánica	5
				Errores de mantenimiento / actualización de programas (software)	5
(lpt)	FU_HW_LP	Laptop	Equipos de usuarios finales.	Contaminación mecánica	5
				Errores de mantenimiento / actualización de programas (software)	5
(md)	FU_HW_MD	Marcador digital	Marcador de hora de entrada y salida de personal.	Contaminación mecánica	3
(router - in)	FU_HW_RI	Router de internet	Equipo principal de internet.	Contaminación mecánica	5
				Avería de origen físico o lógico	3
				Manipulación de los equipos	4
(router - telf)	FU_HW_RT	Router de telefonía	Equipo principal de telefonía.	Contaminación mecánica	5
				Avería de origen físico o lógico	3
				Manipulación de los equipos	4
(switch)	FU_HW_SI	Switch de datos - Internet	Enlace entre router y puntos de red.	Contaminación mecánica	5
				Avería de origen físico o lógico	3
				Manipulación de los equipos	4

Tesis publicada con autorización del autor
No olvide citar esta tesis

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (AMENAZAS)

ACTIVOS CRÍTICOS				AMENAZAS	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN	PROBABILIDAD DE OCURRENCIA
(switch)	FU_HW_ST	Switch de datos - Telefonia	Enlace entre router y líneas telefónicas.	Contaminación mecánica	5
				Avería de origen físico o lógico	3
				Manipulación de los equipos	4
(switch)	FU_HW_SD	Switch de datos inalámbrico	Equipo de comuicación entre los access point.	Contaminación mecánica	5
				Avería de origen físico o lógico	3
				Manipulación de los equipos	4
(fo)	FU_HW_CF	Convertidor a fibra óptica	Enlace entre la central del proveedor y el router.	Contaminación mecánica	5
				Manipulación de los equipos	5
(firewall)	FU_HW_FW	Firewall de datos	Equipo de protección.	Contaminación mecánica	5
				Avería de origen físico o lógico	3
				Manipulación de los equipos	4
(pabx)	FU_HW_CT	Central telefónica	Equipo de comunicación telefónica.	Contaminación mecánica	5
				Avería de origen físico o lógico	3
				Manipulación de los equipos	4
(ipphone)	FU_HW_TP	Teléfonos IP	Anexos.	Contaminación mecánica	1
				Avería de origen físico o lógico	2
(ap)	FU_HW_AC	Access point 1	AP principal	Contaminación mecánica	1
				Avería de origen físico o lógico	2
(ap)		Access point 2	AP repetidor 1	Contaminación mecánica	1
				Avería de origen físico o lógico	2
(ap)		Access point 3	AP repetidor 2	Contaminación mecánica	1
				Avería de origen físico o lógico	2
(print)	FU_HW_MI	Medios de impresión	Impresoras.	Contaminación mecánica	1
				Avería de origen físico o lógico	2
(svr-backup)	FU_HW_ER	Equipos de respaldo	Servidor de respaldo.	Errores de monitorización	5
				Errores de mantenimiento / actualización de programas (software)	5
				Errores de configuración	5

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (AMENAZAS)

ACTIVOS CRÍTICOS				AMENAZAS	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN	PROBABILIDAD DE OCURRENCIA
(COM) REDES DE COMUNICACIÓN					
(internet)	FU_COM_IN	Red de internet	Servicio interno (web) y externo (VPN).	Fallo de servicios de comunicaciones	3
(pstn)	FU_COM_RT	Red telefónica	Servicio telefónico.	Fallo de servicios de comunicaciones	3
(wifi)	FU_COM_RI	Red inalámbirca	Servicio inalámbrico.	Fallo de servicios de comunicaciones	3
(MEDIA) SOPORTE DE INFORMACIÓN					
(disk)	FU_MEDIA_DX	Discos externos	Unidades para respaldo de infromación.	Manipulación de los equipos	5
(san)	FU_MEDIA_AR	Almacenamiento en red	Unidades para respaldo de información.	Condiciones inadecuadas de temperatura o humedad	5
				Degradación de los soportes de almacenamiento de la información	5
				Errores de mantenimiento / actualización de equipos (hardware)	5
				Acceso no autorizado.	5
(printed)	FU_MEDIA_MI	Material impreso	Almacenaje de información.	Fugas de información	4
(cd)	FU_MEDIA_CR	CD-ROM	Almacenaje de información.	Fugas de información	4
(AUX) EQUIPAMIENTO AUXILIAR					
(power)	FU_AU_FA	Fuentes de alimentación	Equipos de soporte.	Contaminación mecánica	5
				Avería de origen físico o lógico	5
(power)	FU_AU_UP	UPS	Equipos de soporte.	Contaminación mecánica	3
				Avería de origen físico o lógico	2
(ac)	FU_AU_EC	Equipos de aclimatación	Equipos de soporte.	Contaminación mecánica	3
				Errores de mantenimiento / actualización de equipos (hardware)	3
(cabling)	FU_AU_CE	Cableado estructurado	Equipos de soporte.	Contaminación mecánica	3
(fiber)	FU_AU_FO	Fibra óptica	Equipos de soporte.	Contaminación mecánica	3
(furniture)	FU_AU_MB	Mobiliario: armarios, racks.	Equipos de soporte.	Acceso no autorizado	5
				Manipulación de los equipos	5
				Pérdida de equipos	5
				Contaminación mecánica	5

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (AMENAZAS)

ACTIVOS CRÍTICOS				AMENAZAS	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN	PROBABILIDAD DE OCURRENCIA
(L) INSTALACIONES					
(building)	FU_L_ED	Edificio	Almacenaje de los sistemas de información y comunicaciones	Condiciones inadecuadas de temperatura o humedad	3
				Contaminación mecánica	3
				Uso no previsto	3
(site)	FU_L_OF	Oficina	Almacenaje de los sistemas de información y comunicaciones	Condiciones inadecuadas de temperatura o humedad	3
				Contaminación mecánica	3
				Uso no previsto	4
				Acceso no autorizado	3
(shelter)	FU_L_AL	Almacén	Almacenaje de los sistemas de información y comunicaciones	Condiciones inadecuadas de temperatura o humedad	3
				Contaminación mecánica	3
(local)	FU_L_CS	Cuarto de servidor	Almacenaje de los sistemas de información y comunicaciones	Condiciones inadecuadas de temperatura o humedad	3
				Contaminación mecánica	3
				Uso no previsto	4
				Acceso no autorizado	3
(channel)	FU_L_CN	Canalización	Almacenaje de los sistemas de información y comunicaciones	Contaminación mecánica	3
(P) PERSONAL					
(ui)	FU_P_UF	Usuarios finales	Personal	Ataques de ingenieria social.	4
				Deficiencias en la organización	4
(adm)	FU_P_AS	Administrador de Sistemas	Personal	Errores del administrador	5
(ue)	FU_P_UE	Usuarios externos (Proveedores)	Personal	Deficiencias en la organización	5

Tesis publicada con autorización del autor
No olvide citar esta tesis

4.3.2. Vulnerabilidades

De igual manera, se identifican las vulnerabilidades, en este caso se mencionan los controles ausentes que son base para los ataques de las amenazas en los activos. Se encontraron los siguientes:

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (VULNERABILIDADES)

ACTIVOS CRÍTICOS				VULNERABILIDADES	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	CONTROLES AUSENTES	NIVEL
(essential) ACTIVOS ESENCIALES					
(adm)	FU_A_DP	Datos públicos	Data confidencial de la institución.	Actualización de procedimientos para acceso a la información.	4
					4
(vr)	FU_A_RO	Registros de la organización	Data confidencial de la institución.	Actualización de procedimientos para acceso a la información.	4
					4
(per)	FU_A_CP	Datos de carácter personal	Data confidencial de la institución.	Actualización de procedimientos para acceso a la información.	4
					4
(classified)	FU_A_DC	Datos clasificados	Data confidencial de la institución.	Actualización de procedimientos para acceso a la información.	4
					4
(S) SERVICIOS					
(int)	FU_SR_EX	Usuarios externos (asociadas)	Prestación de servicios externos (asociadas)	Actualización de procedimientos para acceso a la información.	4
(ext)	FU_SR_IN	Usuarios internos	Usuarios de la propia institución.	Actualización de procedimientos para acceso a la información.	4
(www)	FU_SR_TR	Internet	Uso de paginas web.	Control de acceso a pagina web.	5
				Actualización de procedimientos para acceso a la información.	4
				Configuración adecuada del acceso a internet.	5
(telnet)	FU_SR_AR	Acceso remoto	Trabajos remotos de usuarios.	Conocimiento de la forma de acceder remotamente.	5
(email)	FU_SR_CE	Correo electrónico	Correo por aplicación y web.	La información debe ser enviada solo por el correo institucional.	4
(file)	FU_SR_AD	Almacenamiento de datos	Servidor de archivos	Configuración y ordenamiento de los datos.	5
				Monitorización del hardware y software de los activos.	5
				Configuración de acceso a información.	4
(passw)	FU_SR_CA	Claves de autenticación	Claves de acceso a usuarios internos y externos.	Políticas de creación de contraseña	5
				Conocimiento del personal sobre lo vulnerable de las contraseñas.	5
				Configuración de acceso a información.	5
(ftp)	FU_SR_TR	Transferencia de datos	Conexiones VPN.	Actualización de procedimientos para acceso a la información.	5
				Control de acceso a los usuarios.	5
(idm)	FU_SR_GI	Gestión de identidades	Alta y baja a usuarios en el sistema.	Actualización de usuarios que ya no laboran (suspención y/o eliminación).	5
(ipm)	FU_SR_GP	Gestión de privilegios	Acceso a la información.	Usuarios tienen acceso a otras carpetas.	5
				Configuración de acceso a información.	5

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (VULNERABILIDADES)

ACTIVOS CRÍTICOS				VULNERABILIDADES	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	CONTROLES AUSENTES	NIVEL
(SW) SOFTWARE - APLICACIONES INFORMÁTICAS					
(prp)	FU_SW_CN	Software CONCAR	Software contable para usuarios internos.	Realización de backups	4
				Creación de usuarios para cada trabajador.	4
(email - client)	FU_SW_CE	Cliente de correo electrónico	Correo por la web (office 365).	Conocimiento del usuario a enlaces externos o ataques de ingenieria social.	3
(av)	FU_SW_AN	Antivirus	Software de seguridad en las computadoras.	Licencia y fatla de antivirus en computadoras finales y servidor.	5
(os)	FU_SW_SO	Sistema Operativo	Software licenciado para las computadoras.	Licencia y activación del sistema operativo en computadoras.	5
(backup)	FU_SW_SB	Sistema de backups	Software para copias de información de las computadoras y servidor	Programación adecuada de respaldos de la información y sistema.	5
				Actualización de procedimientos para acceso a la información.	5
(HW) EQUIPAMIENTO INFORMÁTICO (HARDWARE)					
(host)	FU_HW_SV	Servidor	Servidor principal de dominio.	Antivirus actualizado y permisos de usuario.	5
				Mantenimiento de servidor.	5
				Seguridad física en el centro de datos.	5
(pc)	FU_HW_DP	Desktop	Equipos de usuarios finales.	Mantenimiento y limpieza de los equipos.	3
				Actualizaciones programadas y antivirus.	4
(lpt)	FU_HW_LP	Laptop	Equipos de usuarios finales.	Mantenimiento y limpieza de los equipos.	3
				Actualizaciones programadas y antivirus.	5
(md)	FU_HW_MD	Marcador digital	Marcador de hora de entrada y salida de personal.	Backups de información.	3
(router - in)	FU_HW_RI	Router de internet	Equipo principal de internet.	Mantenimiento y limpieza de los equipos.	5
				Equipos de respaldo	5
				Seguridad física en el centro de datos.	5
(router - telf)	FU_HW_RT	Router de telefonía	Equipo principal de telefonía.	Mantenimiento y limpieza de los equipos.	5
				Equipos de respaldo	5
				Seguridad física en el centro de datos.	5
(switch)	FU_HW_SI	Switch de datos - Internet	Enlace entre router y puntos de red.	Mantenimiento y limpieza de los equipos.	5
				Equipos de respaldo	5
				Seguridad física en el centro de datos.	5
(switch)	FU_HW_ST	Switch de datos - Telefonía	Enlace entre router y líneas telefónicas.	Mantenimiento y limpieza de los equipos.	5
				Equipos de respaldo	5
				Seguridad física en el centro de datos.	5

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (VULNERABILIDADES)

ACTIVOS CRÍTICOS				VULNERABILIDADES	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	CONTROLES AUSENTES	NIVEL
(switch)	FU_HW_SD	Switch de datos inalámbrico	Equipo de comuicación entre los access point.	Mantenimiento y limpieza de los equipos.	5
				Equipos de respaldo	5
				Seguridad física en el centro de datos.	5
(fo)	FU_HW_CF	Convertidor a fibra óptica	Enlace entre la central del proveedor y el router.	Mantenimiento y limpieza de los equipos.	5
				Seguridad física en el centro de datos.	5
(firewall)	FU_HW_FW	Firewall de datos	Equipo de protección.	Mantenimiento y limpieza de los equipos.	5
				Equipos de respaldo	5
				Seguridad física en el centro de datos.	5
(pabx)	FU_HW_CT	Central telefónica	Equipo de comunicación telefónica.	Mantenimiento y limpieza de los equipos.	5
				Equipos de respaldo	5
				Seguridad física en el centro de datos.	5
(ipphone)	FU_HW_TP	Teléfonos IP	Anexos.	Mantenimiento y limpieza de los equipos.	3
				Equipos de respaldo	3
(ap)	FU_HW_AC	Access point 1	AP principal	Mantenimiento y limpieza de los equipos.	3
				Equipos de respaldo	3
(ap)		Access point 2	AP repetidor 1	Mantenimiento y limpieza de los equipos.	3
				Equipos de respaldo	3
(ap)		Access point 3	AP repetidor 2	Mantenimiento y limpieza de los equipos.	3
				Equipos de respaldo	3
(print)	FU_HW_MI	Medios de impresión	Impresoras.	Mantenimiento y limpieza de los equipos.	3
				Equipos de respaldo	3
(svr-backup)	FU_HW_ER	Equipos de respaldo	Servidor de respaldo.	Monitorización del hardware y software de los activos.	5
				Actualizaciones programadas y antivirus.	5
				Registro de actividades y privilegios de acceso.	5
(COM) REDES DE COMUNICACIÓN					
(internet)	FU_COM_IN	Red de internet	Servicio interno (web) y externo (VPN).	Políticas de restricción de acceso a páginas web no necesarias.	4
(pstn)	FU_COM_RT	Red telefónica	Servicio telefónico.	Políticas de restricción de acceso. (Usuarios nuevos usan anexos de otras áreas).	4
(wifi)	FU_COM_RI	Red inalámbirca	Servicio inalámbrico.	Políticas de restricción de acceso a páginas web no necesarias.	4

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (VULNERABILIDADES)

ACTIVOS CRÍTICOS				VULNERABILIDADES	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	CONTROLES AUSENTES	NIVEL
(MEDIA) SOPORTE DE INFORMACIÓN					
(disk)	FU_MEDIA_DX	Discos externos	Unidades para respaldo de infromación.	Seguridad física en el centro de datos.	5
(san)	FU_MEDIA_AR	Almacenamiento en red	Unidades para respaldo de información.	Seguridad física en el centro de datos.	5
				Desgaste de equipo por el uso.	5
				Mantenimiento físico.	5
				Políticas de acceso al usuario.	5
(printed)	FU_MEDIA_MI	Material impreso	Almacenaje de información.	Etiquetado de información	2
(cd)	FU_MEDIA_CR	CD-ROM	Almacenaje de información.	Etiquetado de información	2
(AUX) EQUIPAMIENTO AUXILIAR					
(power)	FU_AU_FA	Fuentes de alimentación	Equipos de soporte.	Mantenimiento y limpieza de los equipos.	3
				Equipos de respaldo	3
(power)	FU_AU_UP	UPS	Equipos de soporte.	Mantenimiento y limpieza de los equipos.	3
				Equipos de respaldo	3
(ac)	FU_AU_EC	Equipos de aclimatación	Equipos de soporte.	Mantenimiento y limpieza de los equipos.	3
				Equipos de respaldo	3
(cabling)	FU_AU_CE	Cableado estructurado	Equipos de soporte.	Mantenimiento y limpieza del cableado.	4
(fiber)	FU_AU_FO	Fibra óptica	Equipos de soporte.	Mantenimiento y limpieza del cableado.	4
(furniture)	FU_AU_MB	Mobiliario: armarios, racks.	Equipos de soporte.	Seguridad física en el centro de datos.	5
				Seguridad física en el centro de datos.	5
				Seguridad física en el centro de datos.	5
				Mantenimiento y limpieza.	5
(L) INSTALACIONES					
(building)	FU_L_ED	Edificio	Almacenaje de los sistemas de información y comunicaciones	Acondicionamiento apropiado de ventilación.	3
				Mantenimiento y limpieza.	4
				Instalaciones de uso para otras actividades.	5
(site)	FU_L_OF	Oficina	Almacenaje de los sistemas de información y comunicaciones	Cuarto de servidores y equipos sin seguridad.	5
				Mantenimiento y limpieza.	3
				Instalaciones de uso para otras actividades.	5
				Seguridad física en el centro de datos.	5

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (VULNERABILIDADES)

ACTIVOS CRÍTICOS				VULNERABILIDADES	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	CONTROLES AUSENTES	NIVEL
(shelter)	FU_L_AL	Almacén	Almacenaje de los sistemas de información y comunicaciones	Acondicionamiento apropiado de ventilación.	3
				Mantenimiento y limpieza.	3
(local)	FU_L_CS	Cuarto de servidor	Almacenaje de los sistemas de información y comunicaciones	Acondicionamiento apropiado de ventilación.	5
				Mantenimiento y limpieza.	3
				Instalaciones de uso para otras actividades.	5
				Seguridad física en el centro de datos.	5
(channel)	FU_L_CN	Canalización	Almacenaje de los sistemas de información y comunicaciones	Mantenimiento y limpieza.	3
(P) PERSONAL					
(ui)	FU_P_UF	Usuarios finales	Personal	Concientización sobre seguridad y normas de uso.	5
				Conocimientos básicos en caso de algún incidente con los equipos que usa.	5
(adm)	FU_P_AS	Administrador de Sistemas	Personal	Implementación de concientización al usuario en seguridad.	5
(ue)	FU_P_UE	Usuarios externos (Proveedores)	Personal	Evaluación de rendimiento del proveedor en servicio, costo, calidad, etc.	5
					4.32

Tesis publicada con autorización del autor
No olvide citar esta tesis

4.3.3. Identificación del impacto

El impacto es la medida del daño que causa una amenaza sobre un activo. Según el cuadro que se detalla, se asignó el valor a cada amenaza que tiene un impacto en los criterios legal, operativo y económico en la Institución. Finalmente, el impacto será del resultado de la medición de los criterios mencionado. El impacto en cada activo se valoró según el cuadro siguiente:

ESCALA	VALOR	CRITERIO		
		LEGAL	OPERATIVO	ECONÓMICO
Muy grave	5	Compromete irreversiblemente a la Fundación.	Compromete irreversiblemente la operatividad de la Fundación.	Compromete irreversiblemente a la Fundación, sin posibilidad de recuperación económica.
Severo	4	Compromete drásticamente a la Fundación.	Compromete drásticamente la operatividad de la Fundación.	Compromete drásticamente a la Fundación, con recuperación económica a largo plazo.
Medio	3	Compromete seriamente a la Fundación.	Compromete seriamente la operatividad de la Fundación.	Compromete seriamente a la Fundación, con recuperación económica a mediano plazo.
Leve	2	Compromete parcialmente a la Fundación.	Compromete parcialmente la operatividad de la Fundación.	Compromete parcialmente a la Fundación, con recuperación económica a corto plazo.
Sin impacto	1	No compromete a la Fundación.	No compromete la operatividad de la Fundación.	No compromete económicamente a la Fundación, sin pérdida económica.

Tesis publicada con autorización del autor
No olvide citar esta tesis

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (IMPACTO)

ACTIVOS CRÍTICOS				AMENAZAS	EVALUACIÓN DEL RIESGO			
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN	LEGAL	OPERATIVO	ECONÓMICO	IMPACTO
(essential) ACTIVOS ESENCIALES								
(adm)	FU_A_DP	Datos públicos	Data confidencial de la institución.	Fugas de información Alteración accidental de la información	5	5	5	5
(vr)	FU_A_RO	Registros de la organización	Data confidencial de la institución.	Fugas de información Alteración accidental de la información	5	5	5	5
(per)	FU_A_CP	Datos de carácter personal	Data confidencial de la institución.	Fugas de información Alteración accidental de la información	5	5	5	5
(classified)	FU_A_DC	Datos clasificados	Data confidencial de la institución.	Fugas de información Alteración accidental de la información	5	5	5	5
(S) SERVICIOS								
(int)	FU_SR_EX	Usuarios externos (asociadas)	Prestación de servicios externos (asociadas)	Alteración accidental de la información	4	4	4	4
(ext)	FU_SR_IN	Usuarios internos	Usuarios de la propia institución.	Alteración accidental de la información	4	4	4	4
(www)	FU_SR_TR	Internet	Uso de paginas web.	Errores de re-encaminamiento Fugas de información Errores del administrador	2	3	3	3
(telnet)	FU_SR_AR	Acceso remoto	Trabajos remotos de usuarios.	Errores de configuración	3	4	4	4
(email)	FU_SR_CE	Correo electrónico	Correo por aplicación y web.	Fugas de información	4	4	4	4
(file)	FU_SR_AD	Almacenamiento de datos	Servidor de archivos	Errores del administrador Errores de monitorización Errores de configuración	4	4	4	4
(passw)	FU_SR_CA	Claves de autenticación	Claves de acceso a usuarios internos y externos.	Errores del administrador Errores de los usuarios Fugas de información	4	4	4	4
(ftp)	FU_SR_TR	Transferencia de datos	Conexiones VPN.	Fugas de información Errores de re-encaminamiento	4	4	4	4
(idm)	FU_SR_GI	Gestión de identidades	Alta y baja a usuarios en el sistema.	Errores de monitorización	4	4	4	4
(ipm)	FU_SR_GP	Gestión de privilegios	Acceso a la información.	Errores de configuración Errores del administrador	4	4	4	4

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (IMPACTO)

ACTIVOS CRÍTICOS				AMENAZAS	EVALUACIÓN DEL RIESGO			
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN	LEGAL	OPERATIVO	ECONOMICO	IMPACTO
(SW) SOFTWARE - APLICACIONES INFORMÁTICAS								
(prp)	FU_SW_CN	Software CONCAR	Software contable para usuarios internos.	Errores de los usuarios	4	4	4	4
				Errores del administrador	3	3	3	
(email - client)	FU_SW_CE	Cliente de correo electrónico	Correo por la web (office 365).	Errores de los usuarios	3	3	3	3
(av)	FU_SW_AN	Antivirus	Software de seguridad en las computadoras.	Errores de mantenimiento / actualización de programas (software)	3	4	4	4
(os)	FU_SW_SO	Sistema Operativo	Software licenciado para las computadoras.	Errores de mantenimiento / actualización de programas (software)	3	4	4	4
(backup)	FU_SW_SB	Sistema de backups	Software para copias de información de las computadoras y servidor	Errores de mantenimiento / actualización de programas (software)	3	4	4	4
				Fugas de información				
(HW) EQUIPAMIENTO INFORMÁTICO (HARDWARE)								
(host)	FU_HW_SV	Servidor	Servidor principal de dominio.	Denegación de servicio	3	4	4	4
				Errores de mantenimiento / actualización de programas (software)				
				Pérdida de equipos				
(pc)	FU_HW_DP	Desktop	Equipos de usuarios finales.	Contaminación mecánica	3	4	4	4
				Errores de mantenimiento / actualización de programas (software)				
(lpt)	FU_HW_LP	Laptop	Equipos de usuarios finales.	Contaminación mecánica	3	4	4	4
				Errores de mantenimiento / actualización de programas (software)				
(md)	FU_HW_MD	Marcador digital	Marcador de hora de entrada y salida de personal.	Contaminación mecánica	1	2	2	2
(router - in)	FU_HW_RI	Router de internet	Equipo principal de internet.	Contaminación mecánica	4	4	4	4
				Avería de origen físico o lógico				
				Manipulación de los equipos				
(router - telf)	FU_HW_RT	Router de telefonía	Equipo principal de telefonía.	Contaminación mecánica	4	4	4	4
				Avería de origen físico o lógico				
				Manipulación de los equipos				
(switch)	FU_HW_SI	Switch de datos - Internet	Enlace entre router y puntos de red.	Contaminación mecánica	4	4	4	4
				Avería de origen físico o lógico				
				Manipulación de los equipos				

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (IMPACTO)

ACTIVOS CRÍTICOS				AMENAZAS	EVALUACIÓN DEL RIESGO			
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN	LEGAL	OPERATIVO	ECONOMICO	IMPACTO
(switch)	FU_HW_ST	Switch de datos - Telefonía	Enlace entre router y líneas telefónicas.	Contaminación mecánica Avería de origen físico o lógico Manipulación de los equipos	4	4	4	4
(switch)	FU_HW_SD	Switch de datos inalámbrico	Equipo de comuicación entre los access point.	Contaminación mecánica Avería de origen físico o lógico Manipulación de los equipos	4	4	4	4
(fo)	FU_HW_CF	Convertidor a fibra óptica	Enlace entre la central del proveedor y el router.	Contaminación mecánica Manipulación de los equipos	2	3	2	2
(firewall)	FU_HW_FW	Firewall de datos	Equipo de protección.	Contaminación mecánica Avería de origen físico o lógico Manipulación de los equipos	4	4	4	4
(pabx)	FU_HW_CT	Central telefónica	Equipo de comunicación telefónica.	Contaminación mecánica Avería de origen físico o lógico Manipulación de los equipos	4	4	4	4
(ipphone)	FU_HW_TP	Teléfonos IP	Anexos.	Contaminación mecánica Avería de origen físico o lógico	1	3	2	2
(ap)	FU_HW_AC	Access point 1	AP principal	Contaminación mecánica Avería de origen físico o lógico	1	3	2	2
(ap)		Access point 2	AP repetidor 1	Contaminación mecánica Avería de origen físico o lógico	1	3	2	2
(ap)		Access point 3	AP repetidor 2	Contaminación mecánica Avería de origen físico o lógico	1	3	2	2
(print)	FU_HW_MI	Medios de impresión	Impresoras.	Contaminación mecánica Avería de origen físico o lógico	1	3	2	2
(svr-backup)	FU_HW_ER	Equipos de respaldo	Servidor de respaldo.	Errores de monitorización Errores de mantenimiento / actualización de programas (software) Errores de configuración	3	4	4	4

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (IMPACTO)

ACTIVOS CRÍTICOS				AMENAZAS	EVALUACIÓN DEL RIESGO			
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN	LEGAL	OPERATIVO	ECONOMICO	IMPACTO
(COM) REDES DE COMUNICACIÓN								
(internet)	FU_COM_IN	Red de internet	Servicio interno (web) y externo (VPN).	Fallo de servicios de comunicaciones	3	4	4	4
(pstn)	FU_COM_RT	Red telefónica	Servicio telefónico.	Fallo de servicios de comunicaciones	2	4	4	3
(wifi)	FU_COM_RI	Red inalámbirca	Servicio inalámbrico.	Fallo de servicios de comunicaciones	2	2	2	2
(MEDIA) SOPORTE DE INFORMACIÓN								
(disk)	FU_MEDIA_DX	Discos externos	Unidades para respaldo de infromación.	Manipulación de los equipos	2	3	3	3
(san)	FU_MEDIA_AR	Almacenamiento en red	Unidades para respaldo de información.	Condiciones inadecuadas de temperatura o humedad Degradación de los soportes de almacenamiento de la información Errores de mantenimiento / actualización de equipos (hardware) Acceso no autorizado.	2	4	4	4
(printed)	FU_MEDIA_MI	Material impreso	Almacenaje de información.	Fugas de información	4	3	4	4
(cd)	FU_MEDIA_CR	CD-ROM	Almacenaje de información.	Fugas de información	4	3	4	4
(AUX) EQUIPAMIENTO AUXILIAR								
(power)	FU_AU_FA	Fuentes de alimentación	Equipos de soporte.	Contaminación mecánica Avería de origen físico o lógico	1	3	2	2
(power)	FU_AU_UP	UPS	Equipos de soporte.	Contaminación mecánica Avería de origen físico o lógico	1	3	2	2
(ac)	FU_AU_EC	Equipos de aclimatación	Equipos de soporte.	Contaminación mecánica Errores de mantenimiento / actualización de equipos (hardware)	1	4	4	3
(cabling)	FU_AU_CE	Cableado estructurado	Equipos de soporte.	Contaminación mecánica	1	4	3	3
(fiber)	FU_AU_FO	Fibra óptica	Equipos de soporte.	Contaminación mecánica	1	4	3	3
(furniture)	FU_AU_MB	Mobiliario: armarios, racks.	Equipos de soporte.	Acceso no autorizado Manipulación de los equipos Pérdida de equipos Contaminación mecánica	4	5	5	5

Tesis publicada con autorización del autor
No olvide citar esta tesis

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (IMPACTO)

ACTIVOS CRÍTICOS				AMENAZAS	EVALUACIÓN DEL RIESGO			
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN	LEGAL	OPERATIVO	ECONOMICO	IMPACTO
(L) INSTALACIONES								
(building)	FU_L_ED	Edificio	Almacenaje de los sistemas de información y comunicaciones	Condiciones inadecuadas de temperatura o humedad	4	4	4	4
				Contaminación mecánica				
				Uso no previsto				
(site)	FU_L_OF	Oficina	Almacenaje de los sistemas de información y comunicaciones	Condiciones inadecuadas de temperatura o humedad	4	4	4	4
				Contaminación mecánica				
				Uso no previsto				
				Acceso no autorizado				
(shelter)	FU_L_AL	Almacén	Almacenaje de los sistemas de información y comunicaciones	Condiciones inadecuadas de temperatura o humedad	3	3	3	3
				Contaminación mecánica				
(local)	FU_L_CS	Cuarto de servidor	Almacenaje de los sistemas de información y comunicaciones	Condiciones inadecuadas de temperatura o humedad	4	4	4	4
				Contaminación mecánica				
				Uso no previsto				
				Acceso no autorizado				
(channel)	FU_L_CN	Canalización	Almacenaje de los sistemas de información y comunicaciones	Contaminación mecánica	1	2	2	2
(P) PERSONAL								
(ui)	FU_P_UF	Usuarios finales	Personal	Ataques de ingeniería social.	4	4	4	4
				Deficiencias en la organización				
(adm)	FU_P_AS	Administrador de Sistemas	Personal	Errores del administrador	3	4	4	4
(ue)	FU_P_UE	Usuarios externos (Proveedores)	Personal	Deficiencias en la organización	3	3	3	3
							TOTAL	4

Tesis publicada con autorización del autor
No olvide citar esta tesis

4.3.4. Evaluación de riesgo

El valor de riesgo se obtiene del producto de la probabilidad y el nivel de impacto (Riesgo = probabilidad x impacto). El resultado obtenido identifica que activos se priorizan, a través de un cuadro de colores (rojo, anaranjado, amarillo, verde) y así buscar las mejores salvaguardas.

Para obtener el valor de riesgo, se usará una tabla que va a clasificar el nivel de riesgo de cada activo.

ESCALA	RANGO	SIGNIFICANCIA	IDENTIFICACIÓN
Crítico	16-20	No aceptable	
Alto	11-15	No aceptable	
Moderado	5-10	Aceptable / No aceptable	
Bajo	1-4	Aceptable	

Los riesgos que den como resultado un valor entre 1-4 será de una escala bajo, los activos serán tratados con procedimientos de acuerdo a la institución. Los que tengan un valor entre 5-10, serán de escala moderada, asimismo los activos serán tratados con protocolos de seguridad establecidos de la institución. Los riesgos de valor entre 11-15, se consideran de escala Alta, los cuales deberán ser tratados de manera inmediata por la institución, ya que, puede causar daños mayores. Finalmente, los riesgos con un valor entre 16-20 se consideran de escala Muy alta, así como la anterior, se tratarán de manera inmediata ya que son activos críticos de la institución y puede verse afectado gravemente.

Tesis publicada con autorización del autor
No olvide citar esta tesis

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (RIESGO)

ACTIVOS CRÍTICOS				AMENAZAS	PROBABILIDAD DE OCURRENCIA	EVALUACIÓN DEL RIESGO					
										RIESGO	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN		LEGAL	OPERATIVO	ECONOMICO	IMPACTO	VALOR DE EXPOSICIÓN AL RIESGO	NIVEL DE RIESGO
(essential) ACTIVOS ESENCIALES											
(adm)	FU_A_DP	Datos públicos	Data confidencial de la institución.	Fugas de información	4	5	5	5	5	20.00	Crítico
				Alteración accidental de la información	4						
(vr)	FU_A_RO	Registros de la organización	Data confidencial de la institución.	Fugas de información	4	5	5	5	5	20.00	Crítico
				Alteración accidental de la información	4						
(per)	FU_A_CP	Datos de carácter personal	Data confidencial de la institución.	Fugas de información	4	5	5	5	5	20.00	Crítico
				Alteración accidental de la información	4						
(classified)	FU_A_DC	Datos clasificados	Data confidencial de la institución.	Fugas de información	4	5	5	5	5	20.00	Crítico
				Alteración accidental de la información	4						
(S) SERVICIOS											
(int)	FU_SR_EX	Usuarios externos (asociadas)	Prestación de servicios externos (asociadas)	Alteración accidental de la información	5	4	4	4	4	20.00	Crítico
(ext)	FU_SR_IN	Usuarios internos	Usuarios de la propia institución.	Alteración accidental de la información	5	4	4	4	4	20.00	Crítico
(www)	FU_SR_TR	Internet	Uso de paginas web.	Errores de re-encaminamiento	4	2	3	3	3	12.00	Alto
				Fugas de información	4						
				Errores del administrador	4						
(telnet)	FU_SR_AR	Acceso remoto	Trabajos remotos de usuarios.	Errores de configuración	4	3	4	4	4	16.00	Crítico
(email)	FU_SR_CE	Correo electrónico	Correo por aplicación y web.	Fugas de información	4	4	4	4	4	16.00	Crítico
(file)	FU_SR_AD	Almacenamiento de datos	Servidor de archivos	Errores del administrador	5	4	4	4	4	20.00	Crítico
				Errores de monitorización	5						
				Errores de configuración	5						
(passw)	FU_SR_CA	Claves de autenticación	Claves de acceso a usuarios internos y externos.	Errores del administrador	5	4	4	4	4	20.00	Crítico
				Errores de los usuarios	5						
				Fugas de información	5						

Tesis publicada con autorización del autor
No olvide citar esta tesis

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (RIESGO)

ACTIVOS CRÍTICOS				AMENAZAS	PROBABILIDAD DE OCURRENCIA	EVALUACIÓN DEL RIESGO					
										RIESGO	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN		LEGAL	OPERATIVO	ECONOMICO	IMPACTO	VALOR DE EXPOSICIÓN AL RIESGO	NIVEL DE RIESGO
(ftp)	FU_SR_TR	Transferencia de datos	Conexiones VPN.	Fugas de información	4	4	4	4	4	16.00	Crítico
				Errores de re-encaminamiento	4						
(idm)	FU_SR_GI	Gestión de identidades	Alta y baja a usuarios en el sistema.	Errores de monitorización	5	4	4	4	4	20.00	Crítico
(ipm)	FU_SR_GP	Gestión de privilegios	Acceso a la información.	Errores de configuración	5	4	4	4	4	20.00	Crítico
				Errores del administrador	5						
(SW) SOFTWARE - APLICACIONES INFORMÁTICAS											
(prp)	FU_SW_CN	Software CONCAR	Software contable para usuarios internos.	Errores de los usuarios	5	4	4	4	4	18.00	Crítico
				Errores del administrador	4	3	3	3			
(email - client)	FU_SW_CE	Cliente de correo electrónico	Correo por la web (office 365).	Errores de los usuarios	3	3	3	3	3	9.00	Moderado
(av)	FU_SW_AN	Antivirus	Software de seguridad en las computadoras.	Errores de mantenimiento / actualización de programas (software)	5	3	4	4	4	20.00	Crítico
(os)	FU_SW_SO	Sistema Operativo	Software licenciado para las computadoras.	Errores de mantenimiento / actualización de programas (software)	4	3	4	4	4	16.00	Crítico
(backup)	FU_SW_SB	Sistema de backups	Software para copias de información de las computadoras y servidor	Errores de mantenimiento / actualización de programas (software)	5	3	4	4	4	20.00	Crítico
				Fugas de información	5						
(HW) EQUIPAMIENTO INFORMÁTICO (HARDWARE)											
(host)	FU_HW_SV	Servidor	Servidor principal de dominio.	Denegación de servicio	5	3	4	4	4	20.00	Crítico
				Errores de mantenimiento / actualización de programas (software)	5						
				Pérdida de equipos	5						
(pc)	FU_HW_DP	Desktop	Equipos de usuarios finales.	Contaminación mecánica	5	3	4	4	4	20.00	Crítico
				Errores de mantenimiento / actualización de programas (software)	5						
(lpt)	FU_HW_LP	Laptop	Equipos de usuarios finales.	Contaminación mecánica	5	3	4	4	4	20.00	Crítico
				Errores de mantenimiento / actualización de programas (software)	5						
(md)	FU_HW_MD	Marcador digital	Marcador de hora de entrada y salida de personal.	Contaminación mecánica	3	1	2	2	2	6.00	Moderado

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (RIESGO)

ACTIVOS CRÍTICOS				AMENAZAS	PROBABILIDAD DE OCURRENCIA	EVALUACIÓN DEL RIESGO					
										RIESGO	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN		LEGAL	OPERATIVO	ECONOMICO	IMPACTO	VALOR DE EXPOSICIÓN AL RIESGO	NIVEL DE RIESGO
(router - in)	FU_HW_RI	Router de internet	Equipo principal de internet.	Contaminación mecánica	5	4	4	4	4	16.0	Crítico
				Avería de origen físico o lógico	3						
				Manipulación de los equipos	4						
(router - telf)	FU_HW_RT	Router de telefonía	Equipo principal de telefonía.	Contaminación mecánica	5	4	4	4	4	16.0	Crítico
				Avería de origen físico o lógico	3						
				Manipulación de los equipos	4						
(switch)	FU_HW_SI	Switch de datos - Internet	Enlace entre router y puntos de red.	Contaminación mecánica	5	4	4	4	4	16.0	Crítico
				Avería de origen físico o lógico	3						
				Manipulación de los equipos	4						
(switch)	FU_HW_ST	Switch de datos - Telefonía	Enlace entre router y líneas telefónicas.	Contaminación mecánica	5	4	4	4	4	16.0	Crítico
				Avería de origen físico o lógico	3						
				Manipulación de los equipos	4						
(switch)	FU_HW_SD	Switch de datos inalámbrico	Equipo de comuicación entre los access point.	Contaminación mecánica	5	4	4	4	4	16.0	Crítico
				Avería de origen físico o lógico	3						
				Manipulación de los equipos	4						
(fo)	FU_HW_CF	Convertidor a fibra óptica	Enlace entre la central del proveedor y el router.	Contaminación mecánica	5	2	3	2	2	10.0	Moderado
				Manipulación de los equipos	5						
(firewall)	FU_HW_FW	Firewall de datos	Equipo de protección.	Contaminación mecánica	5	4	4	4	4	16.0	Crítico
				Avería de origen físico o lógico	3						
				Manipulación de los equipos	4						
(pabx)	FU_HW_CT	Central telefónica	Equipo de comunicación telefónica.	Contaminación mecánica	5	4	4	4	4	16.0	Crítico
				Avería de origen físico o lógico	3						
				Manipulación de los equipos	4						
(ipphone)	FU_HW_TP	Teléfonos IP	Anexos.	Contaminación mecánica	1	1	3	2	2	4.00	Bajo
				Avería de origen físico o lógico	2						
(ap)	FU_HW_AC	Access point 1	AP principal	Contaminación mecánica	1	1	3	2	2	4.00	Bajo
				Avería de origen físico o lógico	2						
(ap)		Access point 2	AP repetidor 1	Contaminación mecánica	1	1	3	2	2	4.00	Bajo
				Avería de origen físico o lógico	2						
(ap)		Access point 3	AP repetidor 2	Contaminación mecánica	1	1	3	2	2	4.00	Bajo
				Avería de origen físico o lógico	2						

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (RIESGO)

ACTIVOS CRÍTICOS				AMENAZAS	PROBABILIDAD DE OCURRENCIA	EVALUACIÓN DEL RIESGO					
										RIESGO	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN		LEGAL	OPERATIVO	ECONOMICO	IMPACTO	VALOR DE EXPOSICIÓN AL RIESGO	NIVEL DE RIESGO
(print)	FU_HW_MI	Medios de impresión	Impresoras.	Contaminación mecánica	1	1	3	2	2	4.00	Bajo
				Avería de origen físico o lógico	2						
(svr-backup)	FU_HW_ER	Equipos de respaldo	Servidor de respaldo.	Errores de monitorización	5	3	4	4	4	20.00	Crítico
				Errores de mantenimiento / actualización de programas (software)	5						
				Errores de configuración	5						
(COM) REDES DE COMUNICACIÓN											
(internet)	FU_COM_IN	Red de internet	Servicio interno (web) y externo (VPN).	Fallo de servicios de comunicaciones	3	3	4	4	4	12.00	Alto
(pstn)	FU_COM_RT	Red telefónica	Servicio telefónico.	Fallo de servicios de comunicaciones	3	2	4	4	3	9.00	Moderado
(wifi)	FU_COM_RI	Red inalámbirca	Servicio inalámbrico.	Fallo de servicios de comunicaciones	3	2	2	2	2	6.00	Moderado
(MEDIA) SOPORTE DE INFORMACIÓN											
(disk)	FU_MEDIA_DX	Discos externos	Unidades para respaldo de infromación.	Manipulación de los equipos	5	2	3	3	3	15.00	Alto
(san)	FU_MEDIA_AR	Almacenamiento en red	Unidades para respaldo de información.	Condiciones inadecuadas de temperatura o humedad	5	2	4	4	4	20.00	Crítico
				Degradación de los soportes de almacenamiento de la información	5						
				Errores de mantenimiento / actualización de equipos (hardware)	5						
				Acceso no autorizado.	5						
(printed)	FU_MEDIA_MI	Material impreso	Almacenaje de información.	Fugas de información	4	4	3	4	4	16.00	Muy alto
(cd)	FU_MEDIA_CR	CD-ROM	Almacenaje de información.	Fugas de información	4	4	3	4	4	16.00	Muy alto
(AUX) EQUIPAMIENTO AUXILIAR											
(power)	FU_AU_FA	Fuentes de alimentación	Equipos de soporte.	Contaminación mecánica	5	1	3	2	2	10.00	Medio
				Avería de origen físico o lógico	5						
(power)	FU_AU_UP	UPS	Equipos de soporte.	Contaminación mecánica	3	1	3	2	2	6.00	Moderado
				Avería de origen físico o lógico	2						
(ac)	FU_AU_EC	Equipos de aclimatación	Equipos de soporte.	Contaminación mecánica	3	1	4	4	3	9.00	Moderado
				Errores de mantenimiento / actualización de equipos (hardware)	3						
(cabling)	FU_AU_CE	Cableado estructurado	Equipos de soporte.	Contaminación mecánica	2	1	4	3	3	6.00	Moderado
(fiber)	FU_AU_FO	Fibra óptica	Equipos de soporte.	Contaminación mecánica	2	1	4	3	3	6.00	Moderado
(furniture)	FU_AU_MB	Mobiliario: armarios, racks.	Equipos de soporte.	Acceso no autorizado	5	4	5	5	5	25.00	Crítico
				Manipulación de los equipos	5						
				Pérdida de equipos	5						
				Contaminación mecánica	5						

Tesis publicada con autorización del autor
No olvide citar esta tesis

GRUPO FUNDADES
Mejorando vidas

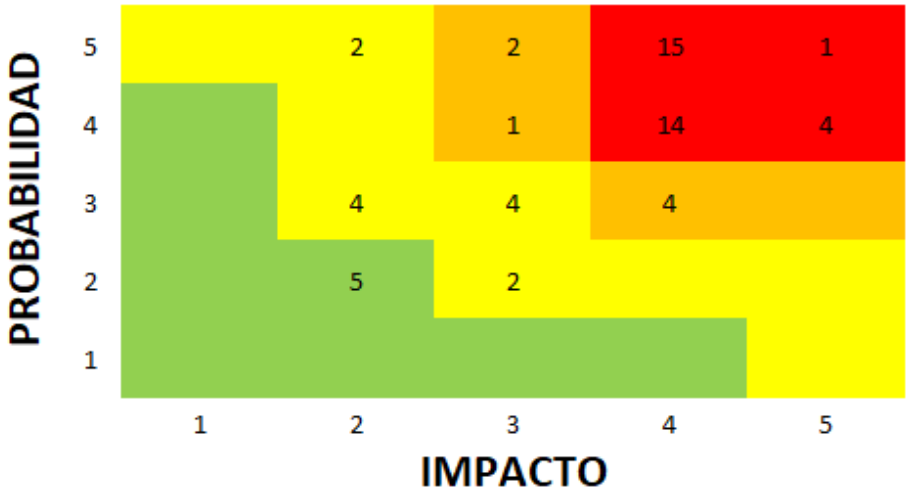
IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (RIESGO)

ACTIVOS CRÍTICOS				AMENAZAS	PROBABILIDAD DE OCURRENCIA	EVALUACIÓN DEL RIESGO					
										RIESGO	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN		LEGAL	OPERATIVO	ECONÓMICO	IMPACTO	VALOR DE EXPOSICIÓN AL RIESGO	NIVEL DE RIESGO
(L) INSTALACIONES											
(building)	FU_L_ED	Edificio	Almacenaje de los sistemas de información y comunicaciones	Condiciones inadecuadas de temperatura o humedad	3	4	4	4	4	12.00	Alto
				Contaminación mecánica	3						
				Uso no previsto	3						
(site)	FU_L_OF	Oficina	Almacenaje de los sistemas de información y comunicaciones	Condiciones inadecuadas de temperatura o humedad	3	4	4	4	4	13.00	Alto
				Contaminación mecánica	3						
				Uso no previsto	4						
				Acceso no autorizado	3						
(shelter)	FU_L_AL	Almacén	Almacenaje de los sistemas de información y comunicaciones	Condiciones inadecuadas de temperatura o humedad	3	3	3	3	3	9.00	Moderado
				Contaminación mecánica	3						
(local)	FU_L_CS	Cuarto de servidor	Almacenaje de los sistemas de información y comunicaciones	Condiciones inadecuadas de temperatura o humedad	3	4	4	4	4	13.00	Alto
				Contaminación mecánica	3						
				Uso no previsto	4						
				Acceso no autorizado	3						
(channel)	FU_L_CN	Canalización	Almacenaje de los sistemas de información y comunicaciones	Contaminación mecánica	3	1	2	2	2	6.00	Moderado
(P) PERSONAL											
(ui)	FU_P_UF	Usuarios finales	Personal	Ataques de ingenieria social.	4	4	4	4	4	16.00	Crítico
				Deficiencias en la organización	4						
(adm)	FU_P_AS	Administrador de Sistemas	Personal	Errores del administrador	5	3	4	4	4	20.00	Crítico
(ue)	FU_P_UE	Usuarios externos (Proveedores)	Personal	Deficiencias en la organización	5	3	3	3	3	15.00	Alto
									Valor de riesgo	**14.33**	

Tesis publicada con autorización del autor
No olvide citar esta tesis

a. Análisis pre test:

El resultado al desarrollar el inventario de activos y verificar el nivel de riesgo (pre test), genera el promedio de 14.19 como riesgo general, escala alta y de significancia no aceptable. La metodología Magerit a través de sus procesos y salvaguardas juntamente con los controles que se implementen nos mostrarán si la seguridad de la información va a influir significativamente en el proceso de gestión de riesgo en la Fundación para el Desarrollo Solidario.



El mapa de calor muestra como resultado que los activos informáticos tienen deficiencias en cuanto a la seguridad. Tal como lo indica la tabla de rango de valores hay 41 activos que se deben poner atención y ver los medios necesarios para minimizar el riesgo o aceptarlas.

4.4. Salvaguardas

En la etapa final se demostrará como la seguridad de la información influye en el tratamiento de riesgo, a través de los resultados obtenidos por el instrumento como son los controles que se aplicaran de acuerdo a la evaluación de riesgo previamente analizado. Se seguirá los siguientes pasos:

- Aplicación de controles para minimizar los riesgos resultantes.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Se desarrollan políticas para mejorar la seguridad que involucra a los activos, usuarios, gerencia y proveedores.
- Establecer los riesgos residuales (post test).

En esta etapa se verifica que la institución no tiene un modelo de seguimiento de controles de seguridad a excepción de unos cuantos como son:

- Retorno de activos.
- Acceso a la red interna.
- Áreas entrega y salida de equipos
- Suministros eléctricos
- Cableado interno
- Seguridad de servicios de red
- Protección de datos personales

Al terminar el inventario de activos, conocer las amenazas, vulnerabilidades, impacto y riesgo, se elegirán que salvaguardas y cuales estrategias se implementarán según lo define la metodología Magerit en el siguiente cuadro:

EFECTO	TIPO
Preventivas: reducen la probabilidad	[PR] prevención
	[DR] disuasión
	[EL] eliminación
Acotan la degradación	[IM] minimización
	[CR] corrección
	[RC] recuperación
Consolidan el efecto de las demás	[MN] de monitorización
	[DC] de detección
	[AW] de concienciación
	[AD] administración

Las estrategias de salvaguardas, el cual está representada por el Activo (código, activo afectado), riesgo (código, nivel, nombre), estrategia (Magerit), vulnerabilidad y controles ISO 27001 (control y código); Este último es el que ayudará a controlar el riesgo que hay en cada activo.

Tesis publicada con autorización del autor
No olvide citar esta tesis

GRUPO FUNDADES
Mejorando vidas

ESTRATÉGIAS DE SALVAGUARAS

CODIGO DEL ACTIVO	ACTIVOS AFECTADOS	RIESGO			ESTRATÉGIA (MAGERIT)	VULNERABILIDAD	ISO 27001	
		CÓDIGO	NIVEL	NOMBRE			CONTROL DE MITIGACIÓN	CONTROL ISO
FU_A_DP	Datos públicos	RA	20.00	Riesgos de acceso	[PR] preventivas	Actualización de procedimientos para acceso a la información	Política de control de acceso	A.9.1.1
FU_A_RO	Registros de la organización	RA	20.00	Riesgos de acceso	[PR] preventivas	Actualización de procedimientos para acceso a la información	Política de control de acceso	A.9.1.2
FU_A_CP	Datos de carácter personal	RA	20.00	Riesgos de acceso	[PR] preventivas	Actualización de procedimientos para acceso a la información	Política de control de acceso	A.9.1.3
FU_A_DC	Datos clasificados	RA	20.00	Riesgos de acceso	[PR] preventivas	Actualización de procedimientos para acceso a la información	Política de control de acceso	A.9.1.3
FU_SR_EX	Usuarios externos	RA	20.00	Riesgos de acceso	[PR] preventivas	Actualización de procedimientos para acceso a la información.	Acceso a redes y servicios de red	A.9.1.2
FU_SR_IN	Usuarios internos	RA	20.00	Riesgos de acceso	[PR] preventivas	Actualización de procedimientos para acceso a la información.	Acceso a redes y servicios de red	A.9.1.2
FU_SR_TR	Internet	RA	12.00	Riesgos de acceso	[MN] monitorización	Control de acceso a pagina web.	Restricción de acceso a la información	A.9.4.1
FU_SR_AR	Acceso remoto	RA	16.00	Riesgos de acceso	[AW] concienciación	Conocimiento de la forma de acceder remotamente.	Teletrabajo	A.6.2.2
FU_SR_CE	Correo electrónico	RA	16.00	Riesgos de acceso	[AW] concienciación	La información debe ser enviada solo por el correo institucional.	Mensajes electrónicos	A.13.2.3
FU_SR_AD	Almacenamiento de datos	RH	20.00	Riesgos de hardware	[CR] corrección	Alta disponibilidad, mantenimiento físico.	Equipos de usuario desatendidos	A.11.2.8
FU_SR_CA	Claves de autenticación	RA	20.00	Riesgos de acceso	[PR] preventivas	Políticas de creación de contraseña	Sistema de gestión de contraseñas	A.9.4.3
FU_SR_TR	Transferencia de datos	RR	16.00	Riesgo de red	[MN] monitorización	Control de acceso al usuario.	Políticas y procedimientos de transferencia de la información	A.13.2.1
FU_SR_GI	Gestión de identidades	RA	20.00	Riesgos de acceso	[EL] eliminación	Actualización de usuarios que ya no laboran (suspención y/o eliminación).	Remoción o ajuste de derechos de acceso	A.9.2.6
FU_SR_GP	Gestión de privilegios	RA	20.00	Riesgos de acceso	[PR] preventivas	Usuarios tienen acceso a otras carpetas.	Gestión de los derechos de acceso asignados a usuarios	A.9.2.2

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

ESTRATÉGIAS DE SALVAGUARAS

CODIGO DEL ACTIVO	ACTIVOS AFECTADOS	RIESGO			ESTRATÉGIA (MAGERIT)	VULNERABILIDAD	ISO 27001	
		CÓDIGO	NIVEL	NOMBRE			CONTROL DE MITIGACIÓN	CONTROL ISO
FU_SW_CN	Software CONCAR	RS	18.00	Riesgos de software	[PR] preventivas	Creación de usuarios para cada trabajador. Procedimientos para el uso adecuado.	Procedimientos de ingreso seguro	A.9.4.2
FU_SW_CE	Cliente de correo electrónico	RS	9.00	Riesgos de software	[AW] concienciación	Conocimiento de los accesos a la web, descarga por mensajes.	Conciencia, educación y capacitación sobre la seguridad de la información	A.7.2.2
FU_SW_AN	Antivirus	RS	20.00	Riesgos de software	[AD] Administración	Antivirus en computadoras finales y servidor y licencias vencidas.	Instalación de software en sistemas operacionales	A.12.5.1
FU_SW_SO	Sistema Operativo	RS	16.00	Riesgos de software	[AD] Administración	Equipos con licencias vencidas, sistemas operativos desactualziados.	Mantenimiento de equipos	A.11.2.4
FU_SW_SB	Sistema de backups	RR	20.00	Riesgo de respaldo	[MN] monitorización	Programación adecuada de respaldos de la información y sistema.	Respaldo de la información	A.12.3.1
FU_HW_SV	Servidor	RH	20.00	Riesgos de hardware	[MN] monitorización	Pruebas semanales, mantenimiento físico y lógico.	Equipos de usuario desatendidos	A.11.2.8
FU_HW_DP	Desktop	RH	20.00	Riesgos de hardware	[MN] monitorización	Pruebas semanales, mantenimiento físico y lógico.	Equipos de usuario desatendidos	A.11.2.8
FU_HW_LP	Laptop	RI	20.00	Riesgos de hardware	[MN] monitorización	Pruebas semanales, mantenimiento físico y lógico.	Equipos de usuario desatendidos	A.11.2.8
FU_HW_MD	Marcador digital	RI	6.00	Riesgo de información	[AD] Administración	Backups de información.	Respaldo de la información	A.12.3.1
FU_HW_RI	Router de internet	RH	16.00	Riesgos de hardware	[EL] eliminación	Seguridad física en el centro de datos.	Emplazamiento y protección de los equipos	A.11.2.1
FU_HW_RT	Router de telefonía	RH	16.00	Riesgos de hardware	[EL] eliminación	Seguridad física en el centro de datos.	Emplazamiento y protección de los equipos	A.11.2.1
FU_HW_SI	Switch de datos - Internet	RH	16.00	Riesgos de hardware	[EL] eliminación	Seguridad física en el centro de datos.	Emplazamiento y protección de los equipos	A.11.2.1
FU_HW_ST	Switch de datos - Telefonía	RH	16.00	Riesgos de hardware	[EL] eliminación	Seguridad física en el centro de datos.	Emplazamiento y protección de los equipos	A.11.2.1

Tesis publicada con autorización del autor
No olvide citar esta tesis

GRUPO FUNDADES
Mejorando vidas

ESTRATÉGIAS DE SALVAGUARAS

CODIGO DEL ACTIVO	ACTIVOS AFECTADOS	RIESGO			ESTRATÉGIA (MAGERIT)	VULNERABILIDAD	ISO 27001	
		CÓDIGO	NIVEL	NOMBRE			CONTROL DE MITIGACIÓN	CONTROL ISO
FU_HW_SD	Switch de datos inalámbrico	RH	16.00	Riesgos de hardware	[EL] eliminación	Seguridad fisica en el centro de datos.	Emplazamiento y protección de los equipos	A.11.2.1
FU_HW_CF	Convertidor a fibra óptica	RH	10.00	Riesgos de hardware	[EL] eliminación	Seguridad fisica en el centro de datos.	Emplazamiento y protección de los equipos	A.11.2.1
FU_HW_FW	Firewall de datos	RH	16.00	Riesgos de hardware	[EL] eliminación	Seguridad fisica en el centro de datos.	Emplazamiento y protección de los equipos	A.11.2.1
FU_HW_CT	Central telefónica	RH	16.00	Riesgos de hardware	[EL] eliminación	Seguridad fisica en el centro de datos.	Emplazamiento y protección de los equipos	A.11.2.1
FU_HW_TP	Teléfonos IP	RH	4.00	Riesgos de hardware	[MN] monitorización	Pruebas, mantenimiento fisico y lógico.	Mantenimiento de equipos	A.11.2.4
FU_HW_AC	Access point 1	RH	4.00	Riesgos de hardware	[MN] monitorización	Pruebas, mantenimiento fisico y lógico.	Mantenimiento de equipos	A.11.2.4
	Access point 2	RH	4.00	Riesgos de hardware	[MN] monitorización	Pruebas, mantenimiento fisico y lógico.	Mantenimiento de equipos	A.11.2.4
	Access point 3	RH	4.00	Riesgos de hardware	[MN] monitorización	Pruebas, mantenimiento fisico y lógico.	Mantenimiento de equipos	A.11.2.4
FU_HW_MI	Medios de impresión	RH	4.00	Riesgos de hardware	[MN] monitorización	Pruebas, mantenimiento fisico y lógico.	Mantenimiento de equipos	A.11.2.4
FU_HW_ER	Equipos de respaldo	RR	20.00	Riesgo de respaldo	[MN] monitorización	Alta disponibilidad	Mantenimiento de equipos	A.11.2.4
FU_COM_IN	Red de internet	RS	12.00	Riesgos de servicio	[EL] eliminación	Políticas de restricción de acceso a páginas web no necesarias.	Restricción de acceso a la información	A.9.4.1
FU_COM_RT	Red telefónica	RS	9.00	Riesgos de servicio	[EL] eliminación	Políticas de restricción de acceso. (Usuarios nuevos usan anexos de otras áreas).	Revisión de derecho de acceso de usuarios	A.9.2.5
FU_COM_RI	Red inalámbirca	RS	6.00	Riesgos de servicio	[EL] eliminación	Políticas de restricción de acceso a páginas web no necesarias.	Restricción de acceso a la información	A.9.4.1
FU_MEDIA_DX	Discos externos	RR	15.00	Riesgo de respaldo	[IM] minimización del impacto	Equipos de respaldo	Retirada o reutilización segura de dispositivos de almacenamiento	A.11.2.7

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

ESTRATÉGIAS DE SALVAGUARAS

CODIGO DEL ACTIVO	ACTIVOS AFECTADOS	RIESGO			ESTRATÉGIA (MAGERIT)	VULNERABILIDAD	ISO 27001	
		CÓDIGO	NIVEL	NOMBRE			CONTROL DE MITIGACIÓN	CONTROL ISO
FU_MEDIA_AR	Almacenamiento en red	RR	20.00	Riesgo de respaldo	[IM] minimización del impacto	Equipos de respaldo	Retirada o reutilización segura de dispositivos de almacenamiento	A.11.2.7
FU_MEDIA_MI	Material impreso	RD	16.00	Riesgo de documentación	[PR] preventivas	Mal manejo del usuario.	Clasificación de la información	A.8.2.2
FU_MEDIA_CR	CD-ROM	RM	16.00	Riesgo de materiales	[PR] preventivas	Mal manejo del usuario.	Clasificación de la información	A.8.2.3
FU_AU_FA	Fuentes de alimentación	RH	10.00	Riesgos de hardware	[MN] monitorización	Pruebas, mantenimiento físico y lógico.	Mantenimiento de equipos	A.11.2.4
FU_AU_UP	UPS	RH	6.00	Riesgos de hardware	[IM] minimización del impacto	Equipos de respaldo	Servicios de suministro	A.11.2.2
FU_AU_EC	Equipos de aclimatación	RH	9.00	Riesgos de hardware	[IM] minimización del impacto	Equipos de respaldo	Protección contra amenazas externas y ambientales	A.11.1.4
FU_AU_CE	Cableado estructurado	RH	6.00	Riesgos de hardware	[MN] monitorización	Pruebas, mantenimiento físico y lógico.	Mantenimiento de equipos	A.11.2.4
FU_AU_FO	Fibra óptica	RH	6.00	Riesgos de hardware	[MN] monitorización	Pruebas, mantenimiento físico y lógico.	Mantenimiento de equipos	A.11.2.4
FU_AU_MB	Mobiliario: armarios, racks.	RF	25.00	Riesgo de infraestructura	[EL] eliminación	Seguridad física en el centro de datos.	Asegurar oficinas, áreas e instalaciones	A.11.1.3
FU_L_ED	Edificio	RF	12.00	Riesgo de infraestructura	[EL] eliminación	Seguridad física en el centro de datos.	Asegurar oficinas, áreas e instalaciones	A.11.1.3
FU_L_OF	Oficina	RF	13.00	Riesgo de infraestructura	[EL] eliminación	Seguridad física en el centro de datos.	Asegurar oficinas, áreas e instalaciones	A.11.1.3
FU_L_AL	Almacén	RF	9.00	Riesgo de infraestructura	[EL] eliminación	Ordenamineto de activo físico	Protección contra amenazas externas y ambientales	A.11.1.4
FU_L_CS	Cuarto de servidor	RF	13.00	Riesgo de infraestructura	[EL] eliminación	Seguridad física, mantenimiento, señalización	Asegurar oficinas, áreas e instalaciones	A.11.1.3
FU_L_CN	Canalización	RH	6.00	Riesgo de infraestructura	[EL] eliminación	Seguridad física, mantenimiento, señalización	Contaminación mecánica	A.11.2.4

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

ESTRATÉGIAS DE SALVAGUARAS

CODIGO DEL ACTIVO	ACTIVOS AFECTADOS	RIESGO			ESTRATÉGIA (MAGERIT)	VULNERABILIDAD	ISO 27001	
		CÓDIGO	NIVEL	NOMBRE			CONTROL DE MITIGACIÓN	CONTROL ISO
FU_P_UF	Usuarios finales	RC	16.00	Riesgo de concientización	[AW] concienciación	Concientización sobre seguridad y normas de uso.	Conciencia, educación y capacitación sobre la seguridad de la información	A.7.2.2
FU_P_AS	Administrador de Sistemas	RC	20.00	Riesgo de concientización	[AD] Administración	Realización de inventario de activos, análisis de riesgo.	Inventario de activos	A.8.1.1
FU_P_UE	Usuarios externos (Proveedores)	RC	15.00	Riesgo de concientización	[AW] concienciación	Requisitos de políticas de seguridad de la información.	Política de seguridad de la información para las relaciones con los proveedores	A.15.1.1

Tesis publicada con autorización del autor
No olvide citar esta tesis

4.5. Análisis de riesgo residual

Al aplicar los controles en los activos con mayor riesgo, además de una madurez en el proceso de gestión de riesgo, la seguridad queda en una situación de riesgo llamada residual.

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (RIESGO)

ACTIVOS CRÍTICOS				AMENAZAS	PROBABILIDAD DE OCURRENCIA	EVALUACIÓN DEL RIESGO					
										RIESGO	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN		LEGAL	OPERATIVO	ECONOMICO	IMPACTO	VALOR DE EXPOSICIÓN AL RIESGO	NIVEL DE RIESGO
(essential) ACTIVOS ESENCIALES											
(adm)	FU_A_DP	Datos públicos	Data confidencial de la institución.	Fugas de información	2	5	5	5	5	10	Moderado
				Alteración accidental de la información	2						
(vr)	FU_A_RO	Registros de la organización	Data confidencial de la institución.	Fugas de información	2	5	5	5	5	10	Moderado
				Alteración accidental de la información	2						
(per)	FU_A_CP	Datos de carácter personal	Data confidencial de la institución.	Fugas de información	2	5	5	5	5	10	Moderado
				Alteración accidental de la información	2						
(classified)	FU_A_DC	Datos clasificados	Data confidencial de la institución.	Fugas de información	2	5	5	5	5	10	Moderado
				Alteración accidental de la información	2						
(S) SERVICIOS											
(int)	FU_SR_EX	Usuarios externos (asociadas)	Prestación de servicios externos (asociadas)	Alteración accidental de la información	2	4	4	4	4	8	Moderado
(ext)	FU_SR_IN	Usuarios internos	Usuarios de la propia institución.	Alteración accidental de la información	2	4	4	4	4	8	Moderado
(www)	FU_SR_TR	Internet	Uso de paginas web.	Errores de re-encaminamiento	3	2	3	3	3.0	9	Moderado
				Fugas de información	3						
				Errores del administrador	3						
(telnet)	FU_SR_AR	Acceso remoto	Trabajos remotos de usuarios.	Errores de configuración	2	3	4	4	4.0	8	Moderado
(email)	FU_SR_CE	Correo electrónico	Correo por aplicación y web.	Fugas de información	2	4	4	4	4	8	Moderado
(file)	FU_SR_AD	Almacenamiento de datos	Servidor de archivos	Errores del administrador	2	4	4	4	4	8	Moderado
				Errores de monitorización	2						
				Errores de configuración	2						
(passw)	FU_SR_CA	Claves de autenticación	Claves de acceso a usuarios internos y externos.	Errores del administrador	2	4	4	4	4	8	Moderado
				Errores de los usuarios	2						
				Fugas de información	2						

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (RIESGO)

ACTIVOS CRÍTICOS				AMENAZAS	PROBABILIDAD DE OCURRENCIA	EVALUACIÓN DEL RIESGO					
										RIESGO	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN		LEGAL	OPERATIVO	ECONÓMICO	IMPACTO	VALOR DE EXPOSICIÓN AL RIESGO	NIVEL DE RIESGO
(essential) ACTIVOS ESENCIALES											
(adm)	FU_A_DP	Datos públicos	Data confidencial de la institución.	Fugas de información	2	5	5	5	5	10	Moderado
				Alteración accidental de la información	2						
(vr)	FU_A_RO	Registros de la organización	Data confidencial de la institución.	Fugas de información	2	5	5	5	5	10	Moderado
				Alteración accidental de la información	2						
(per)	FU_A_CP	Datos de carácter personal	Data confidencial de la institución.	Fugas de información	2	5	5	5	5	10	Moderado
				Alteración accidental de la información	2						
(classified)	FU_A_DC	Datos clasificados	Data confidencial de la institución.	Fugas de información	2	5	5	5	5	10	Moderado
				Alteración accidental de la información	2						
(S) SERVICIOS											
(int)	FU_SR_EX	Usuarios externos (asociadas)	Prestación de servicios externos (asociadas)	Alteración accidental de la información	2	4	4	4	4	8	Moderado
(ext)	FU_SR_IN	Usuarios internos	Usuarios de la propia institución.	Alteración accidental de la información	2	4	4	4	4	8	Moderado
(www)	FU_SR_TR	Internet	Uso de paginas web.	Errores de re-encaminamiento	3	2	3	3	3.0	9	Moderado
				Fugas de información	3						
				Errores del administrador	3						
(telnet)	FU_SR_AR	Acceso remoto	Trabajos remotos de usuarios.	Errores de configuración	2	3	4	4	4.0	8	Moderado
(email)	FU_SR_CE	Correo electrónico	Correo por aplicación y web.	Fugas de información	2	4	4	4	4	8	Moderado
(file)	FU_SR_AD	Almacenamiento de datos	Servidor de archivos	Errores del administrador	2	4	4	4	4	8	Moderado
				Errores de monitorización	2						
				Errores de configuración	2						
(passw)	FU_SR_CA	Claves de autenticación	Claves de acceso a usuarios internos y externos.	Errores del administrador	2	4	4	4	4	8	Moderado
				Errores de los usuarios	2						
				Fugas de información	2						
(ftp)	FU_SR_TR	Transferencia de datos	Conexiones VPN.	Fugas de información	3	4	4	4	4	8	Moderado
				Errores de re-encaminamiento	1						
(idm)	FU_SR_GI	Gestión de identidades	Alta y baja a usuarios en el sistema.	Errores de monitorización	2	4	4	4	4	8	Moderado
(ipm)	FU_SR_GP	Gestión de privilegios	Acceso a la información.	Errores de configuración	2	4	4	4	4	8	Moderado
				Errores del administrador	2						

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (RIESGO)

ACTIVOS CRÍTICOS				AMENAZAS	PROBABILIDAD DE OCURRENCIA	EVALUACIÓN DEL RIESGO					
										RIESGO	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN		LEGAL	OPERATIVO	ECONOMICO	IMPACTO	VALOR DE EXPOSICIÓN AL RIESGO	NIVEL DE RIESGO
(SW) SOFTWARE - APLICACIONES INFORMÁTICAS											
(prp)	FU_SW_CN	Software CONCAR	Software contable para usuarios internos.	Errores de los usuarios	2	4	4	4	4	8	Moderado
				Errores del administrador	2	3	3	3			
(email - client)	FU_SW_CE	Cliente de correo electrónico	Correo por la web (office 365).	Errores de los usuarios	3	3	3	3	3	9	Moderado
(av)	FU_SW_AN	Antivirus	Software de seguridad en las computadoras.	Errores de mantenimiento / actualización de programas (software)	2	3	4	4	4	8	Moderado
(os)	FU_SW_SO	Sistema Operativo	Software licenciado para las computadoras.	Errores de mantenimiento / actualización de programas (software)	2	3	4	4	4	8	Moderado
(backup)	FU_SW_SB	Sistema de backups	Software para copias de información de las computadoras y servidor	Errores de mantenimiento / actualización de programas (software)	2	3	4	4	4	8	Moderado
				Fugas de información	2						
(HW) EQUIPAMIENTO INFORMÁTICO (HARDWARE)											
(host)	FU_HW_SV	Servidor	Servidor principal de dominio.	Denegación de servicio	1	3	4	4	4	8	Moderado
				Errores de mantenimiento / actualización de programas (software)	3						
				Pérdida de equipos	1						
(pc)	FU_HW_DP	Desktop	Equipos de usuarios finales.	Contaminación mecánica	2	3	4	4	4	8	Moderado
				Errores de mantenimiento / actualización de programas (software)	2						
(lpt)	FU_HW_LP	Laptop	Equipos de usuarios finales.	Contaminación mecánica	2	3	4	4	4	8	Moderado
				Errores de mantenimiento / actualización de programas (software)	2						
(md)	FU_HW_MD	Marcador digital	Marcador de hora de entrada y salida de personal.	Contaminación mecánica	3	1	2	2	2.0	6	Moderado
(router - in)	FU_HW_RI	Router de internet	Equipo principal de internet.	Contaminación mecánica	2	4	4	4	4.0	4	Bajo
				Avería de origen físico o lógico	1						
				Manipulación de los equipos	1						
(router - telf)	FU_HW_RT	Router de telefonía	Equipo principal de telefonía.	Contaminación mecánica	2	4	4	4	4.0	4	Bajo
				Avería de origen físico o lógico	1						
				Manipulación de los equipos	1						
(switch)	FU_HW_SI	Switch de datos - Internet	Enlace entre router y puntos de red.	Contaminación mecánica	2	4	4	4	4.0	4	Bajo
				Avería de origen físico o lógico	1						
				Manipulación de los equipos	1						
(switch)	FU_HW_ST	Switch de datos - Telefonía	Enlace entre router y líneas telefónicas.	Contaminación mecánica	2	4	4	4	4.0	4	Bajo
				Avería de origen físico o lógico	1						
				Manipulación de los equipos	1						
(switch)	FU_HW_SD	Switch de datos inalámbrico	Equipo de comuicación entre los access point.	Contaminación mecánica	2	4	4	4	4.0	4	Bajo
				Avería de origen físico o lógico	1						
				Manipulación de los equipos	1						
(fo)	FU_HW_CF	Convertidor a fibra óptica	Enlace entre la central del proveedor y el router.	Contaminación mecánica	2	2	3	2	2.3	4	Bajo
				Manipulación de los equipos	1						
(firewall)	FU_HW_FW	Firewall de datos	Equipo de protección.	Contaminación mecánica	2	4	4	4	4.0	4	Bajo
				Avería de origen físico o lógico	1						
				Manipulación de los equipos	1						

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (RIESGO)

ACTIVOS CRÍTICOS				AMENAZAS	PROBABILIDAD DE OCURRENCIA	EVALUACIÓN DEL RIESGO					
										RIESGO	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN		LEGAL	OPERATIVO	ECONÓMICO	IMPACTO	VALOR DE EXPOSICIÓN AL RIESGO	NIVEL DE RIESGO
(pabx)	FU_HW_CT	Central telefónica	Equipo de comunicación telefónica.	Contaminación mecánica	2	4	4	4	4.0	4	Bajo
				Avería de origen físico o lógico	1						
				Manipulación de los equipos	1						
(ipphone)	FU_HW_TP	Teléfonos IP	Anexos.	Contaminación mecánica	1	1	3	2	2.0	4	Bajo
				Avería de origen físico o lógico	2						
(ap)	FU_HW_AC	Access point 1	AP principal	Contaminación mecánica	1	1	3	2	2.0	4	Bajo
				Avería de origen físico o lógico	2						
(ap)		Access point 2	AP repetidor 1	Contaminación mecánica	1	1	3	2	2.0	4	Bajo
				Avería de origen físico o lógico	2						
(ap)		Access point 3	AP repetidor 2	Contaminación mecánica	1	1	3	2	2.0	4	Bajo
				Avería de origen físico o lógico	2						
(print)	FU_HW_MI	Medios de impresión	Impresoras.	Contaminación mecánica	1	1	3	2	2.0	4	Bajo
				Avería de origen físico o lógico	2						
(svr-backup)	FU_HW_ER	Equipos de respaldo	Servidor de respaldo.	Errores de monitorización	3	3	4	4	4.0	8	Moderado
				Errores de mantenimiento / actualización de programas (software)	2						
				Errores de configuración	1						
(COM) REDES DE COMUNICACIÓN											
(internet)	FU_COM_IN	Red de internet	Servicio interno (web) y externo (VPN).	Fallo de servicios de comunicaciones	2	3	4	4	4.0	8	Moderado
(pstn)	FU_COM_RT	Red telefónica	Servicio telefónico.	Fallo de servicios de comunicaciones	3	2	4	4	3.0	9	Moderado
(wifi)	FU_COM_RI	Red inalámbirca	Servicio inalámbrico.	Fallo de servicios de comunicaciones	3	2	2	2	2.0	6	Moderado
(MEDIA) SOPORTE DE INFORMACIÓN											
(disk)	FU_MEDIA_DX	Discos externos	Unidades para respaldo de infromación.	Manipulación de los equipos	2	2	3	3	3.0	6.0	Moderado
(san)	FU_MEDIA_AR	Almacenamiento en red	Unidades para respaldo de información.	Condiciones inadecuadas de temperatura o humedad	2	2	4	4	4.0	8.0	Moderado
				Degradación de los soportes de almacenamiento de la información	3						
				Errores de mantenimiento / actualización de equipos (hardware)	2						
				Acceso no autorizado.	2						
(printed)	FU_MEDIA_MI	Material impreso	Almacenaje de información.	Fugas de información	3	4	3	4	4.0	12	Alto
(cd)	FU_MEDIA_CR	CD-ROM	Almacenaje de información.	Fugas de información	3	4	3	4	4.0	12	Alto

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

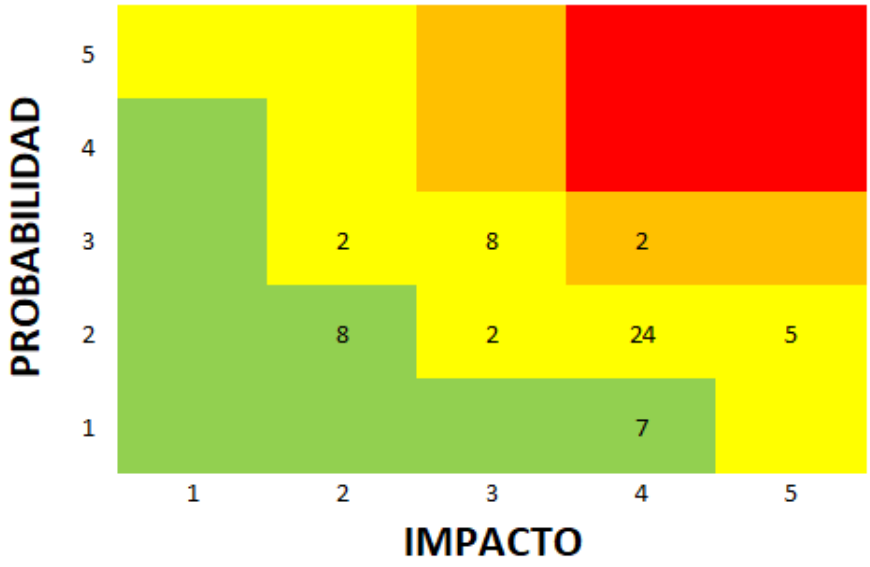
IDENTIFICACIÓN Y ANÁLISIS DE RIESGO (RIESGO)

ACTIVOS CRÍTICOS				AMENAZAS	PROBABILIDAD DE OCURRENCIA	EVALUACIÓN DEL RIESGO					
										RIESGO	
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	DESCRIPCIÓN		LEGAL	OPERATIVO	ECONOMICO	IMPACTO	VALOR DE EXPOSICIÓN AL RIESGO	NIVEL DE RIESGO
(AUX) EQUIPAMIENTO AUXILIAR											
(power)	FU_AU_FA	Fuentes de alimentación	Equipos de soporte.	Contaminación mecánica	2	1	3	2	2.0	4	Bajo
				Avería de origen físico o lógico	2						
(power)	FU_AU_UP	UPS	Equipos de soporte.	Contaminación mecánica	3	1	3	2	2.0	6	Moderado
				Avería de origen físico o lógico	2						
(ac)	FU_AU_EC	Equipos de aclimatación	Equipos de soporte.	Contaminación mecánica	3	1	4	4	3.0	9	Moderado
				Errores de mantenimiento / actualización de equipos (hardware)	3						
(cabling)	FU_AU_CE	Cableado estructurado	Equipos de soporte.	Contaminación mecánica	3	1	4	3	3.0	9	Moderado
(fiber)	FU_AU_FO	Fibra óptica	Equipos de soporte.	Contaminación mecánica	3	1	4	3	3.0	9	Moderado
(furniture)	FU_AU_MB	Mobiliario: armarios, racks.	Equipos de soporte.	Acceso no autorizado	2	4	5	5	5.0	10	Moderado
				Manipulación de los equipos	2						
				Pérdida de equipos	2						
				Contaminación mecánica	2						
(L) INSTALACIONES											
(building)	FU_L_ED	Edificio	Almacenaje de los sistemas de información y comunicaciones	Condiciones inadecuadas de temperatura o humedad	2	4	4	4	4.0	8	Moderado
				Contaminación mecánica	2						
				Uso no previsto	3						
(site)	FU_L_OF	Oficina	Almacenaje de los sistemas de información y comunicaciones	Condiciones inadecuadas de temperatura o humedad	2	4	4	4	4.0	8	Moderado
				Contaminación mecánica	3						
				Uso no previsto	2						
				Acceso no autorizado	2						
(shelter)	FU_L_AL	Almacén	Almacenaje de los sistemas de información y comunicaciones	Condiciones inadecuadas de temperatura o humedad	2	3	3	3	3.0	9	Moderado
				Contaminación mecánica	3						
(local)	FU_L_CS	Cuarto de servidor	Almacenaje de los sistemas de información y comunicaciones	Condiciones inadecuadas de temperatura o humedad	2	4	4	4	4.0	8	Moderado
				Contaminación mecánica	3						
				Uso no previsto	2						
				Acceso no autorizado	2						
(channel)	FU_L_CN	Canalización	Almacenaje de los sistemas de información y	Contaminación mecánica	2	1	2	2	2.0	4	Bajo
(P) PERSONAL											
(ui)	FU_P_UF	Usuarios finales	Personal	Ataques de ingeniería social.	2	4	4	4	4.0	8	Moderado
				Deficiencias en la organización	2						
(adm)	FU_P_AS	Administrador de Sistemas	Personal	Errores del administrador	2	3	4	4	4.0	8	Moderado
(ue)	FU_P_UE	Usuarios externos (Proveedores)	Personal	Deficiencias en la organización	3	3	3	3	3.0	9	Moderado
									Valor de riesgo	**7.28**	

Tesis publicada con autorización del autor
No olvide citar esta tesis

a. Análisis post test:

El resultado del análisis de riesgo en la etapa post test en promedio es de 7.28, escala moderada y de significancia aceptable, ya que, se aplicó el tratamiento mediante las salvaguardas señaladas anteriormente obteniendo un nuevo riesgo llamado "riesgo residual". En la siguiente imagen se muestra cómo queda el mapa de calor con los nuevos resultados:

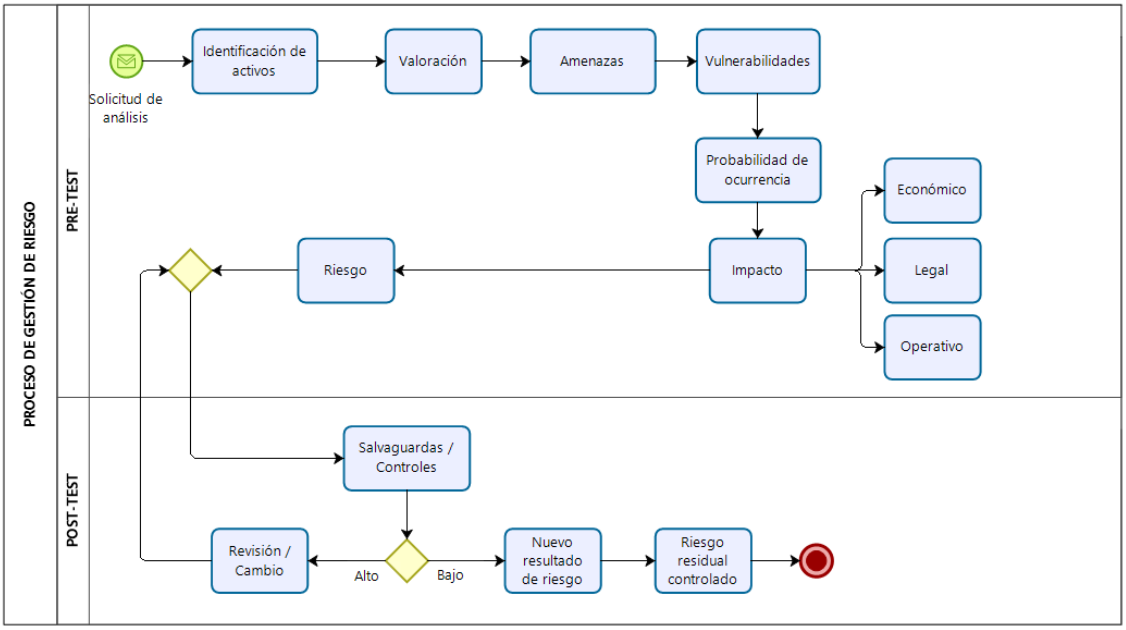


Entonces se puede ver como el riesgo de los activos informáticos mejoró en la seguridad. Los 41 activos que estaban en un rango alto de riesgo (en el pre test) se distribuyeron en zonas de menor riesgo entre alto y moderado, demostrando que las salvaguardas tuvieron un efecto positivo al minimizar el riesgo.

Tesis publicada con autorización del autor
No olvide citar esta tesis

5. Diagrama del proceso de la gestión de riesgo

El diagrama se realiza con BPMN (business Process Modelling Notation), el cual describe el proceso del inicio de la gestión de riesgo desde la etapa pre test, que inicia desde la solicitud de análisis, identificación de activos, valoración, amenazas, vulnerabilidades, probabilidad, impacto y riesgo. En este mismo proceso para la etapa post test se aumentará a lo mencionado anteriormente las salvaguardas / controles, una etapa de revisión y/o cambio si fuese necesario, nuevo resultado de riesgo y finalmente el riesgo residual. Se relacionan mediante una flecha que indica la secuencia del proceso.



Caracterización

La caracterización ayuda a realizar un análisis profundo de este proceso describiendo los elementos que se van a originar de principio a fin, contando con una entrada, actividad, salida, definición y responsables

Tesis publicada con autorización del autor
No olvide citar esta tesis

Caracterización del proceso de Gestión de Riesgo					
	Área Responsable:	Sistemas	Objetivo:	Recopilar, ingresar, recolectar, almacenar y presentar el estado de riesgo de los activos de información.	
	Indicadores:	Fórmula	Periodicidad	Responsable	
	Análisis de riesgo		Mensual	Personal de sistemas.	
	Controles				
	Recursos	PC	Información de activos	Jefes de área	
	ENTRADA	**ACTIVIDAD**	**SALIDA**	**DEFINICIÓN**	**RESPONSABLES**
	Solicitud de análisis	Inicio	Identificación de activos	El proceso inicia con identificar los activos que son necesarios para el trabajo.	Sistemas, jefes de área
	Identificación de activos	Seleccionar los activos necesarios	Valoración	Selección de activos	Sistemas, jefes de área
	Valoración	Escala del 1-5	Amenazas	Actividad donde se valoran los activos de acuerdo a su importancia.	Sistemas, Gerencia
	Amenazas	Identificar que amenazas	-	Actividad en la cual se recopila información de las amenazas que hay en la institución.	Sistemas, jefes de área
	Vulnerabilidades	Identificar las vulnerabilidades	Nivel de vulnerabilidades	Actividad en la cual se recopila información de las vulnerabilidades que hay en los activos.	Sistemas, jefes de área
	Nivel vulnerabilidades	Escala del 1-5	Controles ISO 27001	Se agrega de la escala del 1 – 5 el nivel de vulnerabilidad para cada activo	Sistemas
	Controles ISO 27001	Selección de control	Probabilidad de ocurrencia	Seleccionar los controles adecuados para reducir el nivel de riesgo.	Sistemas

Tesis publicada con autorización del autor
No olvide citar esta tesis

	Probabilidad de ocurrencia	Escala del 1-5	Económico Legal Operativo	La probabilidad de las amenazas de da en una escala del 1-5.	Sistemas
	Económico Legal Operativo	Escala del 1-5	Impacto	El impacto será el resultado del promedio del aspecto económico, legal y operativo en que se verá afectado el activo.	Sistemas
	Impacto	Probabilidad	Riesgo	El riesgo será el resultado del impacto por la probabilidad.	Sistemas
	Riesgo	Escala del 1-20	-	Fin del proceso	Sistemas

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

ANEXO 7: IMPLEMENTACIÓN DE POLÍTICAS DE CONTROL EMPLEANDO ISO 27001

Política de Seguridad de la Información

Fundación para el Desarrollo Solidario

PO- SGSI-27001-2020-001

USO INTERNO

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

Datos del documento

HISTORIA DEL DOCUMENTO			
Nombre del Documento	Política General de Seguridad de la Información		
Preparado por	Elmer Santisteban		
Responsable del Documento	Elmer Santisteban	**Fecha de Creación**	11/08/2020
Aprobado por		**Fecha de Aprobación**	

CONTROL DE VERSIONES			
VERSIÓN	**FECHA**	**DESCRIPCIÓN**	**ELABORADO**
1.0	11/08/2020	Creación y primera versión del documento	E. Santisteban

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

1. INTRODUCCIÓN 1
2. OBJETIVO 1
3. ALCANCE 1
4. RESPONSABILIDADES 1
5. GENERALIDADES 1
   5.1. Políticas de Seguridad de la Información 1
   5.2. Revisión de las Políticas de Seguridad de la Información 2
6. POLITICAS 2

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

1. INTRODUCCIÓN

La Fundación para el Desarrollos Solidario que reconoce el valor y la importancia de la información en el trabajo diario. Por esta razón, se establece las siguientes políticas de control orientadas a definir medidas que resguarden la confidencialidad, integridad y disponibilidad de la información.

2. OBJETIVO

Crear un marco referencial para proteger la información y a los usuarios.

Establecer políticas que infunda conciencia al personal sobre la necesidad y comprensión de la seguridad de la información.

Especificar medidas esenciales de seguridad de la información para protegerse contra amenazas que podrían afectar alguna propiedad del activo en cuanto a su disponibilidad, integridad y disponibilidad.

3. ALCANCE

Estas políticas aplican a todos los colaboradores, proveedores y clientes que la Fundación para el Desarrollo Solidario estime conveniente brindar acceso a la información.

4. RESPONSABILIDADES

Corresponde a la gerencia, responsable del activo, personal, que interactúan habitual u ocasionalmente con los activos de información. Asimismo, serán responsables de informar, publicar, asegurar y cumplir el contenido de las Políticas implementadas.

El incumplimiento de la Política, tendrá como resultado la aplicación de la respectiva sanción dependiendo de la magnitud y característica de lo incumplido.

5. GENERALIDADES

5.1. Políticas de Seguridad de la Información

El presente documento fija las bases que los usuarios, proveedores y terceros de la Fundación para el Desarrollo Solidario deben cumplir para preservar la confidencialidad, disponibilidad e integridad de la información.

Estas políticas deberán estar alineadas a los objetivas de la Institución. Así mismo, deberán ser aprobadas, comunicadas, publicadas, actualizadas y monitoreadas por el equipo asignado a esta tarea.

Deberá ser publicada a todo el personal de la Fundación para el Desarrollo Solidario y proveedores con los que se tienen acuerdos.

Tesis publicada con autorización del autor
No olvide citar esta tesis

5.2. Revisión de las Políticas de Seguridad de la Información

Estas políticas deberán ser revisadas para asegurar que se están aplicando dentro de la institución. Así mismo las políticas se deberán actualizar o agregar por si surgen nuevas medidas.

Estas revisiones serán útiles en los siguientes casos:

- Optimiza los recursos que son asignados a las áreas.
- Mejora los controles y seguridad a la información.
- Tomar mejores decisiones en implementaciones de proyectos.

6. POLITICAS

6.1. Política de teletrabajo

- El acceso a la red de la organización desde ubicaciones remotas, se deberá tener la autorización del Administrador de sistemas.
- El acceso remoto deberá estar disponible solo por canales seguros, igualmente deberán estar seguros por medio de una autenticación entre el cliente y servidor.
- El usuario no tendrá acceso a la información confidencial. Solo se hará excepción a esta regla cuando tenga autorización de un jefe o gerente.
- El personal deberá conectarse a través de equipos seguros de la empresa y no desde ordenadores públicos.

6.2. Respaldo de la información

- Base de datos, aplicaciones, información debe ser respaldados en forma periódica.
  Se debe programar al menos 1 vez al mes una prueba de recuperación de información.
- La información respaldada debe encontrarse en dispositivos físicos o virtuales que no estén dentro de la Institución.

6.3. Inventario de activos

- Deberá ser desarrollado y actualizado por el personal encargado de sistemas.
- Deberá incluir activos esenciales, instalaciones, aplicaciones, etc. que deberán estar codificados, indicando el área o usuario que tiene el activo.
- El inventario deberá ser actualizado cada mes para llevar un control para realizar cambios, dar de baja o adquirir nuevos activos.
- La administración, entrega, devolución, reparación de los activos, así como el acceso a la información mediante políticas a cada usuario, será dado por el personal de sistemas de acuerdo con los requerimientos.
- Mediante procedimientos establecidos por el área de sistemas los usuarios deberán saber las medidas que deben tomaran en caso de algún incidente.

Tesis publicada con autorización del autor
No olvide citar esta tesis

6.4. Capacitación sobre la seguridad de la información

- Planear la capacitación para empleados e interesados, para elevar los niveles de sensibilización frente a la protección de la información.
- Mediante correos electrónicos, afiches, publicaciones se informará sobre los posibles ataques y como evitarlos.

6.5. Perímetro de seguridad física y de acceso

- Fijar perímetros de seguridad y proteger los activos esenciales de comunicación como son servidores, router, switch, etc.
- Así mismo, se debe acondicionar los ambientes de acuerdo a la información que estará almacenada.
- Los ambientes deben estar aptos para que se desarrolle un buen trabajo, tanto el personal como los sistemas, manteniéndolos en buen estado y mejorando en los que se requiera.
- El acceso a los sistemas deberá tener restricciones físicas como control de visitas, cámara de seguridad, etc.

6.6. Aseguramiento de oficinas, área e instalaciones

- La entrada a las instalaciones donde se encuentra los servidores y equipos esenciales de red deberán ser controlados.
- Identificación de personal interno, proveedores y contratistas.
- Asegurar con llave, equipos de videovigilancia, señalizaciones las áreas donde se encuentren los equipos a fin de evitar alguna amenaza.
- Contar con equipos extintores para equipos eléctricos en caso se produjese alguna incidencia de corte o fuego.

6.7. Acceso a áreas de carga y descarga

- Se solicitará las autorizaciones para el ingreso del personal que descargue los productos.
- Se asignará lugares específicos dentro de la institución para recibir los productos adquiridos y donaciones a fin de proteger la información contra terceros.

6.8. Seguridad física y ambiental

- Mantener el cuarto de equipos de red a una temperatura adecuada.
- Mantener limpio los equipos del polvo y otros efectos ambientales para evitar el daño y el periodo de vida de los equipos informáticos.
- Diseñar un cronograma de limpieza.

Tesis publicada con autorización del autor
No olvide citar esta tesis

6.9. Política de control de acceso

- La información almacenada en dispositivos físicos, lógicos y externos deben estar protegidas con un control de acceso basado en contraseñas.
- El acceso a la información debe estar en función a grupos o áreas y no en función a cada usuario salvo excepciones coordinadas con la gerencia.
- El acceso debe estar sujeto a "privilegios", el personal tendrá solo el acceso necesario a fin de cumplir con su trabajo.
- Los usuarios no deberán forzar los privilegios de acceso que se les brinda.
- Si se requiere acceso adicional deberá solicitarlo a su jefe directo y la gerencia y si se aprueba deberán comunicarlo por correo electrónico al área de sistemas.
- Todo personal externo (proveedores, visitas, etc.) que requieran conectarse a la red, deberán pasar por un control del personal de sistemas a fin de eliminar cualquier amenaza.

6.10. Etiquetado de la información

- Emplear un método para clasificar la información. Etiquetas indicando confidencial, uso restringido, no imprimir, etc.
- La información confidencial, crítica deberá ser protegida si es necesario por elementos criptográficos.
- Los documentos deberán tener control de cambios y versiones.
- La información digital deberá tener un control de acceso.
- Deberá ser almacenada de manera ordenada y codificada en equipos y lugares seguros a fin de tener un mejor control y búsqueda en caso se requiera información pasada.

6.11. Sistema de gestión de contraseñas

- Toda información que tenga carácter de confidencial debe estar debidamente protegido por una contraseña.
- La contraseña debe ser personal e intransferible para los diversos accesos (archivos, programas, etc.) que son controlados a nivel de identificación de usuarios.
- La información, los accesos, los sistemas deben crearse con 5 caracteres entre letras mayúsculas, minúsculas y caracteres especiales.
- Deberán ser cambiadas cada cierto tiempo (3 meses o cuando se estime conveniente).
- Las contraseñas no deberán ser reveladas o expuestas en papeles, libretas, etc. a vista de los demás usuarios.
- Al saber de un incidente de seguridad en el equipo, la contraseña se deberá cambiar inmediatamente.

6.12. Políticas y procedimientos de transferencia de la información

- El personal deberá usar el correo institucional para envío y recepción de información referente a su trabajo.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Establecer acuerdos de no divulgación con el personal, clientes y proveedores externos que tengan acceso a la información restringida o confidencial.
- Los dispositivos extraíbles que salgan fuera de oficina deberán ser encriptadas a fin de que la información sea protegida y no está a la vista de personas ajenas.
- Los dispositivos extraíbles deberán ser escaneados por el antivirus antes de su uso a fin de evitar algún incidente que afecte la información.
- Todo equipo que salga de las instalaciones deberá ser debidamente informado y coordinado por el área de sistemas.

6.13. Acceso a redes y servicios de red

- Cualquier acceso remoto que se requiera deberá ser autorizado por la gerencia.
- El acceso y los recursos compartidos deben ser autorizados y controlados por el propietario de los datos y serán otorgados por el área de sistema.
- Al cesar a un usuario, se deberá informar al área de sistemas a fin de realizar los respectivos bloqueos de acceso.
- Se realizará bloqueo de páginas web que no sean de carácter laborar y solo se permitirá el ingreso a estas páginas previa autorización de la gerencia.

6.14. Derechos de acceso a usuarios

- Se debe gestionar que usuarios están autorizados a la información a fin de evitar que personas no autorizadas manipulen o alteren la información.

6.15. Ajuste o remoción de acceso a usuarios

- Se realizará una revisión cada cierto tiempo de los accesos que tienen los usuarios a la información.
- Se debe retirar el acceso al personal, proveedores o terceros a los sistemas y la información al término de su contratación, acuerdo o cambios de áreas.
- Registro y baja de usuarios
- Para acceder, cambiar o remover derechos de acceso a la información, se deberá indicar mediante correo o formato escrito con firma de la persona solicitante, jefe a cargo y la gerencia.
- Igualmente, el área encargada de personal deberá comunicarse con el área de sistemas para el acceso, cambio o remoción del usuario a la información, mediante correo o formato escrito con firma de la persona solicitante, jefe a cargo y la gerencia.

6.16. Mantenimiento de los equipos

- Se realizará un cronograma de mantenimiento anual o cuando se requiera de equipos de red, eléctricos, cableado, etc. Con el fin de garantizar su disponibilidad, integridad y disponibilidad.
- El área de sistemas deberá crear y ejecutar un procedimiento de la forma como le dará el mantenimiento preventivo a los equipos informáticos.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- El personal de sistemas es el único autorizado para brindar el servicio de mantenimiento preventivo y correctivo de la información.
- Si los equipos requieren ser reparados fuera de las instalaciones, deberá ser notificada su salida vía correo electrónico y una guía para su traslado.
- Al finalizar el mantenimiento se deberá realizar un reporte de las tareas realizadas, así como los problemas que se encontró y enviarlas a quien corresponda (asociadas, locales).

6.17. Seguridad del cableado

- El cableado eléctrico y de red deberá mantenerse protegido de factores ambientales.
- Se programará mantenimiento y revisión del cableado.
- Todo cableado nuevo deberá realizarse por personal experto y con material de calidad.

6.18. Salida de los activos fuera de la institución

- La salida de los activos informáticos, así como la información deberá ser autorizada mediante un documento

6.19. Suministro de energía

- Las conexiones eléctricas, paneles, pozo a tierra y estabilizadores deberán ser revisados 1 vez al año o cuando sea conveniente a fin de evitar corto circuito, incendios que dañen los equipos.

6.20. Retiro o reutilización de dispositivos de almacenamiento

- Para eliminar, reutilizar o donar un dispositivo se deberá realizar un borrado total de la información contenida en el soporte.
- Se deberán emplear técnicas como borrado, sobre escritura o destrucción a través de software u herramientas que realicen esta tarea.
- Antes de la entrega de computadoras, laptops, celulares, etc. a otros usuarios de la oficina, se deberá extraer la información y colocarlo en un almacenamiento externo. Así mismo se entregará un cargo de entrega del dispositivo que quedará bajo su responsabilidad.

6.21. Puesto de trabajo y bloqueo de pantalla

- Concientizar e instruir al usuario para no dejar información confidencial a la vista de las personas, dentro de su hora de trabajo o al finalizar.
- Los puestos de trabajo deberán mantenerse libres sin documentación en físico, igualmente el poner las contraseñas de los equipos a la vista.
- Bloquear la pantalla al estar ausente en su puesto de trabajo como buena práctica para que la información no sea vulnerada.

Tesis publicada con autorización del autor
No olvide citar esta tesis

6.22. Gestión de incidentes

- Los incidentes serán reportados al área de sistemas para su revisión y solución.
- Estos deberán ser clasificados en una base de datos a fin solucionar futuros problemas.
- Se deberá llevar un control de incidentes y si son contantes realizar un plan para mitigar, controlar o eliminarlos.

6.23. Instalación de software

- Se utilizará software autorizado y recomendado por el área de sistemas.
- Está prohibido instalar programas que puedan afectar el rendimiento de las computadoras y la red, cualquier instalación requerida deberá ser solicitada al personal de sistemas con la debida autorización de su jefe a cargo.
- La instalación de cualquier software será administrada por el personal de sistemas.
- El personal de sistemas será el responsable de asegurar el licenciamiento de las aplicaciones que se usen en la institución.
- La empresa deberá contar con un servidor de domino que controlará la instalación y acceso de programas que el usuario quiera instalar y puedan ocasionar daños a la estación de trabajo.
- Los equipos serán revisados y probados cada cierto tiempo para buscar software instalado que pueda provocar algún incidente de seguridad.
- Se debe establecer, documentar y mantener los principios de seguridad que se extrae de los análisis para conocer las vulnerabilidad e impacto y lo que se encuentra bien en los activos de información.

6.24. Mensajería electrónica

- El correo institucional solo deberá usarse para envío de información referente a su trabajo.
- Los archivos adjuntos que se envíen por el correo no deberán superar el límite de los 15MB para evitar tráfico y saturación de internet. De ser necesario se empleará plataformas en la nube (onedrive).
- El usuario de la institución deberá tener la instrucción de enviar mensajes por la aplicación del Outlook y por la web si realiza trabajos remotos.
- El administrador de red deberá proporcionar una contraseña segura a cada usuario en la creación de su correo.
- La creación del correo deberá ser solicitada por su jefe inmediato y presentada a la gerencia. Luego será creada por el administrador de sistemas.

6.25. Seguridad de equipos fuera de la oficina

- Los equipos que se requieran para eventos, reuniones, capacitaciones, etc. deberán ser solicitados a su jefe inmediato y a la gerencia. Al ser aprobado el administrador de red deberá realizar un cargo de entrega con firma del responsable y la gerencia.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Se deberá tener los equivalentes cuidados que, en la oficina para propósitos de trabajo, teniendo en cuenta los riesgos externos.

6.26. Políticas con relación a los proveedores

- Se deberán establecer permisos especiales a los proveedores o terceros si requieren acceso a la información, siempre con la autorización de la gerencia y ser creadas por el administrador de sistemas.
- La adquisición de repuestos, equipos, etc. con proveedores deberá seguir un procedimiento como: la solicitud de pedido, la cotización, la confirmación y envió del producto por medios autorizados y envío de la factura.
- Se deberá establecer el lugar de envió de los productos y el proveedor deberá cumplir con los protocolos establecidos en las sedes.
- Se deberá revisar los contratos (SLA) que tiene la institución con los proveedores de servicios, para determinar si cumplen con lo acordado.
- En caso se requiera que el proveedor acceda a la información, red o activos, deberá solicitarlo previamente a la gerencia y al área de sistemas.
- En los acuerdos se deberá establecer las condiciones para plantear los incidentes de seguridad, especificando la tecnología por la cual será transportada la información y como los proveedores accederán a estos.

6.27. Continuidad de la seguridad de la información

- La seguridad de la información deberá ser integrada en la gestión de continuidad del negocio de la organización.
- Se deberá establecer, implementar, documentar y mantener los procesos de continuidad para asegurar la información ante situaciones adversas.
- La institución deberá revisar regularmente estos procesos para garantizar su autenticidad y operatividad ante situaciones adversas.

6.28. Seguridad de la información en la gestión de proyectos

- Los proyectos que se realicen en la institución y dependan de la tecnología se consultará con el personal de sistemas para aportar con recomendaciones.
- Se debe establecer con anticipación las decisiones en los proyectos de incluir al área de sistemas.
- Establecer un presupuesto al área de sistemas para la realización del proyecto y los que habría en un determinado tiempo.

6.29. Dispositivos móviles

- Al personal que se le asigne dispositivos móviles, se le deberá dar un cargo de entrega del equipo y sus accesorios haciéndose responsable del mismo.
- Ante cualquier avería o problema, deberá informar al área de sistemas para realizar los procedimientos que correspondan.
- Solo se deberá tener instaladas aplicaciones validadas, correo electrónico de la empresa y no ser usado para fines personales.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Cuando concluya su contrato laboral o disposición de la gerencia deberá entregar el equipo y sus accesorios a la institución, haciéndole un cargo de entrega.

6.30. Investigación de antecedentes

- Al contratar personal de diferentes áreas, se deberán utilizar las redes sociales como herramientas de búsqueda del perfil del candidato para verificación de antecedentes que ayuden con la elección.

6.31. Condiciones de contratación

- La gerencia deberá establecer puntos que indiquen al personal, proveedores y terceros aceptar términos y condiciones en su contrato en relación a mantener la información que usen confiable, integra y disponible con el fin de no verse expuesta.
- Así mismo los empleados, contratistas y terceros deberán usar los medios y herramientas que se detallen en las políticas o procedimientos internos de la institución.
- Al término de contratación, deberán firmar un cargo de entrega de equipos asignados, contraseñas, trabajos realizados y pendientes a fin de poder asignarle a otro personal.

6.32. Acuerdos de confidencialidad y no divulgación

- Deben ser secretos y tenerlos firmados por escrito antes de usar la información. Abarca al personal de la institución y proveedores con acceso a los activos.
- Los acuerdos deberán cubrir responsabilidades, procedimientos de uso, la duración del acuerdo, el uso permitido, los procesos en caso de incumplimiento, entre otros que estime la institución.

6.33. Proceso disciplinario

- Si se determina que un empleado, contratista o tercero realiza acciones que produzcan brechas de seguridad de información, se le impondrá una sanción que será determinado según el daño ocasionado. Esta sanción la ejecutará las áreas pertinentes.

6.34. Terminación o cambio de puesto de empleo

- Al termino o cambio de responsabilidades del trabajo, se deberá definir el acceso y los privilegios que tenga el usuario a la información considerando la posición o rol que tenga.
- Así mismo, al término de su labor en la institución deberá devolver los equipos asignados para su trabajo mediante un cargo firmado por ambas partes, contemplando el estado de los activos.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Definir las tareas pendientes que tenga hasta el momento del término de su contrato o cambio de puesto.

6.35. Salida de activos fuera de la institución

- Los activos si requieren ser trasladados fuera de la institución, deberán contar con documento de traslado indicando lo que se está llevando, el lugar y la persona que estará a cargo.
- Será de total responsabilidad a la persona que se le entrega y deberá tener los mismos cuidados que se tiene en la oficina.

6.36. Seguridad de los activos y equipos fuera de la institución

- Se le deberá dar las pautas al usuario para que pueda mantener la seguridad de los equipos.
- En caso se trabaje fuera de la oficina, el usuario no deberá usar los equipos para trabajos personales y tendrá que informar de cualquier incidente que pueda ocurrir.

6.37. Gestión de medios removibles

- Servidores y equipos principales que no sea necesario el acceso por USB serán bloqueados para evitar cualquier incidente externo o interno.

6.38. Control de acceso al código fuente del programa

- Programas ERP y base de datos deben estar protegidos en equipos seguros con antivirus y respaldo diario en otros equipos.
- En caso de algún incidente externo o interno, se deberá recurrir a los planes de acción que se harían en esos casos.

6.39. Controles criptográficos

- Los controles criptográficos se usarán para proteger la información, de los sistemas y los servicios.
- Se usará para proteger la transmisión de los mensajes, fuera de la red de la institución.
- Se deberá especificar como se usará, su ciclo de vida y como protegerá las claves criptográficas.

6.40. Procedimiento de operaciones y cambios

- Todo procedimiento operativo, de verificación, instalación y administración de sistemas que se realiza deberá ser documentada a fin de saber qué es lo que se hizo y pudiéndose usar para futuros proyectos.
- Gestión de respaldo de la información el cual deben indicar las pruebas de verificación realizadas.
- Procedimientos de manejo de información.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Procedimiento del monitoreo de red y de los activos.
- Se harán cambios cuando se realice un análisis de riesgo y esté debidamente sustentado.
- Las evaluaciones de cambio deben tener autorización por los representantes de la institución.

6.41. Capacidad de los recursos

- Se debe establecer procedimientos para medir la capacidad de los equipos, programas, red, darles seguimiento y prevenir incidentes.
- Si es necesario se debe optimizar los recursos.

6.42. Control de código malicioso

- Educar a los usuarios a cómo deben actuar cuando se reciba una alarma de detección de código malicioso.
- Establecer procedimientos ante un ataque de código malicioso.
- Realizar planes de acción para ver la efectividad en caso de recuperación de incidentes y la mejora de la continuidad del negocio.
- Los equipos tendrán programada tareas de escaneo periódico, así como realizar backups de la información.

6.43. Registro de eventos

- Se mantendrá eventos mediante un registro de accesos remotos del personal a la red y servidores.
- Los eventos deberán registrarse a fin de monitorear actividades internas y externas, detectar que actividades se realizan y detectar orígenes de fallos de mal funcionamiento para evitar incidentes.
- Los registros deberán tener copias de seguridad para evitar cualquier pérdida.
- No permitir al personal el acceso a los registros para evitar modificaciones o pérdida ante una auditoría.

6.44. Sincronización de relojes

- Debe ser establecido por el servidor de dominio, a fin de que los registros del software tengan una hora en común.

6.45. Controles de auditoría de sistemas de información

- Se debe considerar la información que se realiza en las auditorías internas o externas de los sistemas a fin de mejorar y hacer más seguro los sistemas.
- A través del inventario de activos, el escaneo de registro de actividades, etc. se puede determinar las mejoras que se pueden hacer.

Tesis publicada con autorización del autor
No olvide citar esta tesis

6.46. Controles de la red

- Se deberá gestionar los elementos de una red que se interconectan con el exterior (router, switch, etc.).
- Monitoreo de registros, control de acceso, control de privilegios de manera interna para realizar programas de concientización.
- Acuerdos (SLA) con proveedores de internet y seguridad para el monitoreo externo y la administración de los servicios de red. Determinar sus responsabilidades, mejoras, calidad del servicio, etc. con la institución.
- Las redes en lo posible deben estar segregadas para mantener la separación de equipos e información clasificada de los usuarios dentro de la institución.

6.47. Protección de servicios de aplicación

- Cuando se planifica un proyecto de servicio, se debe tener en cuenta los requisitos de seguridad; Un análisis ayudará a encontrar posibles fallos de seguridad.
- Los servicios que se ofrecen por internet (e-comerse) deben tener controles que garanticen las transacciones.
- Se debe contar con firma digital, validación de autenticación, cifrado de comunicación, protocolos de seguridad.
- Se deben trabajar con proveedores que garanticen lo contratado mediante acuerdos.
- La plataforma donde se desarrolla el sistema, debe ser confiable y con un proveedor que garantice la disponibilidad, confidencialidad e integridad y responda a los cambios requeridos.
- Las pruebas del desarrollo del sistema se deberán llevar con datos no reales y se deberán realizar como sea establecido entre el proveedor y la institución.

6.48. Monitoreo, revisión y cambios en los servicios de los proveedores

- Se controlará los acuerdos con los proveedores, verificando si cumple con lo definido en el contrato y si requiere hacer cambios durante o posterior a su vigencia.
- Todo proveedor que requiera acceso a la información deberá hacerlo desde la oficina con los accesos brindados previa autorización.
- Los proveedores deben cumplir con la confidencialidad de la información que se les dé a través de acuerdos según la tarea y los permisos a realizar.

6.49. Gestionar los incidentes y eventos

- El personal tendrá que observar y reportar cualquier debilidad de seguridad que pueda estar aconteciendo en los sistemas o servicios.
- Se establecerá a los responsables de cada área que comunicará al área de sistemas sobre algún incidente de seguridad que este presentando.
- La comunicación deberá ser por medios digitales (llamada, correo electrónico u otros que operen en el momento).

Tesis publicada con autorización del autor
No olvide citar esta tesis

- El incidente al ser reportado, deberá ser detectado y analizado por el área de sistemas quien a través de un informe evaluará el problema y elaborará el procedimiento para resolverlo.
- Determina si la institución cuenta con los medíos para la solución o transferir el problema con un tercero, el cual tendrá que cumplir con las tareas de reporte y capacitación si se diera el caso.
- Cuando el incidente sea controlado se le brindará la información de como ha sucedido y la capacitación adecuada al usuario para que no pase nuevamente.
- El informe y las capacitaciones se darán de manera virtual y breve estando abiertos a cualquier consulta que requieran.
- Cerrar la incidencia de manera formal cuando sea controlado o resuelto.
- Los incidentes deberán ser almacenados en una bitácora para solucionar futuros problemas que se puedan dar.
- El área de sistemas deberá evaluar los incidentes que reporte donde determinarán otros aspectos más técnicos como el origen, el impacto, la urgencia, entre otros, a través de procedimientos que determinarán la magnitud del problema.
- Los informes se deberán desarrollar de 2 formas: De manera técnica y de manera simple para que sea más sencillo el entendimiento para el personal de otras áreas.
- Los informes finales ayudarán ver cómo está el sistema de seguridad de la información y como se puede mejorar.
- Si se llega a confirmar que el incidente fue por negligencia de un usuario, se pueden requerir acciones posteriores como sanciones o acciones legales. Para ello se tendrá que mostrar las evidencias del caso como indicios, estado de los equipos, documentación, etc.

6.50. Continuidad del negocio

- Se debe establecer procedimientos ante algún desastre o crisis a fin de no detener las operaciones en lo posible.
- Temer un análisis de impacto para determinar que activos pueden requerir protección ante un desastre.
- El trabajo remoto como plan de continuidad se debe emplear en caso no se pueda trabajar en el sitio, con los protocolos de seguridad de información que se dará a cada usuario.
- Para los trabajos remotos, se recomienda que el usuario emplee los equipos de la institución, ya que, cuentan con la protección debida.
- Los equipos principales de comunicación deberán tener una protección adicional de corriente como un UPS, en caso de fallas eléctricas, así como los ambientes adecuados y equipos de redundancia, esto ayudará a que el trabajo no se vea afectado por tiempo y costo.
- Durante la implementación se deberá llevar reportes de las acciones que tomen los usuarios (mediante reportes de su trabajo) o los equipos (mediante registros) para verificar si hubiera incidentes.
- Los usuarios deberán reportar cualquier problema que vean para evitar incidentes mayores.

Tesis publicada con autorización del autor
No olvide citar esta tesis

- Al estar solucionado y controlado el incidente, se debe generar un informe final de como a operado la implementación y determinar si se mantiene como se planificó o habría cambios por hacer.

Tesis publicada con autorización del autor
No olvide citar esta tesis

ANEXO 8: FICHAS DE OBSERVACIÓN

GRUPO FUNDADES
Mejorando vidas

EVALUACIÓN DE RIESGO
FICHA DE OBSERVACIÓN 1 (PRE-TEST)

CÓDIGO:FU-IA-2001-001
VERSIÓN: 1.0
FECHA:
PÁGINA: 1

ACTIVOS										AMENAZAS	VULNERABILIDADES			EVALUACIÓN DEL RIESGO						
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	UBICACIÓN (física o lógica)	CUSTODIO DEL ACTIVO	VALOR DEL ACTIVO				DESCRIPCIÓN	CONTROLES AUSENTES	ANEXO A ISO 27001	NIVEL	PROBABILIDAD DE OCURRENCIA	LEGAL	OPERATIVO	ECONÓMICO	IMPACTO	RIESGO	
						C	I	D	V										VALOR DE RIESGO	NIVEL DE RIESGO
(essential) ACTIVOS ESENCIALES																				
(adm)	FU_A_DP	Datos públicos	Data confidencial de la institución.	Sede Barranco	TI	5	5	5	5	Fugas de información	Actualización de procedimientos para acceso a la información.	-	4	4	5	5	5	5	20.00	Crítico
										Alteración accidental de la información		-	4	4						
(vr)	FU_A_RO	Registros de la organización	Data confidencial de la institución.	Sede Barranco	TI	5	5	5	5	Fugas de información	Actualización de procedimientos para acceso a la información.	-	4	4	5	5	5	5	20.00	Crítico
										Alteración accidental de la información		-	4	4						
(per)	FU_A_CP	Datos de carácter personal	Data confidencial de la institución.	Sede Barranco	TI	5	5	5	5	Fugas de información	Actualización de procedimientos para acceso a la información.	-	4	4	5	5	5	5	20.00	Crítico
										Alteración accidental de la información		-	4	4						
(classified)	FU_A_DC	Datos clasificados	Data confidencial de la institución.	Sede Barranco	TI	5	5	5	5	Fugas de información	Actualización de procedimientos para acceso a la información.	-	4	4	5	5	5	5	20.00	Crítico
										Alteración accidental de la información		-	4	4						
(S) SERVICIOS																				
(int)	FU_SR_EX	Usuarios externos	Prestación de servicios externos (asociadas)	Sede Barranco	TI	4	4	4	4	Alteración accidental de la información	Actualización de procedimientos para acceso a la información.	-	4	5	4	4	4	4	20.00	Crítico
(ext)	FU_SR_IN	Usuarios internos	Usuarios de la propia institución.	Sede Barranco	TI	4	4	4	4	Alteración accidental de la información	Actualización de procedimientos para acceso a la información.	-	4	5	4	4	4	4	20.00	Crítico
(www)	FU_SR_TR	Internet	Uso de paginas web.	Sede Barranco	TI	3	3	3	3	Errores de re-encaminamiento	Control de acceso a pagina web.	-	5	4	2	3	3	3	12.00	Alto
										Escapes de información	Actualización de procedimientos para acceso a la información.	-	4	4						
										Errores del administrador	Configuración adecuada del acceso a internet.	-	5	4						
(telnet)	FU_SR_AR	Acceso remoto	Trabajos remotos de usuarios.	Sede Barranco	TI	2	2	2	2	Errores de configuración	Conocimiento de la forma de acceder remotamente.	-	5	4	3	4	4	4	16.00	Crítico
(email)	FU_SR_CE	Correo electrónico	Correo por aplicación y web.	Sede Barranco	TI	3	3	3	3	Escapes de información	La información debe ser enviada solo por el correo institucional.	-	4	4	4	4	4	4	16.00	Crítico
(file)	FU_SR_AD	Almacenamiento de datos	Servidor de archivos	Sede Barranco	TI	4	4	4	4	Errores del administrador	Configuración y ordenamiento de los datos.	-	5	5	4	4	4	4	20.00	Crítico
										Errores de monitorización	Monitorización del hardware y software de los activos.	-	5	5						
										Errores de configuración	Configuración de acceso a información.	-	4	5						
(passw)	FU_SR_CA	Claves de autenticación	Claves de acceso a usuarios internos y externos	Sede Barranco	TI	4	4	4	4	Errores del administrador	Políticas de creación de contraseña	-	5	5	4	4	4	4	20.00	Crítico
										Errores de los usuarios	Conocimiento del personal sobre lo vulnerable de las contraseñas.	-	5	5						
										Fugas de información	Configuración de acceso a información.	-	5	5						
(ftp)	FU_SR_TR	Transferencia de datos	Conexiones VPN.	Sede Barranco	TI	3	3	3	3	Fugas de información	Actualización de procedimientos para acceso a la información.	-	5	4	4	4	4	4	16.00	Crítico
										Errores de re-encaminamiento	Control de acceso a los usuarios.	-	5	4						
(idm)	FU_SR_GI	Gestión de identidades	Alta y baja a usuarios en el sistema.	Sede Barranco	TI	4	4	4	4	Errores de monitorización	Actualización de usuarios que ya no laboran (suspención y/o eliminació	-	5	5	4	4	4	4	20.00	Crítico
(ipm)	FU_SR_GP	Gestión de privilegios	Acceso a la información.	Sede Barranco	TI	4	4	4	4	Errores de configuración	Usuarios tienen acceso a otras carpetas.	-	5	5	4	4	4	4	20.00	Crítico
										Errores del administrador	Configuración de acceso a información.	-	5	5						
(SW) SOFTWARE - APLICACIONES INFORMÁTICAS																				
(prp)	FU_SW_CN	Software CONCAR	Software contable para usuarios internos.	Sede Barranco	TI	5	5	5	5	Errores de los usuarios	Realización de backups	-	4	5	4	4	4	4	20.00	Crítico
										Errores del administrador	Creación de usuarios para cada trabajador.	-	4	4						
(email -	FU_SW_CE	Cliente de correo electrónico	Correo por la web (office 365).	Sede Barranco	TI	4	4	4	4	Errores de los usuarios	Conocimiento del usuario a enlaces externos o ataques de ingeniería s	-	3	3	3	3	3	3	9.00	Moderado
(av)	FU_SW_AN	Antivirus	Software de seguridad en las computadoras.	Sede Barranco	TI	4	4	4	4	Errores de mantenimiento / actualización de programas (software	Licencia y falta de antivirus en computadoras finales y servidor.	-	5	5	3	4	4	4	20.00	Moderado
(os)	FU_SW_SO	Sistema Operativo	Software licenciado para las computadoras.	Sede Barranco	TI	4	4	4	4	Errores de mantenimiento / actualización de programas (software	Licencia y activación del sistema operativo en computadoras.	-	5	4	3	4	4	4	16.00	Crítico
(backup)	FU_SW_SB	Sistema de backups	Software para copias de información de las com	Sede Barranco	TI	5	5	5	5	Errores de mantenimiento / actualización de programas (software	Programación adecuada de respaldos de la información y sistema.	-	5	5	3	4	4	4	20.00	Crítico
										Fugas de información	Actualización de procedimientos para acceso a la información.	-	5	5						
(HW) EQUIPAMIENTO INFORMÁTICO (HARDWARE)																				
(host)	FU_HW_SV	Servidor	Servidor principal de dominio.	Sede Barranco	TI	5	5	5	5	Denegación de servicio	Antivirus actualizado y permisos de usuario.	-	5	5	3	4	4	4	20.00	Crítico
										Errores de mantenimiento / actualización de programas (software)	Mantenimiento de servidor.	-	5	5						
										Pérdida de equipos	Seguridad física en el centro de datos.	-	5	5						
(pc)	FU_HW_DP	Desktop	Equipos de usuarios finales.	Sede Barranco	TI	4	4	4	4	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	3	5	3	4	4	4	20.00	Crítico
										Errores de mantenimiento / actualización de programas (software)	Actualizaciones programadas y antivirus.	-	4	5						

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

EVALUACIÓN DE RIESGO
FICHA DE OBSERVACIÓN 1 (PRE-TEST)

CÓDIGO:FU-IA-2001-001
VERSIÓN: 1.0
FECHA:
PÁGINA: 1

ACTIVOS										AMENAZAS	VULNERABILIDADES			EVALUACIÓN DEL RIESGO						
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	UBICACIÓN (física o lógica)	CUSTODIO DEL ACTIVO	VALOR DEL ACTIVO				DESCRIPCIÓN	CONTROLES AUSENTES	ANEXO A ISO 27001	NIVEL	PROBABILIDAD DE OCURRENCIA	LEGAL	OPERATIVO	ECONÓMICO	IMPACTO	RIESGO	
						C	I	D	V										VALOR DE RIESGO	NIVEL DE RIESGO
(lpt)	FU_HW_LP	Laptop	Equipos de usuarios finales.	Sede Barranco	TI	4	4	4	4	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	3	5	3	4	4	4	20.00	Crítico
										Errores de mantenimiento / actualización de programas (software)	Actualizaciones programadas y antivirus.	-	5	5						
(md)	FU_HW_MD	Marcador digital	Marcador de hora de entrada y salida de personal	Sede Barranco	TI	3	3	3	3	Contaminación mecánica	Backups de información.	-	3	3	1	2	2	2	6.00	Moderado
(router - in)	FU_HW_RI	Router de internet	Equipo principal de internet.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	5	5	4	4	4	4	16.00	Crítico
										Avería de origen físico o lógico	Equipos de respaldo	-	5	3						
										Manipulación de los equipos	Seguridad física en el centro de datos.	-	5	4						
(router - telf)	FU_HW_RT	Router de telefonía	Equipo principal de telefonía.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	5	5	4	4	4	4	16.00	Crítico
										Avería de origen físico o lógico	Equipos de respaldo	-	5	3						
										Manipulación de los equipos	Seguridad física en el centro de datos.	-	5	4						
(switch)	FU_HW_SI	Switch de datos - Internet	Enlace entre router y puntos de red.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	5	5	4	4	4	4	16.00	Crítico
										Avería de origen físico o lógico	Equipos de respaldo	-	5	3						
										Manipulación de los equipos	Seguridad física en el centro de datos.	-	5	4						
(switch)	FU_HW_ST	Switch de datos - Telefonía	Enlace entre router y líneas telefónicas.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	5	5	4	4	4	4	16.00	Crítico
										Avería de origen físico o lógico	Equipos de respaldo	-	5	3						
										Manipulación de los equipos	Seguridad física en el centro de datos.	-	5	4						
(switch)	FU_HW_SD	Switch de datos inalámbrico	Equipo de comuicación entre los access point.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	5	5	4	4	4	4	16.00	Crítico
										Avería de origen físico o lógico	Equipos de respaldo	-	5	3						
										Manipulación de los equipos	Seguridad física en el centro de datos.	-	5	4						
(fo)	FU_HW_CF	Convertidor a fibra óptica	Enlace entre la central del proveedor y el router.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	5	5	2	3	2	2	10.00	Moderado
										Manipulación de los equipos	Seguridad física en el centro de datos.	-	5	5						
(firewall)	FU_HW_FW	Firewall de datos	Equipo de protección.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	5	5	4	4	4	4	16.00	Crítico
										Avería de origen físico o lógico	Equipos de respaldo	-	5	3						
										Manipulación de los equipos	Seguridad física en el centro de datos.	-	5	4						
(pabx)	FU_HW_CT	Central telefónica	Equipo de comunicación telefónica.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	5	5	4	4	4	4	16.00	Crítico
										Avería de origen físico o lógico	Equipos de respaldo	-	5	3						
										Manipulación de los equipos	Seguridad física en el centro de datos.	-	5	4						
(ipphone)	FU_HW_TP	Teléfonos IP	Anexos.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	3	1	1	3	2	2	4.00	Bajo
										Avería de origen físico o lógico	Equipos de respaldo	-	3	2						
(ap)	FU_HW_AC	Access point 1	AP principal	Sede Barranco	TI	3	3	3	3	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	3	1	1	3	2	2	4.00	Bajo
										Avería de origen físico o lógico	Equipos de respaldo	-	3	2						
(ap)		Access point 2	AP repetidor 1	Sede Barranco	TI	3	3	3	3	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	3	1	1	3	2	2	4.00	Bajo
										Avería de origen físico o lógico	Equipos de respaldo	-	3	2						
(ap)		Access point 3	AP repetidor 2	Sede Barranco	TI	3	3	3	3	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	3	1	1	3	2	2	4.00	Bajo
										Avería de origen físico o lógico	Equipos de respaldo	-	3	2						
(print)	FU_HW_MI	Medios de impresión	Impresoras.	Sede Barranco	TI	2	2	2	2	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	3	1	1	3	2	2	4.00	Bajo
										Avería de origen físico o lógico	Equipos de respaldo	-	3	2						
(svr-backup)	FU_HW_ER	Equipos de respaldo	Servidor de respaldo.	Sede Barranco	TI	5	5	5	5	Errores de monitorización	Monitorización del hardware y software de los activos.	-	5	5	3	4	4	4	20.00	Crítico
										Errores de mantenimiento / actualización de programas (software)	Actualizaciones programadas y antivirus.	-	5	5						
										Errores de configuración	Registro de actividades y privilegios de acceso.	-	5	5						
(COM) REDES DE COMUNICACIÓN																				
(internet)	FU_COM_IN	Red de internet	Servicio interno (web) y externo (VPN).	Sede Barranco	TI	5	5	5	5	Fallo de servicios de comunicaciones	Políticas de restricción de acceso a páginas web no necesarias.	-	4	3	3	4	4	4	12.00	Alto
(pstn)	FU_COM_RT	Red telefónica	Servicio telefónico.	Sede Barranco	TI	5	5	5	5	Fallo de servicios de comunicaciones	Políticas de restricción de acceso. (Usuarios nuevos usan anexos de otras áreas).	-	4	3	2	4	4	3	9.00	Moderado
(wifi)	FU_COM_RI	Red inalámbirca	Servicio inalámbrico.	Sede Barranco	TI	4	4	4	4	Fallo de servicios de comunicaciones	Políticas de restricción de acceso a páginas web no necesarias.	-	4	3	2	2	2	2	6.00	Moderado

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

EVALUACIÓN DE RIESGO
FICHA DE OBSERVACIÓN 1 (PRE-TEST)

CÓDIGO:FU-IA-2001-001
VERSIÓN: 1.0
FECHA:
PÁGINA: 1

ACTIVOS										AMENAZAS	VULNERABILIDADES			EVALUACIÓN DEL RIESGO						
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	UBICACIÓN (física o lógica)	CUSTODIO DEL ACTIVO	VALOR DEL ACTIVO				DESCRIPCIÓN	CONTROLES AUSENTES	ANEXO A ISO 27001	NIVEL	PROBABILIDAD DE OCURRENCIA	LEGAL	OPERATIVO	ECONÓMICO	IMPACTO	RIESGO	
						C	I	D	V										VALOR DE RIESGO	NIVEL DE RIESGO
(MEDIA) SOPORTE DE INFORMACIÓN																				
(disk)	FU_MEDIA_D	Discos externos	Unidades para respaldo de infromación.	Sede Barranco	TI	5	5	5	5	Manipulación de los equipos	Seguridad física en el centro de datos.	-	5	5	2	3	3	3	15.00	Alto
(san)	FU_MEDIA_AR	Almacenamiento en red	Unidades para respaldo de información.	Sede Barranco	TI	5	5	5	5	Condiciones inadecuadas de temperatura o humedad	Seguridad física en el centro de datos.	-	5	5	2	4	4	4	20.00	Crítico
										Degradación de los soportes de almacenamiento de la información	Desgaste de equipo por el uso.	-	5	5						
										Errores de mantenimiento / actualización de equipos (hardware)	Mantenimiento físico.	-	5	5						
										Acceso no autorizado.	Políticas de acceso al usuario.	-	5	5						
(printed)	FU_MEDIA_	Material impreso	Almacenaje de información.	Sede Barranco	TI	3	3	3	3	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	2	4	4	3	4	3	12.00	Alto
(cd)	FU_MEDIA_C	CD-ROM	Almacenaje de información.	Sede Barranco	TI	3	3	3	3	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	2	4	4	3	4	3	12.00	Alto
(AUX) EQUIPAMIENTO AUXILIAR																				
(power)	FU_AU_FA	Fuentes de alimentación	Equipos de soporte.	Sede Barranco	TI	2	2	2	2	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	3	5	1	3	2	2	10.00	Moderado
										Avería de origen físico o lógico	Equipos de respaldo	-	3	5						
(power)	FU_AU_UP	UPS	Equipos de soporte.	Sede Barranco	TI	3	3	3	3	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	3	3	1	3	2	2	6.00	Moderado
										Avería de origen físico o lógico	Equipos de respaldo	-	3	2						
(ac)	FU_AU_EC	Equipos de aclimatación	Equipos de soporte.	Sede Barranco	TI	3	3	3	3	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	-	3	3	1	4	4	3	9.00	Moderado
										Errores de mantenimiento / actualización de equipos (hardware)	Equipos de respaldo	-	3	3						
(cabling)	FU_AU_CE	Cableado estructurado	Equipos de soporte.	Sede Barranco	TI	4	4	4	4	Contaminación mecánica	Mantenimiento y limpieza del cableado.	-	4	2	1	4	3	3	6.00	Moderado
(fiber)	FU_AU_FO	Fibra óptica	Equipos de soporte.	Sede Barranco	TI	4	4	4	4	Contaminación mecánica	Mantenimiento y limpieza del cableado.	-	4	2	1	4	3	3	6.00	Moderado
(furniture)	FU_AU_MB	Mobiliario: armarios, racks.	Equipos de soporte.	Sede Barranco	TI	4	4	4	4	Acceso no autorizado	Seguridad física en el centro de datos.	-	5	5	4	5	5	5	25.00	Crítico
										Manipulación de los equipos	Seguridad física en el centro de datos.	-	5	5						
										Pérdida de equipos	Seguridad física en el centro de datos.	-	5	5						
										Contaminación mecánica	Mantenimiento y limpieza.	-	5	5						
(L) INSTALACIONES																				
(building)	FU_L_ED	Edificio	Almacenaje de los sistemas de información y co	Sede Barranco	TI	4	4	4	4	Condiciones inadecuadas de temperatura o humedad	Acondicionamiento apropiado de ventilación.	-	3	3	4	4	4	4	12.00	Alto
										Contaminación mecánica	Mantenimiento y limpieza.	-	4	3						
										Uso no previsto	Instalaciones de uso para otras actividades.	-	5	3						
(site)	FU_L_OF	Oficina	Almacenaje de los sistemas de información y co	Sede Barranco	TI	4	4	4	4	Condiciones inadecuadas de temperatura o humedad	Cuarto de servidores y equipos sin seguridad.	-	5	3	4	4	4	4	12.00	Alto
										Contaminación mecánica	Mantenimiento y limpieza.	-	3	3						
										Uso no previsto	Instalaciones de uso para otras actividades.	-	5	4						
										Acceso no autorizado	Seguridad física en el centro de datos.	-	5	3						
(shelter)	FU_L_AL	Almacén	Almacenaje de los sistemas de información y co	Sede Barranco	TI	4	4	4	4	Condiciones inadecuadas de temperatura o humedad	Acondicionamiento apropiado de ventilación.	-	3	3	3	3	3	3	9.00	Moderado
										Contaminación mecánica	Mantenimiento y limpieza.	-	3	3						
(local)	FU_L_CS	Cuarto de servidor	Almacenaje de los sistemas de información y co	Sede Barranco	TI	5	5	5	5	Condiciones inadecuadas de temperatura o humedad	Acondicionamiento apropiado de ventilación.	-	5	3	4	4	4	4	12.00	Alto
										Contaminación mecánica	Mantenimiento y limpieza.	-	3	3						
										Uso no previsto	Instalaciones de uso para otras actividades.	-	5	4						
										Acceso no autorizado	Seguridad física en el centro de datos.	-	5	3						
(channel)	FU_L_CN	Canalización	Almacenaje de los sistemas de información y co	Sede Barranco	TI	4	4	4	4	Contaminación mecánica	Mantenimiento y limpieza.	-	3	3	1	2	2	2	6.00	Moderado
(P) PERSONAL																				
(ui)	FU_P_UF	Usuarios finales	Personal	Sede Barranco	TI	3	3	3	3	Ingeniería Social	Concientización sobre seguridad y normas de uso.	-	5	4	4	4	4	4	16.00	Crítico
										Deficiencias en la organización	Conocimientos básicos en caso de algún incidente con los equipos que usa.	-	5	4						
(adm)	FU_P_AS	Administrador de Sistemas	Personal	Sede Barranco	TI	3	3	3	3	Errores del administrador	Realización de inventario de activos, análisis de riesgo.	-	5	5	3	4	4	4	20.00	Crítico
(ue)	FU_P_UE	Usuarios externos (Proveedo	Personal	Sede Barranco	TI	4	4	4	4	Deficiencias en la organización	Evaluación de rendimiento del proveedor en servicio, costo, calidad, etc.	-	5	5	3	3	3	3	15.00	Crítico
																			Valor de riesgo	14.19

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

EVALUACION DE RIESGO
FICHA DE OBSERVACIÓN 1 (POST-TEST)

CÓDIGO:FU-IA-2001-001
VERSIÓN: 1.0
FECHA:
PÁGINA: 1

ACTIVOS CRÍTICOS										AMENAZAS	VULNERABILIDADES			EVALUACIÓN DEL RIESGO						
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	UBICACIÓN (física o lógica)	CUSTODIO DEL ACTIVO	VALOR DEL ACTIVO				DESCRIPCIÓN	CONTROLES AUSENTES	ANEXO A ISO 27001	NIVEL	PROBABILIDAD DE OCURRENCIA	LEGAL	OPERATIVO	ECONOMICO	IMPACTO	RIESGO	
						C	I	D	V										VALOR DE EXPOSICIÓN AL RIESGO	NIVEL DE RIESGO
(essential) ACTIVOS ESENCIALES																				
(adm)	FU_A_DP	Datos públicos	Data confidencial de la institución.	Sede Barranco	TI	5	5	5	5	Fugas de información	Actualización de procedimientos para acceso a la información.	A.9.1.1	3	2	5	5	5	5	10.00	Moderado
										Alteración accidental de la información			3	2						
(vr)	FU_A_RO	Registros de la organización	Data confidencial de la institución.	Sede Barranco	TI	5	5	5	5	Fugas de información	Actualización de procedimientos para acceso a la información.	A.9.1.1	4	2	5	5	5	5	10.00	Moderado
										Alteración accidental de la información			4	2						
(per)	FU_A_CP	Datos de carácter personal	Data confidencial de la institución.	Sede Barranco	TI	5	5	5	5	Fugas de información	Actualización de procedimientos para acceso a la información.	A.9.1.1	4	2	5	5	5	5	10.00	Moderado
										Alteración accidental de la información			4	2						
(classified)	FU_A_DC	Datos clasificados	Data confidencial de la institución.	Sede Barranco	TI	5	5	5	5	Fugas de información	Actualización de procedimientos para acceso a la información.	A.9.1.1	4	2	5	5	5	5	10.00	Moderado
										Alteración accidental de la información			4	2						
(S) SERVICIOS																				
(int)	FU_SR_EX	Usuarios externos	Prestación de servicios externos (asociadas)	Sede Barranco	TI	4	4	4	4	Alteración accidental de la información	Actualización de procedimientos para acceso a la información.	A.9.1.2	4	2	4	4	4	4	8.00	Moderado
(ext)	FU_SR_IN	Usuarios internos	Usuarios de la propia institución.	Sede Barranco	TI	4	4	4	4	Alteración accidental de la información	Actualización de procedimientos para acceso a la información.	A.9.1.2	4	2	4	4	4	4	8.00	Moderado
(www)	FU_SR_TR	Internet	Uso de paginas web.	Sede Barranco	TI	3	3	3	3	Errores de re-encaminamiento	Control de acceso a pagina web.	A.9.4.1	5	3	2	3	3	3.0	9.00	Moderado
										Fugas de información	Actualización de procedimientos para acceso a la información.		4	3						
										Errores del administrador	Configuración adecuada del acceso a internet.		5	3						
(telnet)	FU_SR_AR	Acceso remoto	Trabajos remotos de usuarios.	Sede Barranco	TI	2	2	2	2	Errores de configuración	Conocimiento de la forma de acceder remotamente.	A.6.2.2	5	2	3	4	4	4.0	8.00	Moderado
(email)	FU_SR_CE	Correo electrónico	Correo por aplicación y web.	Sede Barranco	TI	3	3	3	3	Fugas de información	La información debe ser enviada solo por el correo institucional.	A.13.2.3	2	2	4	4	4	4	8.00	Moderado
(file)	FU_SR_AD	Almacenamiento de datos	Servidor de archivos	Sede Barranco	TI	4	4	4	4	Errores del administrador	Configuración y ordenamiento de los datos.	A.11.2.8	3	2	4	4	4	4	8.00	Moderado
										Errores de monitorización	Monitorización del hardware y software de los activos.		3	2						
										Errores de configuración	Configuración de acceso a información.		3	2						
(passw)	FU_SR_CA	Claves de autenticación	Claves de acceso a usuarios internos y externos	Sede Barranco	TI	4	4	4	4	Errores del administrador	Políticas de creación de contraseña	A.9.4.3	5	2	4	4	4	4	8.00	Moderado
										Errores de los usuarios	Conocimiento del personal sobre lo vulnerable de las contraseñas.		5	2						
										Fugas de información	Configuración de acceso a información.		5	2						
(ftp)	FU_SR_TR	Transferencia de datos	Conexiones VPN.	Sede Barranco	TI	3	3	3	3	Fugas de información	Actualización de procedimientos para acceso a la información.	A.13.2.1	5	3	4	4	4	4	8.00	Moderado
										Errores de re-encaminamiento	Control de acceso a los usuarios.		5	1						
(idm)	FU_SR_GI	Gestión de identidades	Alta y baja a usuarios en el sistema.	Sede Barranco	TI	4	4	4	4	Errores de monitorización	Actualización de usuarios que ya no laboran (suspención y/o eliminació	A.9.2.6	5	2	4	4	4	4	8.00	Moderado
(ipm)	FU_SR_GP	Gestión de privilegios	Acceso a la información.	Sede Barranco	TI	4	4	4	4	Errores de configuración	Usuarios tienen acceso a otras carpetas.	A.9.2.2	5	2	4	4	4	4	8.00	Moderado
										Errores del administrador	Configuración de acceso a información.		5	2						
(SW) SOFTWARE - APLICACIONES INFORMÁTICAS																				
(prp)	FU_SW_CN	Software CONCAR	Software contable para usuarios internos.	Sede Barranco	TI	5	5	5	5	Errores de los usuarios	Realización de backups	A.9.4.2	4	2	4	4	4	4	8.00	Moderado
										Errores del administrador	Creación de usuarios para cada trabajador.		4	2	3	3	3			
(email -	FU_SW_CE	Cliente de correo electrónico	Correo por la web (office 365).	Sede Barranco	TI	4	4	4	4	Errores de los usuarios	Conocimiento del usuario a enlaces externos o ataques de ingenieria so	A.7.2.2	3	3	3	3	3	3	9.00	Moderado
(av)	FU_SW_AN	Antivirus	Software de seguridad en las computadoras.	Sede Barranco	TI	4	4	4	4	Errores de mantenimiento / actualización de programas (software)	Licencia y falta de antivirus en computadoras finales y servidor.	A.12.5.1	5	2	3	4	4	4	8.00	Moderado
(os)	FU_SW_SO	Sistema Operativo	Software licenciado para las computadoras.	Sede Barranco	TI	4	4	4	4	Errores de mantenimiento / actualización de programas (software)	Licencia y activación del sistema operativo en computadoras.	A.11.2.4	5	2	3	4	4	4	8.00	Moderado
(backup)	FU_SW_SB	Sistema de backups	Software para copias de información de las com	Sede Barranco	TI	5	5	5	5	Errores de mantenimiento / actualización de programas (software)	Programación adecuada de respaldos de la información y sistema.	A.12.3.1	5	2	3	4	4	4	8.00	Moderado
										Fugas de información	Actualización de procedimientos para acceso a la información.		5	2						
(HW) EQUIPAMIENTO INFORMÁTICO (HARDWARE)																				
(host)	FU_HW_SV	Servidor	Servidor principal de dominio.	Sede Barranco	TI	5	5	5	5	Denegación de servicio	Antivirus actualizado y permisos de usuario.	A.11.2.8	5	1	3	4	4	4	8.00	Moderado
										Errores de mantenimiento / actualización de programas (software)	Mantenimiento de servidor.		5	3						
										Pérdida de equipos	Seguridad física en el centro de datos.		5	1						
(pc)	FU_HW_DP	Desktop	Equipos de usuarios finales.	Sede Barranco	TI	4	4	4	4	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.8	3	2	3	4	4	4	8.00	Moderado
										Errores de mantenimiento / actualización de programas (software)	Actualizaciones programadas y antivirus.		4	2						

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

EVALUACION DE RIESGO
FICHA DE OBSERVACIÓN 1 (POST-TEST)

CÓDIGO:FU-IA-2001-001
VERSIÓN: 1.0
FECHA:
PÁGINA: 1

ACTIVOS CRÍTICOS										AMENAZAS	VULNERABILIDADES			EVALUACIÓN DEL RIESGO						
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	UBICACIÓN (física o lógica)	CUSTODIO DEL ACTIVO	VALOR DEL ACTIVO				DESCRIPCIÓN	CONTROLES AUSENTES	ANEXO A ISO 27001	NIVEL	PROBABILIDAD DE OCURRENCIA	IMPACTO				RIESGO	
						C	I	D	V						LEGAL	OPERATIVO	ECONOMICO	IMPACTO	VALOR DE EXPOSICIÓN AL RIESGO	NIVEL DE RIESGO
(lpt)	FU_HW_LP	Laptop	Equipos de usuarios finales.	Sede Barranco	TI	4	4	4	4	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.8	3	2	3	4	4	4		
										Errores de mantenimiento / actualización de programas (software)	Actualizaciones programadas y antivirus.		5	2					8.00	Moderado
(md)	FU_HW_MD	Marcador digital	Marcador de hora de entrada y salida de persona	Sede Barranco	TI	3	3	3	3	Contaminación mecánica	Backups de información.	A.12.3.1	3	3	1	2	2	2.0	6.00	Moderado
(router - in)	FU_HW_RI	Router de internet	Equipo principal de internet.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.1	5	2	4	4	4	4.0		
										Avería de origen físico o lógico	Equipos de respaldo		5	1						
										Manipulación de los equipos	Seguridad física en el centro de datos.		5	1					4.0	Bajo
(router - telf)	FU_HW_RT	Router de telefonía	Equipo principal de telefonía.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.1	5	2	4	4	4	4.0		
										Avería de origen físico o lógico	Equipos de respaldo		5	1						
										Manipulación de los equipos	Seguridad física en el centro de datos.		5	1					4.0	Bajo
(switch)	FU_HW_SI	Switch de datos - Internet	Enlace entre router y puntos de red.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.1	5	2	4	4	4	4.0		
										Avería de origen físico o lógico	Equipos de respaldo		5	1						
										Manipulación de los equipos	Seguridad física en el centro de datos.		5	1					4.0	Bajo
(switch)	FU_HW_ST	Switch de datos - Telefonía	Enlace entre router y líneas telefónicas.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.1	5	2	4	4	4	4.0		
										Avería de origen físico o lógico	Equipos de respaldo		5	1						
										Manipulación de los equipos	Seguridad física en el centro de datos.		5	1					4.0	Bajo
(switch)	FU_HW_SD	Switch de datos inalámbrico	Equipo de comuicación entre los access point.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.1	5	2	4	4	4	4.0		
										Avería de origen físico o lógico	Equipos de respaldo		5	1						
										Manipulación de los equipos	Seguridad física en el centro de datos.		5	1					4.0	Bajo
(fo)	FU_HW_CF	Convertidor a fibra óptica	Enlace entre la central del proveedor y el router.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.1	5	2	2	3	2	2.3		
										Manipulación de los equipos	Seguridad física en el centro de datos.		5	1					4.0	Bajo
(firewall)	FU_HW_FW	Firewall de datos	Equipo de protección.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.1	5	2	4	4	4	4.0		
										Avería de origen físico o lógico	Equipos de respaldo		5	1						
										Manipulación de los equipos	Seguridad física en el centro de datos.		5	1					4.0	Bajo
(pabx)	FU_HW_CT	Central telefónica	Equipo de comunicación telefónica.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.1	5	2	4	4	4	4.0		
										Avería de origen físico o lógico	Equipos de respaldo		5	1						
										Manipulación de los equipos	Seguridad física en el centro de datos.		5	1					4.0	Bajo
(ipphone)	FU_HW_TP	Teléfonos IP	Anexos.	Sede Barranco	TI	5	5	5	5	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.4	3	1	1	3	2	2.0		
										Avería de origen físico o lógico	Equipos de respaldo		3	2					4.00	Bajo
(ap)	FU_HW_AC	Access point 1	AP principal	Sede Barranco	TI	3	3	3	3	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.4	3	1	1	3	2	2.0		
										Avería de origen físico o lógico	Equipos de respaldo		3	2					4.00	Bajo
(ap)		Access point 2	AP repetidor 1	Sede Barranco	TI	3	3	3	3	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.4	3	1	1	3	2	2.0		
										Avería de origen físico o lógico	Equipos de respaldo		3	2					4.00	Bajo
(ap)		Access point 3	AP repetidor 2	Sede Barranco	TI	3	3	3	3	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.4	3	1	1	3	2	2.0		
										Avería de origen físico o lógico	Equipos de respaldo		3	2					4.00	Bajo
(print)	FU_HW_MI	Medios de impresión	Impresoras.	Sede Barranco	TI	2	2	2	2	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.4	3	1	1	3	2	2.0		
										Avería de origen físico o lógico	Equipos de respaldo		3	2					4.00	Bajo
(svr-backup)	FU_HW_ER	Equipos de respaldo	Servidor de respaldo.	Sede Barranco	TI	5	5	5	5	Errores de monitorización	Monitorización del hardware y software de los activos.	A.11.2.4	2	3	3	4	4	4.0		
										Errores de mantenimiento / actualización de programas (software)	Actualizaciones programadas y antivirus.		2	2						
										Errores de configuración	Registro de actividades y privilegios de acceso.		2	1					8.00	Moderado
(COM) REDES DE COMUNICACIÓN																				
(internet)	FU_COM_IN	Red de internet	Servicio interno (web) y externo (VPN).	Sede Barranco	TI	5	5	5	5	Fallo de servicios de comunicaciones	Políticas de restricción de acceso a páginas web no necesarias.	A.9.4.1	4	2	3	4	4	4.0	8.00	Moderado
(pstn)	FU_COM_RT	Red telefónica	Servicio telefónico.	Sede Barranco	TI	5	5	5	5	Fallo de servicios de comunicaciones	Políticas de restricción de acceso. (Usuarios nuevos usan anexos de o	A.9.2.5	4	3	2	4	4	3.0	9.00	Moderado
(wifi)	FU_COM_RI	Red inalámbirca	Servicio inalámbrico.	Sede Barranco	TI	4	4	4	4	Fallo de servicios de comunicaciones	Políticas de restricción de acceso a páginas web no necesarias.	A.9.4.1	4	3	2	2	2	2.0	6.00	Moderado

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

EVALUACION DE RIESGO
FICHA DE OBSERVACIÓN 1 (POST-TEST)

CÓDIGO:FU-IA-2001-001
VERSIÓN: 1.0
FECHA:
PÁGINA: 1

ACTIVOS CRÍTICOS										AMENAZAS	VULNERABILIDADES			EVALUACIÓN DEL RIESGO						
CÓDIGO DEL ACTIVO (Magerit)	CODIGO DEL ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN DEL ACTIVO	UBICACIÓN (física o lógica)	CUSTODIO DEL ACTIVO	VALOR DEL ACTIVO				DESCRIPCIÓN	CONTROLES AUSENTES	ANEXO A ISO 27001	NIVEL	PROBABILIDAD DE OCURRENCIA	LEGAL	OPERATIVO	ECONOMICO	IMPACTO	RIESGO	
						C	I	D	V										VALOR DE EXPOSICIÓN AL RIESGO	NIVEL DE RIESGO
(MEDIA) SOPORTE DE INFORMACIÓN																				
(disk)	FU_MEDIA_D	Discos externos	Unidades para respaldo de infromación.	Sede Barranco	TI	5	5	5	5	Manipulación de los equipos	Seguridad física en el centro de datos.	A.11.2.7	5	2	2	3	3	3.0	6.00	Moderado
(san)	FU_MEDIA_AR	Almacenamiento en red	Unidades para respaldo de información.	Sede Barranco	TI	5	5	5	5	Condiciones inadecuadas de temperatura o humedad	Seguridad física en el centro de datos.	A.11.2.7	5	2	2	4	4	4.0	8.00	Moderado
										Degradación de los soportes de almacenamiento de la información	Desgaste de equipo por el uso.		3	3						
										Errores de mantenimiento / actualización de equipos (hardware)	Mantenimiento físico.		5	2						
										Acceso no autorizado.	Políticas de acceso al usuario.		5	2						
(printed)	FU_MEDIA_	Material impreso	Almacenaje de información.	Sede Barranco	TI	3	3	3	3	Fugas de información	Etiquetado de información	A.8.2.2	2	3	4	3	4	4.0	12.00	Alto
(cd)	FU_MEDIA_C	CD-ROM	Almacenaje de información.	Sede Barranco	TI	3	3	3	3	Fugas de información	Etiquetado de información	A.8.2.2	2	3	4	3	4	4.0	12.00	Alto
(AUX) EQUIPAMIENTO AUXILIAR																				
(power)	FU_AU_FA	Fuentes de alimentación	Equipos de soporte.	Sede Barranco	TI	2	2	2	2	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.4	3	2	1	3	2	2.0	4.00	Bajo
										Avería de origen físico o lógico	Equipos de respaldo		3	2						
(power)	FU_AU_UP	UPS	Equipos de soporte.	Sede Barranco	TI	3	3	3	3	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.2.2	3	3	1	3	2	2.0	6.00	Moderado
										Avería de origen físico o lógico	Equipos de respaldo		3	2						
(ac)	FU_AU_EC	Equipos de aclimatación	Equipos de soporte.	Sede Barranco	TI	3	3	3	3	Contaminación mecánica	Mantenimiento y limpieza de los equipos.	A.11.1.4	2	3	1	4	4	3.0	9.00	Moderado
										Errores de mantenimiento / actualización de equipos (hardware)	Equipos de respaldo		2	3						
(cabling)	FU_AU_CE	Cableado estructurado	Equipos de soporte.	Sede Barranco	TI	4	4	4	4	Contaminación mecánica	Mantenimiento y limpieza del cableado.	A.11.2.4	4	3	1	4	3	3.0	9.00	Moderado
(fiber)	FU_AU_FO	Fibra óptica	Equipos de soporte.	Sede Barranco	TI	4	4	4	4	Contaminación mecánica	Mantenimiento y limpieza del cableado.	A.11.2.4	4	3	1	4	3	3.0	9.00	Moderado
(furniture)	FU_AU_MB	Mobiliario: armarios, racks.	Equipos de soporte.	Sede Barranco	TI	4	4	4	4	Acceso no autorizado	Seguridad física en el centro de datos.	A.11.1.3	5	2	4	5	5	5.0	10.00	Moderado
										Manipulación de los equipos	Seguridad física en el centro de datos.		5	2						
										Pérdida de equipos	Seguridad física en el centro de datos.		5	2						
										Contaminación mecánica	Mantenimiento y limpieza.		5	2						
(L) INSTALACIONES																				
(building)	FU_L_ED	Edificio	Almacenaje de los sistemas de información y co	Sede Barranco	TI	4	4	4	4	Condiciones inadecuadas de temperatura o humedad	Acondicionamiento apropiado de ventilación.	A.11.1.3	3	2	4	4	4	4.0	8.00	Moderado
										Contaminación mecánica	Mantenimiento y limpieza.		4	2						
										Uso no previsto	Instalaciones de uso para otras actividades.		5	3						
(site)	FU_L_OF	Oficina	Almacenaje de los sistemas de información y co	Sede Barranco	TI	4	4	4	4	Condiciones inadecuadas de temperatura o humedad	Cuarto de servidores y equipos sin seguridad.	A.11.1.3	5	2	4	4	4	4.0	8.00	Moderado
										Contaminación mecánica	Mantenimiento y limpieza.		3	3						
										Uso no previsto	Instalaciones de uso para otras actividades.		5	2						
										Acceso no autorizado	Seguridad física en el centro de datos.		5	2						
(shelter)	FU_L_AL	Almacén	Almacenaje de los sistemas de información y co	Sede Barranco	TI	4	4	4	4	Condiciones inadecuadas de temperatura o humedad	Acondicionamiento apropiado de ventilación.	A.11.1.4	3	2	3	3	3	3.0	9.00	Moderado
										Contaminación mecánica	Mantenimiento y limpieza.		3	3						
(local)	FU_L_CS	Cuarto de servidor	Almacenaje de los sistemas de información y co	Sede Barranco	TI	5	5	5	5	Condiciones inadecuadas de temperatura o humedad	Acondicionamiento apropiado de ventilación.	A.11.1.3	5	2	4	4	4	4.0	8.00	Moderado
										Contaminación mecánica	Mantenimiento y limpieza.		3	3						
										Uso no previsto	Instalaciones de uso para otras actividades.		5	2						
										Acceso no autorizado	Seguridad física en el centro de datos.		5	2						
(channel)	FU_L_CN	Canalización	Almacenaje de los sistemas de información y co	Sede Barranco	TI	4	4	4	4	Contaminación mecánica	Mantenimiento y limpieza.	A.11.2.4	3	2	1	2	2	2.0	4.00	Bajo
(P) PERSONAL																				
(ui)	FU_P_UF	Usuarios finales	Personal	Sede Barranco	TI	3	3	3	3	Ataques de ingeniería social.	Concientización sobre seguridad y normas de uso.	A.7.2.2	5	2	4	4	4	4.0	8.00	Moderado
										Deficiencias en la organización	Conocimientos básicos en caso de algún incidente con los equipos qu		5	2						
(adm)	FU_P_AS	Administrador de Sistemas	Personal	Sede Barranco	TI	3	3	3	3	Errores del administrador	Implementación de concientización al usuario en seguridad.	A.8.1.1	5	2	3	4	4	4.0	8.00	Moderado
(ue)	FU_P_UE	Usuarios externos (Proveedo	Personal	Sede Barranco	TI	4	4	4	4	Deficiencias en la organización	Evaluación de rendimiento del proveedor en servicio, costo, calidad, etc	A.15.1.1	5	3	3	3	3	3.0	9.00	Moderado
														Valor de riesgo					7.28	

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

DECLARACIÓN DE APLICABILIDAD
TRATAMIENTO DE RIESGO
FICHA DE OBSERVACIÓN 2 (PRE-TEST)

CÓDIGO:FU-CS-2001-001
VERSIÓN: 1.0
PÁGINA: 1

LR: requerimientos legales,CO: obligaciones contractuales,BR/BP: requerimientos del negocio/mejores prácticas adoptadas ,RRA: resultado de la valoración de riesgos;TSE: hasta cierto punto

CLÁUSULA	SECCIÓN	CONTROL	APLICA / NO APLICA	JUSTIFICACIÓN (justificación de exclusión)	ESTADO ACTUAL	Controles seleccionados y razones de selección				OBSERVACIONES DE LA IMPLEMENTACIÓN
						LR	CO	BR/BP	RRA	
5 Políticas de Seguridad	**A.5 Políticas de seguridad de la información**									
	A.5.1 Dirección de la gerencia para la seguridad de la información									
	A.5.1.1	Políticas para la seguridad de la información	Aplica	-	No existente	-	-	-	-	-
	A.5.1.2	Revisión de las políticas para la seguridad de la información	Aplica	-	No existente	-	-	-	-	-
6 Organización de la Seguridad de la Información	**A.6 Organización de la seguridad de la información**									
	A.6.1 Organización interna									
	A.6.1.1	Roles y responsabilidades para la seguridad de la información	Aplica	-	No existente	-	-	-	-	-
	A.6.1.2	Segregación de funciones	Aplica	-	No existente	-	-	-	-	-
	A.6.1.3	Contacto con autoridades	Aplica	-	No existente	-	-	-	-	-
	A.6.1.4	Contacto con grupos especiales de interés	Aplica	-	No existente	-	-	-	-	-
	A.6.1.5	Seguridad de la información en la gestión de proyectos	Aplica	-	No existente	-	-	-	-	-
	A.6.2 Dispositivos móviles y teletrabajo									
	A.6.2.1	Política de dispositivos móviles	Aplica	-	No existente	-	-	-	-	-
	A.6.2.2	Teletrabajo	Aplica	-	No existente	-	-	-	-	-
7 Seguridad en los Recursos Humanos	**A.7 Seguridad de los recursos humanos**									
	A.7.1 Antes del empleo									
	A.7.1.1	Investigación de antecedentes	Aplica	-	No existente	-	-	-	-	-
	A.7.1.2	Términos y condiciones del empleo	Aplica	-	No existente	-	-	-	-	-
	A.7.2 Durante el empleo									
	A.7.2.1	Responsabilidades de la gerencia	Aplica	-	No existente	-	-	-	-	-
	A.7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	Aplica	-	No existente	-	-	-	-	-
	A.7.2.3	Proceso disciplinario	Aplica	-	No existente	-	-	-	-	-
	A.7.3 Terminación y cambio de empleo									
	A7.3.1	Terminación o cambio de responsabilidades del empleo.	Aplica	-	No existente	-	-	-	-	-
8 Gestión de Activos	**A.8 Gestión de activos**									
	A.8.I Responsabilidad por los activos									
	A.8.1.1	Inventario de activos	Aplica	-	No existente	-	-	-	-	-
	A.8.1.2	Propiedad de los activos	Aplica	-	No existente	-	-	-	-	-
	A.8.I.3	Uso aceptable de los activos	Aplica	-	No existente	-	-	-	-	-
	A.8.I.4	Retorno de activos	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.8.2 Clasificación de la información									
	A.8.2.1	Clasificación de la información	Aplica	-	No existente	-	-	-	-	-
	A.8.2.2	Eliminación de soportes	Aplica	-	No existente	-	-	-	-	-
	A.8.2.3	Manejo de activos	Aplica	-	No existente	-	-	-	-	-

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES Mejorando vidas	DECLARACIÓN DE APLICABILIDAD TRATAMIENTO DE RIESGO FICHA DE OBSERVACIÓN 2 (PRE-TEST)	CÓDIGO:FU-CS-2001-001 VERSIÓN: 1.0 PÁGINA: 1

LR: requerimientos legales,CO: obligaciones contractuales,BR/BP: requerimientos del negocio/mejores prácticas adoptadas ,RRA: resultado de la valoración de riesgos;TSE: hasta cierto punto

CLÁUSULA	SECCIÓN	CONTROL	APLICA / NO APLICA	JUSTIFICACIÓN (justificación de exclusión)	ESTADO ACTUAL	Controles seleccionados y razones de selección				OBSERVACIONES DE LA IMPLEMENTACIÓN
						LR	CO	BR/BP	RRA	
	A.8.3 Manejo de los medios									
	A.8.3.1	Gestión de medios removibles	Aplica	-	No existente	-	-	-	-	-
	A.8.3.2	Disposición de medios	Aplica	-	No existente	-	-	-	-	-
	A.8.3.3	Transferencia de medios física	Aplica	-	No existente	-	-	-	-	-
9 Control de Acceso	**A.9 Control de acceso**									
	A.9.1 Requisitos de la empresa para el control de acceso									
	A.9.1.1	Política de control de acceso	Aplica	-	No existente	-	-	-	-	-
	A.9.1.2	Acceso a redes y servicios de red	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.9.2 Gestión de acceso de usuario									
	A.9.2.1	Registro y baja de usuarios	Aplica	-	No existente	-	-	-	-	-
	A.9.2.2	Gestión de los derechos de acceso asignados a usuarios	Aplica	-	No existente	-	-	-	-	-
	A.9.2.3	Gestión de los derechos de acceso con privilegios especiales	Aplica	-	No existente	-	-	-	-	-
	A.9.2.4	Gestión de información de autentificación secreta de usuarios	Aplica	-	No existente	-	-	-	-	-
	A.9.2.5	Revisión de derecho de acceso de usuarios	Aplica	-	No existente	-	-	-	-	-
	A.9.2.6	Remoción o ajuste de derechos de acceso	Aplica	-	No existente	-	-	-	-	-
	A.9.3 Responsabilidades de los usuarios									
	A9.3.1	Uso de información de autentificación secreta	Aplica	-	No existente	-	-	-	-	-
	A.9.4 Control de acceso a sistemas y aplicaciones									
	A.9.4.1	Restricción de acceso a la información	Aplica	-	No existente	-	-	-	-	-
	A.9.4.2	Procedimientos de ingreso seguro	Aplica	-	No existente	-	-	-	-	-
	A.9.4.3	Sistema de gestión de contraseñas	Aplica	-	No existente	-	-	-	-	-
	A.9.4.4	Uso de programas utilitarios privilegiados	Aplica	-	No existente	-	-	-	-	-
	A.9.4.5	Control de acceso al código fuente de los programas	Aplica	-	No existente	-	-	-	-	-
10 Criptografía	**A.10 Criptografía**									
	A.10.1 Controles criptográficos									
	A.10.1.1	Politica sobre el uso de controles criptográficos	Aplica	-	No existente	-	-	-	-	-
	A.10.1.2	Gestión de claves	Aplica	-	No existente	-	-	-	-	-
	A.11 Seguridad física y ambiental									
	A.11.1 Áreas seguras									
	A.11.1.1	Perímetro de seguridad física	Aplica	-	No existente	-	-	-	-	-
	A.11.1.2	Controles de ingreso físico	Aplica	-	No existente	-	-	-	-	-
	A.11.1.3	Asegurar oficinas, áreas e instalaciones	Aplica	-	No existente	-	-	-	-	-
	A.11.1.4	Protección contra amenazas externas y ambientales	Aplica	-	No existente	-	-	-	-	-
	A.11.1.5	Trabajo en áreas seguras	Aplica	-	No existente	-	-	-	-	-

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

DECLARACIÓN DE APLICABILIDAD
TRATAMIENTO DE RIESGO
FICHA DE OBSERVACIÓN 2 (PRE-TEST)

CÓDIGO:FU-CS-2001-001
VERSIÓN: 1.0
PÁGINA: 1

LR: requerimientos legales,CO: obligaciones contractuales,BR/BP: requerimientos del negocio/mejores prácticas adoptadas ,RRA: resultado de la valoración de riesgos;TSE: hasta cierto punto

CLÁUSULA	SECCIÓN	CONTROL	APLICA / NO APLICA	JUSTIFICACIÓN (justificación de exclusión)	ESTADO ACTUAL	Controles seleccionados y razones de selección				OBSERVACIONES DE LA IMPLEMENTACIÓN
						LR	CO	BR/BP	RRA	
11 Seguridad Física y del Entorno	A.11.1.6	Areas de despacho y carga	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11.2 Seguridad de los equipos									
	A.11.2.1	Emplazamiento y protección de los equipos	Aplica	-	No existente	-	-	-	-	-
	A.11.2.2	Servicios de suministro	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11.2.3	Seguridad del cableado	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11.2.4	Mantenimiento de equipos	Aplica	-	No existente	-	-	-	-	-
	A.11.2.5	Salida de activos fuera de las dependencias de la empresa	Aplica	-	No existente	-	-	-	-	-
	A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Aplica	-	No existente	-	-	-	-	-
	A.11.2.7	Retirada o reutilización segura de dispositivos de almacenamiento	Aplica	-	No existente	-	-	-	-	-
	A.11.2.8	Equipos de usuario desatendidos	Aplica	-	No existente	-	-	-	-	-
	A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	Aplica	-	No existente	-	-	-	-	-
12 Seguridad en las Operaciones	**A.12 Seguridad de las operaciones**									
	A.12.1 Procedimientos y responsabilidades operativas									
	A.12.1.1	Documentación de procedimientos de operación	Aplica	-	No existente	-	-	-	-	-
	A.12.1.2	Gestión del cambio	Aplica	-	No existente	-	-	-	-	-
	A.12.1.3	Gestión de la capacidad	Aplica	-	No existente	-	-	-	-	-
	A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	No aplica	No se desarrolla programas propios	No existente	-	-	-	-	-
	A.12.2 Protección contra códigos maliciosos									
	A.12.2.1	Controles contra códigos maliciosos	Aplica	-	No existente	-	-	-	-	-
	A.12.3 Copias de seguridad									
	A.12.3.1	Respaldo de la información	Aplica	-	No existente	-	-	-	-	-
	A.12.4 Registros y monitoreo									
	A.12.4.1	Registro de eventos	Aplica	-	No existente	-	-	-	-	-
	A.12.4.2	Protección de información de registros	Aplica	-	No existente	-	-	-	-	-
	A.12.4.3	Registros del administrador y del operador	Aplica	-	No existente	-	-	-	-	-
	A.12.4.4	Sicronización de reloj	Aplica	-	No existente	-	-	-	-	-
	A.12.5 Control del software operacional									
	A.12.5.1	Instalación de software en sistemas operacionales	Aplica	-	No existente	-	-	-	-	-
	A.12.6 Gestión de vulnerabilidlad técnica									
	A.12.6.1	Gestión de vulnerabilidades técnicas	Aplica	-	No existente	-	-	-	-	-
	A.12.6.2	Restricciones sobre la instalación de software	Aplica	-	No existente	-	-	-	-	-
	A.12.7 Consideraciones para la auditoría de los sistemas de información									
	A.12.7.1	Controles de auditoría de sistemas de información	Aplica	-	No existente	-	-	-	-	-

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

DECLARACIÓN DE APLICABILIDAD
TRATAMIENTO DE RIESGO
FICHA DE OBSERVACIÓN 2 (PRE-TEST)

CÓDIGO:FU-CS-2001-001
VERSIÓN: 1.0
PÁGINA: 1

LR: requerimientos legales,CO: obligaciones contractuales,BR/BP: requerimientos del negocio/mejores prácticas adoptadas ,RRA: resultado de la valoración de riesgos;TSE: hasta cierto punto

CLÁUSULA	SECCIÓN	CONTROL	APLICA / NO APLICA	JUSTIFICACIÓN (justificación de exclusión)	ESTADO ACTUAL	Controles seleccionados y razones de selección				OBSERVACIONES DE LA IMPLEMENTACIÓN
						LR	CO	BR/BP	RRA	
13 Seguridad en las Comunicaciones	**A.13 Seguridad de las comunicaciones**									
	A.13.1 Gestión de seguridad de la red									
	A.13.1.l	Controles de la red	Aplica	-	No existente	-	-	-	-	-
	A.13.1.2	Seguridad de servicios de red	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.13.1.3	Segregación en redes	Aplica	-	No existente	-	-	-	-	-
	A.13.2 Transferencia de información									
	A.13.2.1	Politicas y procedimientos de transferencia de la información	Aplica	-	No existente	-	-	-	-	-
	A.13.2.2	Acuerdo sobre transferencia de información	Aplica	-	No existente	-	-	-	-	-
	A.13.2.3	Mensajes electrónicos	Aplica	-	No existente	-	-	-	-	-
	A.13.2.4	Acuerdos de confidencialidad o no divulgación	Aplica	-	No existente	-	-	-	-	-
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	**A.14 Adquisición, desarrollo y mantenimiento de sistemas**									
	A.14.l Requisitos de seguridad de los sistemas de información									
	A.14.1.l	Análisis y especificación de requisitos de seguridad de la inforrmación	Aplica	-	No existente	-	-	-	-	-
	A.14.1.2	Seguridad de las comunicaciones en servicios accesibles sobre redes	Aplica	-	No existente	-	-	-	-	-
	A.14.1.3	Protección de transacciones en servicios de aplicación	Aplica	-	No existente	-	-	-	-	-
	A.14.2 Seguridad en los procesos de desarrollo y soporte									
	A.14.2.1	Política de desarrollo seguro	No aplica	No se desarrolla programas propios	No existente	-	-	-	-	-
	A.14.2.2	Procedimientos de control de cambio del sistema	No aplica	No se desarrolla programas propios	No existente	-	-	-	-	-
	A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma	Aplica	-	No existente	-	-	-	-	-
	A.14.2.4	Restricciones sobre cambios a los paquetes de software	Aplica	-	No existente	-	-	-	-	-
	A.14.2.5	Principios de ingenieria de sisternas seguros	Aplica	-	No existente	-	-	-	-	-
	A.14.2.6	Ambiente de desarrollo seguro	Aplica	-	No existente	-	-	-	-	-
	A.14.2.7	Desarrollo contratado externamente	Aplica	-	No existente	-	-	-	-	-
	A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	No aplica	No se desarrolla programas propios	No existente	-	-	-	-	-
	A.14.2.9	Pruebas de aceptación del sistema	No aplica	No se desarrolla programas propios	No existente	-	-	-	-	-
	A.14.3 Datos de prueba									
	A.14.3.1	Protección de datos de prueba	Aplica		No existente	-	-	-	-	-
15 Relaciones con Proveedores	**A.15 Relaciones con los proveedores**									
	A.15.1 Seguridad de la información en las re1aciones con los proveedores									
	A.15.1.1	Política de seguridad de la información para las relaciones con los proveed	Aplica	-	No existente	-	-	-	-	-
	A.15.1.2	Tratamiento de riesgo dentro de los acuerdos con proveedores	Aplica	-	No existente	-	-	-	-	-
	A.15.1.3	Cadena de suninistro de tecnología de infromación y comunicación	Aplica	-	No existente	-	-	-	-	-
	A.15.2 Gestión de entrega de servicios del proveedor									
	A.15.2.1	Monitoreo y revisión de servicios de los proveedores	Aplica	-	No existente	-	-	-	-	-

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES Mejorando vidas	DECLARACIÓN DE APLICABILIDAD TRATAMIENTO DE RIESGO FICHA DE OBSERVACIÓN 2 (PRE-TEST)	CÓDIGO:FU-CS-2001-001 VERSIÓN: 1.0 PÁGINA: 1

LR: requerimientos legales,CO: obligaciones contractuales,BR/BP: requerimientos del negocio/mejores prácticas adoptadas ,RRA: resultado de la valoración de riesgos;TSE: hasta cierto punto

CLÁUSULA	SECCIÓN	CONTROL	APLICA / NO APLICA	JUSTIFICACIÓN (justificación de exclusión)	ESTADO ACTUAL	Controles seleccionados y razones de selección				OBSERVACIONES DE LA IMPLEMENTACIÓN
						LR	CO	BR/BP	RRA	
	A.15.2.2	Gestión de cambios a los servicios de proveedores	Aplica	-	No existente	-	-	-	-	-
16 Gestión de Incidentes de Seguridad de la Información	**A.16 Gestión de incidentes de seguridad de la información**									
	A.16.I Gestión de incidentes de seguridad de la información y mejoras									
	A.16.1.I	Responsabilidades y procedimientos	Aplica	-	No existente	-	-	-	-	-
	A.16.1.2	Reporte de eventos de seguridad de la infonnación	Aplica	-	No existente	-	-	-	-	-
	A.16.1.3	Reporte de debilidades de seguridad de la infonnación	Aplica	-	No existente	-	-	-	-	-
	A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	Aplica	-	No existente	-	-	-	-	-
	A.16.1.5	Respuesta a incidentes de seguridad de la infonnación	Aplica	-	No existente	-	-	-	-	-
	A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Aplica	-	No existente	-	-	-	-	-
	A.16.1.7	Recolección de evidencia	Aplica	-	No existente	-	-	-	-	-
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	**A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio**									
	A.17.1 Continuidad de seguridad de la información									
	A.17.1.1	Planificación de continuidad de seguridad de la información	Aplica	-	No existente	-	-	-	-	-
	A.17.1.2	Implementación de continuidad de seguridad de la información	Aplica	-	No existente	-	-	-	-	-
	A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la	Aplica	-	No existente	-	-	-	-	-
	A.17.2 Redundancias									
	A.17.2.1	Instalaciones de procesamiento de la información	Aplica	-	No existente	-	-	-	-	-
18 Cumplimiento	**A.18 Cumplimiento**									
	A.18.1 Cumplimiento con requisitos legales y contractuales									
	A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	Aplica	-	No existente	-	-	-	-	-
	A.18.1.2	Derechos de propiedad intelectual	Aplica	-	No existente	-	-	-	-	-
	A.18.1.3	Protección de registros de la organización	Aplica	-	No existente	-	-	-	-	-
	A.18.1.4	Privacidad y protección de datos personales	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.18.1.5	Regulación de controles criptográficos	Aplica	-	No existente	-	-	-	-	-
	A.18.2 Revisiones de seguridad de la información									
	A.18.2.1	Revisión independiente de la seguridad de la información	Aplica	-	No existente	-	-	-	-	-
	A.18.2.2	Cumplimiento de políticas y normas de seguridad	Aplica	-	No existente	-	-	-	-	-
	A.18.2.3	Revisión del cumplimiento técnico	Aplica	-	No existente	-	-	-	-	-

Políticas implementadas	
No existente	107
Existente	7
Total	114

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES Mejorando vidas	DECLARACIÓN DE APLICABILIDAD TRATAMIENTO DE RIESGO FICHA DE OBSERVACIÓN 2 (POST-TEST)	CÓDIGO:FU-CS-2001-001 VERSIÓN: 1.0 PÁGINA: 1

LR: requerimientos legales,CO: obligaciones contractuales,BR/BP: requerimientos del negocio/mejores prácticas adoptadas ,RRA: resultado de la valoración de riesgos;TSE: hasta cierto punto

CLÁUSULA	SECCIÓN	CONTROL	APLICA	JUSTIFICACIÓN (justificación de exclusión)	ESTADO ACTUAL	Controles seleccionados y razones de selección				OBSERVACIONES DE LA IMPLEMENTACIÓN
						LR	CO	BR/BP	RRA	
5 Políticas de Seguridad	**A.5 Políticas de seguridad de la información**									
	A.5.1 Dirección de la gerencia para la seguridad de la información									
	A.5.1.1	Políticas para la seguridad de la información	Aplica	-	Existente	-	-	x		Implementación al 100%
	A.5.1.2	Revisión de las políticas para la seguridad de la información	Aplica	-	Existente	-	-	x		Implementación al 100%
6 Organización de la Seguridad de la Información	**A.6 Organización de la seguridad de la información**									
	A.6.1 Organización interna									
	A.6.1.1	Roles y responsabilidades para la seguridad de la información	No aplica	-	Existente	-	-	x		Implementación al 100%
	A.6.1.2	Segregación de funciones	No aplica	-	Existente	-	-	x		Implementación al 100%
	A.6.1.3	Contacto con autoridades	Aplica	-	No existente	-	-			
	A.6.1.4	Contacto con grupos especiales de interés	Aplica	-	Existente	-	-	x		Implementación al 100%
	A.6.1.5	Seguridad de la información en la gestión de proyectos	Aplica	-	Existente	-	-	x		Implementación al 100%
	A.6.2 Dispositivos móviles y teletrabajo									
	A.6.2.1	Política de dispositivos móviles	Aplica	-	Existente	-	-	x		Implementación al 100%
	A..6.2.2	Teletrabajo	Aplica	-	Existente	-	-	x		Implementación al 100%
7 Seguridad en los Recursos Humanos	**A.7 Seguridad de los recursos humanos**									
	A.7.1 Antes del empleo									
	A.7.1.1	Investigación de antecedentes	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.7.1.2	Términos y condiciones del empleo	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.7.2 Durante el empleo									
	A.7.2.1	Responsabilidades de la gerencia	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.7.2.3	Proceso disciplinario	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.7.3 Terminación y cambio de empleo									
	A.7.3.1	Terminación o cambio de responsabilidades del empleo.	Aplica	-	Existente	-	-	x	-	Implementación al 100%
8 Gestión de Activos	**A.8 Gestión de activos**									
	A.8.1 Responsabilidad por los activos									
	A.8.1.1	Inventario de activos	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.8.1.2	Propiedad de los activos	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.8.1.3	Uso aceptable de los activos	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.8.1.4	Retorno de activos	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.8.2 Clasificación de la información									
	A.8.2.1	Clasificación de la información	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.8.2.2	Etiquetado de la información	Aplica	-	Existente	-	-	x	-	Implementación al 100%

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES Mejorando vidas	DECLARACIÓN DE APLICABILIDAD TRATAMIENTO DE RIESGO FICHA DE OBSERVACIÓN 2 (POST-TEST)	CÓDIGO:FU-CS-2001-001 VERSIÓN: 1.0 PÁGINA: 1

LR: requerimientos legales,CO: obligaciones contractuales,BR/BP: requerimientos del negocio/mejores prácticas adoptadas ,RRA: resultado de la valoración de riesgos;TSE: hasta cierto punto

CLÁUSULA	SECCIÓN	CONTROL	APLICA	JUSTIFICACIÓN (justificación de exclusión)	ESTADO ACTUAL	Controles seleccionados y razones de selección				OBSERVACIONES DE LA IMPLEMENTACIÓN
						LR	CO	BR/BP	RRA	
	A.8.2.3	Manejo de activos	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.8.3 Manejo de los medios									
	A.8.3.1	Gestión de medios removibles	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.8.3.2	Eliminación de medios	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.8.3.3	Transferencia de medios física	Aplica	-	Existente	-	-	x	-	Implementación al 100%
9 Control de Acceso	**A.9 Control d.e acceso**									
	A.9.1 Requisitos de la empresa para el control de acceso									
	A.9.1.1	Política de control de acceso	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.9.1.2	Acceso a redes y servicios de red	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.9.2 Gestión de acceso de usuario									
	A.9.2.1	Registro y baja de usuarios	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.9.2.2	Gestión de los derechos de acceso asignados a usuarios	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.9.2.3	Gestión de los derechos de acceso con privilegios especiales	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.9.2.4	Gestión de información de autentificación secreta de usuarios	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.9.2.5	Revisión de derecho de acceso de usuarios	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.9.2.6	Remoción o ajuste de derechos de acceso	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.9.3 Responsabilidades de los usuarios									
	A9.3.1	Uso de información de autentificación secreta	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.9.4 Control de acceso a sistemas y aplicaciones									
	A.9.4.1	Restricción de acceso a la información	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.9.4.2	Procedimientos de ingreso seguro	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.9.4.3	Sistema de gestión de contraseñas	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.9.4.4	Uso de programas utilitarios privilegiados	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.9.4.5	Control de acceso al código fuente de los programas	Aplica	-	Existente	-	-	x	-	Implementación al 100%
10 Criptografía	**A.10 Criptografía**									
	A.10.1 Controles criptográficos									
	A.10.1.1	Política sobre el uso de controles criptográficos	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.10.1.2	Gestión de claves	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11 Seguridad física y ambiental									
	A.11.1 Áreas seguras									
	A.11.1.1	Perímetro de seguridad física	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11.1.2	Controles de ingreso físico	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11.1.3	Asegurar oficinas, áreas e instalaciones	Aplica	-	Existente	-	-	x	-	Implementación al 100%

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

DECLARACIÓN DE APLICABILIDAD
TRATAMIENTO DE RIESGO
FICHA DE OBSERVACIÓN 2 (POST-TEST)

CÓDIGO:FU-CS-2001-001
VERSIÓN: 1.0
PÁGINA: 1

LR: **requerimientos legales,**CO: **obligaciones contractuales,**BR/BP: **requerimientos del negocio/mejores prácticas adoptadas ,**RRA: **resultado de la valoración de riesgos;**TSE: hasta cierto punto

CLÁUSULA	SECCIÓN	CONTROL	APLICA	JUSTIFICACIÓN (justificación de exclusión)	ESTADO ACTUAL	Controles seleccionados y razones de selección				OBSERVACIONES DE LA IMPLEMENTACIÓN
						LR	CO	BR/BP	RRA	
11 Seguridad Física y del Entorno	A.11.1.4	Protección contra amenazas externas y ambientales	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11.1.5	Trabajo en áreas seguras	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11.1.6	Areas de despacho y carga	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11.2 Seguridad de los equipos									
	A.11.2.1	Emplazamiento y protección de los equipos	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11.2.2	Servicios de suministro	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11.2.3	Seguridad del cableado	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11.2.4	Mantenimiento de equipos	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11.2.5	Salida de activos fuera de las dependencias de la empresa	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11.2.7	Retirada o reutilización segura de dispositivos de almacenamiento	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11.2.8	Equipos de usuario desatendidos	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla	Aplica	-	Existente	-	-	x	-	Implementación al 100%
12 Seguridad en las Operaciones	**A.12 Seguridad de las operaciones**									
	A.12.1 Procedimientos y responsabilidades operativas									
	A.12.1.1	Documentación de procedimientos de operación	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.12.1.2	Gestión del cambio	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.12.1.3	Gestión de la capacidad	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	No aplica	No se desarrolla programas propios	No existente	-	-	-	-	-
	A.12.2 Protección contra códigos maliciosos									
	A.12.2.1	Controles contra códigos maliciosos	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.12.3 Copias de seguridad									
	A.12.3.1	Respaldo de la información	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.12.4 Registros y monitoreo									
	A.12.4.1	Registro de eventos	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.12.4.2	Protección de información de registros	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.12.4.3	Registros del administrador y del operador	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.12.4.4	Sicronización de reloj	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.12.5 Control del software operacional									
	A.12.5.1	Instalación de software en sistemas operacionales	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.12.6 Gestión de vulnerabilidad técnica									
	A.12.6.1	Gestión de vulnerabilidades técnicas	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.12.6.2	Restricciones sobre la instalación de software	Aplica	-	Existente	-	-	x	-	Implementación al 100%

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

DECLARACIÓN DE APLICABILIDAD
TRATAMIENTO DE RIESGO
FICHA DE OBSERVACIÓN 2 (POST-TEST)

CÓDIGO:FU-CS-2001-001
VERSIÓN: 1.0
PÁGINA: 1

LR: requerimientos legales,CO: obligaciones contractuales,BR/BP: requerimientos del negocio/mejores prácticas adoptadas ,RRA: resultado de la valoración de riesgos;TSE: hasta cierto punto

CLÁUSULA	SECCIÓN	CONTROL	APLICA	JUSTIFICACIÓN (justificación de exclusión)	ESTADO ACTUAL	Controles seleccionados y razones de selección				OBSERVACIONES DE LA IMPLEMENTACIÓN
						LR	CO	BR/BP	RRA	
	A.12.7 Consideraciones para la auditoría de los sistemas de información									
	A.12.7.1	Controles de auditoria de sistemas de información	Aplica	-	Existente	-	-	x	-	Implementación al 100%
13 Seguridad en las Comunicaciones	**A.13 Seguridad de las comunicaciones**									
	A.13.1 Gestión de seguridad de la red									
	A.13.1.1	Controles de la red	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.13.1.2	Seguridad de servicios de red	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.13.1.3	Segregación en redes	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.13.2 Transferencia de información									
	A.13.2.1	Politicas y procedimientos de transferencia de la información	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.13.2.2	Acuerdo sobre transferencia de información	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.13.2.3	Mensajes electrónicos	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.13.2.4	Acuerdos de confidencialidad o no divulgación	Aplica	-	Existente	-	-	x	-	Implementación al 100%
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	**A.14 Adquisición, desarrollo y mantenimiento de sistemas**									
	A.14.1 Requisitos de seguridad de los sistemas de información									
	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.14.1.2	Seguridad de las comunicaciones en servicios accesibles sobre redes públicas	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.14.1.3	Protección de transacciones en servicios de aplicación	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.14.2 Seguridad en los procesos de desarrollo y soporte									
	A.14.2.1	Politica de desarrollo seguro	No aplica	No se desarrolla programas propios	No existente	-	-	-	-	-
	A.14.2.2	Procedimientos de control de cambio del sistema	No aplica	No se desarrolla programas propios	No existente	-	-	-	-	-
	A.14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	Aplica	-	Existente	-	-	-	-	Implementación al 100%
	A.14.2.4	Restricciones sobre cambios a los paquetes de software	No aplica	-	No existente	-	-	-	-	-
	A.14.2.5	Principios de ingenieria de sistemas seguros	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.14.2.6	Ambiente de desarrollo seguro	No aplica	No se cuenta con las versiones de las copias	No existente	-	-	-	-	-
	A.14.2.7	Desarrollo contratado externamente	No aplica	-	No existente	-	-	-	-	-
	A.14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas	No aplica	No se desarrolla programas propios	No existente	-	-	-	-	-
	A.14.2.9	Pruebas de aceptación del sistema	No aplica	No se desarrolla programas propios	No existente	-	-	-	-	-
	A.14.3 Datos de prueba									
	A.14.3.1	Protección de datos de prueba	Aplica	-	Existente	-	-	x	-	Implementación al 100%
15 Relaciones con Proveedores	**A.15 Relaciones con los proveedores**									
	A.15.1 Seguridad de la información en las relaciones con los proveedores									
	A.15.1.1	Politica de seguridad de la información para las relaciones con los proveedores	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.15.1.2	Tratamiento de riesgo dentro de los acuerdos con proveedores	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.15.1.3	Cadena de suninistro de tecnologia de infromación y comunicación	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.15.2 Gestión de entrega de servicios del proveedor									

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

GRUPO FUNDADES
Mejorando vidas

DECLARACIÓN DE APLICABILIDAD
TRATAMIENTO DE RIESGO
FICHA DE OBSERVACIÓN 2 (POST-TEST)

CÓDIGO:FU-CS-2001-001
VERSIÓN: 1.0
PÁGINA: 1

LR: requerimientos legales,CO: obligaciones contractuales,BR/BP: requerimientos del negocio/mejores prácticas adoptadas ,RRA: resultado de la valoración de riesgos;TSE: hasta cierto punto

CLÁUSULA	SECCIÓN	CONTROL	APLICA	JUSTIFICACIÓN (justificación de exclusión)	ESTADO ACTUAL	Controles seleccionados y razones de selección				OBSERVACIONES DE LA IMPLEMENTACIÓN
						LR	CO	BR/BP	RRA	
	A.15.2.1	Monitoreo y revisión de servicios de los proveedores	Aplica	-	No existente	-	-	-	-	-
	A.15.2.2	Gestión de cambios a los servicios de proveedores	Aplica	-	No existente	-	-	-	-	-
16 Gestión de Incidentes de Seguridad de la Información	**A.16 Gestión de incidentes de seguridad de la información**									
	A.16.1 Gestión de incidentes de seguridad de la información y mejoras									
	A.16.1.1	Responsabilidades y procedimientos	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.16.1.2	Reporte de eventos de seguridad de la infonnación	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.16.1.3	Reporte de debilidades de seguridad de la infonnación	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.16.1.5	Respuesta a incidentes de seguridad de la infonnación	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.16.1.7	Recolección de evidencia	Aplica	-	Existente	-	-	x	-	Implementación al 100%
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	**A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio**									
	A.17.1 Continuidad de seguridad de la información									
	A.17.1.1	Planificación de continuidad de seguridad de la información	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.17.1.2	Implementación de continuidad de seguridad de la información	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.17.2 Redundancias									
	A.17.2.1	Instalaciones de procesamiento de la información	Aplica	-	Existente	-	-	x	-	Implementación al 100%
18 Cumplimiento	**A.18 Cumplimiento**									
	A.18.1 Cumplimiento con requisitos legales y contractuales									
	A.18.1.1	Identificación de requisitos contractuales y de legislación aplicables	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.18.1.2	Derechos de propiedad intelectual	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.18.1.3	Protección de registros de la organización	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.18.1.4	Privacidad y protección de datos personales	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.18.1.5	Regulación de controles criptográficos	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.18.2 Revisiones de seguridad de la información									
	A.18.2.1	Revisión independiente de la seguridad de la información	Aplica	-	No existente	-	-	x	-	-
	A.18.2.2	Cumplimiento de políticas y normas de seguridad	Aplica	-	Existente	-	-	x	-	Implementación al 100%
	A.18.2.3	Revisión del cumplimiento técnico	Aplica	-	Existente	-	-	x	-	Implementación al 100%

Políticas implementadas	
No existente	12
Existente	102
Total	**114**

Tesis publicada con autorización del autor
No olvide citar esta tesis