UNIVERSIDAD AMAZÓNICA DE PANDO
ÁREA DE CIENCIAS Y TECNOLOGÍA
CARRERA DE INGENIERÍA DE SISTEMAS

TESIS DE GRADO

PARA OPTAR POR EL TITULO DE LICENCIATURA EN INGENIERÍA DE SISTEMAS

"DISEÑO DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE INFORMACION PARA EL SISTEMA SIRINGUERO"

Postulante	:	Univ. Marcos Roman Rojas Choque
Tutor Colectivo	:	Ing. Juan Carlos Gallardo Jiménez
Asesor	:	Ing. José Edgar Balderrama Méndez

Cobija – Pando - Bolivia

2014

AGRADECIEMIENTOS:

A todas aquellas personas que han formado parte del desarrollo de la presente Tesis les hago llegar mis más sentidos respetos con la humildad que se me caracteriza, de tal forma agradezco a la Universidad Amazónica de Pando por haber sido como mi segundo hogar en el transcurso de la formación como universitario, brindándome conocimiento y experiencias para el máximo desenvolvimiento en la sociedad y así coadyuvar al desarrollo del progreso del departamento de Pando, al plantel docente el cual me ha brindado el conocimiento básico que toda persona se necesita para iniciar un nuevo y propio camino que con esmero, sacrificio y humildad de seguro trazare para llevar en alto el prestigio de la Universidad Amazónica de Pando.

“La dependencia hace que una persona no descubra el don que tiene”
Marcos R. Rojas Ch.

DEDICATORIA:

La presente Tesis de Grado, es el fruto del apoyo sentimental emitido por mis padres Jorge Rojas Salgueiro y Martha Beatriz Choque de Rojas quienes han sido la motivación principal, para el cumplimiento de uno de mis objetivos, a mi sobrina Teisha Escarlet Azurduy Rojas que desde el momento que llego a mi vida, me enseño a valorar las cosas que hago y hacerme notar que la vida es una sonrisa a mamá y papá, también a mis hermanos Jorge Valentín Rojas Choque Yarmila Lisset Rojas Choque pues ellos han sido el punto de referencia más valioso y un gran ejemplo a seguir, pues de ellos aprendí hacer luchador .

RESUMEN:

La utilización de controles que permitan proporcionar mayor seguridad a la información, con la cual trabajan los sistemas de información son muy necesarias y útiles, de tal forma que para ello se siguen y establecen una serie de procesos definidos en los Sistemas de Gestión de la Seguridad en la Información, cuyo eje troncal consiste en la aplicación de metodologías para realizar el análisis de riesgos y así establecer salvaguardas para poder disminuir el riesgo total, a uno aceptable para la entidad, el cual se contemplara para posteriores estudios en bienestar de la seguridad de la información que emplea la Institución.

De tal forma se realiza esta investigación como aporte a la Dirección de Información Académica perteneciente a la Universidad Amazónica de Pando (U.A.P) en la cual se realizó el trabajo de campo correspondiente, acorde a metodologías de investigación y normas establecidas con relación a la gestión de seguridad en la información.

La Tesis de Grado consiste en realizar el diseño de un Sistema de Gestión de la Seguridad de la Información para identificar y salvaguardar el nivel de seguridad que contempla el Sistema Académico Siringuero de la Universidad Amazónica de Pando U.A.P. De tal forma se identificó el problema de **gestión en la seguridad de la información del Sistema Académico Siringuero**. Especificando también los objetivos específicos y los alcances que tendrá el proyecto de grado en su desarrollo y ejecución.

Obteniendo como resultados significativos, en base a la Tesis de Grado "Diseño de un Sistema de Gestión de Seguridad en la Información para el Sistema Siringuero", cuyo problema identificado fue: **¿Cómo mejorar la seguridad en la gestión de la información del Sistema Académico Siringuero con normas ISO 27000?** Especificando también los objetivos específicos y los alcances que tendrá la tesis en su desarrollo y ejecución.

Palabras Claves:
S.G.S.I (Sistemas de Gestión en la Seguridad de la Información).
A.AR.R (Análisis y Gestión de Riesgos).

INDICE

1.1. ANTECEDENTES: 1

1.2. DESCRIPCIÓN DEL PROBLEMA: 1

1.3. OBJETIVOS: 2

1.3.1.1. Objetivo general: 2

1.3.2. Objetivos específicos: 2

1.4. HIPOTESIS: 3

1.5. ALCANCES: 3

2.1. MARCO CONTEXTUAL: 5

2.2. MARCO NORMATIVO: 6

2.2.1. Instituto Boliviano de Normalización y Calidad (IBNORCA): 6

2.3. MARCO TEMÁTICO: 8

2.3.1. Sistemas de Gestión: 8

2.3.2. Seguridad de Información: 8

2.3.2.1. Confidencialidad: 8

2.3.2.2. Integridad: 8

2.3.2.3. Disponibilidad: 8

2.3.2.4. Trazabilidad: 9

2.3.2.5. Autenticidad: 9

2.3.3. Sistema de Gestión de la seguridad de información: 9

2.3.4. Análisis y Gestión de Riesgos: 9

2.3.5. MAGERIT: 10

2.3.6. Activos: 11

2.3.7. Amenaza: 11

2.3.8. Vulnerabilidad: 11

2.3.9. Impacto: 12

2.3.10. Frecuencia/probabilidad: 12

2.3.11. Riesgo: 12

2.3.12. Salvaguardas: 12

2.3.13. Política de Seguridad de Información: 13

2.3.14. Norma ISO/IEC: 13

2.3.15. Etapas de desarrollo de las normas ISO: 14

2.3.16. Modelo PDCA: 15

2.3.17. Modelos de madurez: 15

2.3.18. Modelos de madurez de la seguridad de la información: 16
2.3.18.1. NIST-CSEAT: 16
2.3.18.2. CITI-ISEM: 16
2.3.18.3. COBIT: 17
2.3.18.4. ISM3: 17
2.3.18.5. SSE-CMM: 17
2.3.18.6. CERT-CSO: 18
3.1. Sistema de hipótesis: 20
3.2. Tipo de investigación: 20
3.3. Método de Muestreo: 21
3.4. Tipo de Muestreo: 21
3.5. Universo y Muestra: 22
3.5.1. Universo: 22
3.5.2. Muestra: 22
3.6. Técnicas de Reelección de la Información: 22
3.6.1. Entrevista: 23
3.6.2. Encuesta: 23
3.7. Instrumentos de recolección de datos: 23
3.8. Forma en que se analizaran e interpretan los resultados: 24
3.8.1. Preguntas: 24
3.8.2. Objetivo: 24
3.8.3. Cuadro de Resultados: 24
3.8.4. Representación Gráfica: 24
3.8.5. Interpretación: 24
3.9. Capitulado Tentativo: 25
3.10. Fases de un Sistema de Gestión en Seguridad de la Información (SGSI): 26
3.11. Políticas de Seguridad de Información: 29
3.11.1. Etapas de la aplicación de Políticas de Seguridad de la Información: 29
3.11.1.1. Creación: 29
3.11.1.2. Revisión: 30
3.11.1.3. Aprobación: 31
3.11.1.4. Comunicación: 31
3.11.1.5. Cumplimiento: 31
3.11.1.6. Excepciones: 32
3.11.1.7. Concienciación: 32
3.11.1.8. Monitoreo: 33
3.11.1.9. Garantía de cumplimiento: 33
3.11.1.10. Mantenimiento: 34
3.11.1.11. Retiro: 34
3.11.2. Prácticas recomendadas para escribir una política: 35
4.1. Análisis de la información obtenida: *38*
4.1.1. Servicio de Tramitación: 38
4.1.2. Servicio de archivo central: 38
4.1.3. Equipamiento informático: 39

4.1.4. Comunicaciones: 39
4.1.5. Seguridad física: 40
4.2. Dependencia de activos: 40
4.3. Valoración de Activos: 43
4.4. Caracterización de las amenazas: 46
4.5. Estimación de impacto y riesgo: 53
4.5.1. Impacto Acumulado: 54
4.5.2. Riesgo Acumulado: 55
4.5.3. Impacto repercutido: 56
4.5.4. Caracterización de las salvaguardas: 58
4.6. Estimación del estado de riesgo: 63
4.7. Gestión de riesgos: 66
4.7.1. Toma de decisiones: 66
4.8. Plan de seguridad: 67
4.9. Evolución de los indicadores de impacto y riesgo: 68
4.9.1. Impacto acumulado: 69
4.9.2. Riesgo acumulado: 69
4.9.3. Impacto repercutido: 70
4.9.4. Riesgo repercutido: 70
4.10. Diseño de las políticas de seguridad: 71
4.10.1. Políticas para el dominio de redes: 71
4.10.2. Políticas para el dominio de hardware: 74
4.10.3. Políticas para el dominio de software: 76
4.10.4. Políticas para el dominio de datos: 78
4.10.5. Políticas para el dominio de sistema eléctrico: 79
4.10.6. Políticas para el dominio de talento humano: 80
5.1. CONCLUSIONES: 83
5.2. RECOMENDACIONES: 83
Bibliografía: 84
ANEXOS 85
ANEXO A 86
ANEXO B 91

ANEXO C..... 94

INDICE DE GRAFICOS

GRAFICO 1: IBNORCA 6
GRAFICO 2: IBNORCA en Bolivia 7
GRAFICO 3: Niveles de Normas 7
GRAFICO 4: Análisis de Riesgos. 10
GRAFICO 5. Sistemas de Gestión 14
GRAFICO 6: Mejora Continua PDCA 15
GRAFICO 7: Fases de un SGSI 26
GRAFICO 8: Actividades de Implantación de un SGSI 27
GRAFICO 9: ETAPAS EN EL DESARROLLO DE POLITICAS 29
GRAFICO 10: Identificación de Activos 41
GRAFICO 11: Dependencia de Activos 42
GRAFICO 12: Criterio de valoración 44
GRAFICO 13 Impacto Acumulado 54
GRAFICO 14: Riesgo Acumulado 55
GRAFICO 15: Impacto Repercutido 57
GRAFICO 16: Riesgo Repercutido 58
GRAFICO 17: Impacto Acumulado Residual: 64
GRAFICO 18: Riesgo Acumulado Residual: 64
GRAFICO 19: Impacto Repercutido Residual 65
GRAFICO 20: Riesgo Repercutido Residual 66
GRAFICO 21: Impacto Acumulado 69
GRAFICO 22: Riesgo acumulado 69
GRAFICO 23: Impacto Repercutido 70
GRAFICO 24: Riesgo repercutido 70

INDICE DE TABLAS

TABLA 1: Universo 22
TABLA 2: Actividades de un SGSI 28
Tabla 3: Modelo de responsabilidad por etapa para cada tipo de política 36
TABLA 4: Dependencia de Activos 42
TABLA 5: Valoración de activos 43
TABLA 6: CRITERIO DE VALORACION 45
TABLA 7: Valor Acumulado 46
TABLA 8: Amenazas Expedientes en Curso 47
TABLA 9: Amenazas Tramitación Presencial 48
TABLA 10: Amenazas Archivo Histórico Central 48
TABLA 11: Amenazas Tramitación de Expedientes 49
TABLA 12: Amenazas Puestos de Trabajo 50
TABLA 13: Amenazas Servidor 51
TABLA 14: Amenazas Firewall 52
TABLA 15: Amenazas Red Local 52
TABLA 16: Amenazas Oficinas 53
TABLA 17: Amenazas Sala de Equipos 53
TABLA 18: Interpretación de valores: 54
TABLA 19: Interpretación de Valores 55
TABLA 20: Interpretacion Nivel de Criticidad 56
TABLA 21: Niveles de Seguridad 67

CAPITULO I

1. MARCO INTRODUCTORIO

1.1.ANTECEDENTES:

Hoy la administración automatizada de la información que circula a través de diferentes procesos, el cual es imprescindible en las entidades, tales como ser: Bancos, hospitales, colegios, universidades, entre otros, ya que estos hacen la utilización de sistemas de información para la ejecución de los procesos que realizan. Logrando así manejar grandes cantidades de información valiosa, a través de medios tecnológicos, **Tecnologías de Información y Comunicación** (Tics), permitiendo así la administración de la información de una manera más eficiente y eficaz, así como las TIC's ofrecen grandes ventajas en la administración de información, también presentan algunas desventajas o inconvenientes en cuanto a la seguridad(riesgos inherentes a los medios tecnológicos) es de tal forma que en estos casos los **Sistema de Gestión de la Seguridad de Información** (SGSI) juegan un papel importante puesto que permiten identificar a través de métodos, procesos y estándares de seguridad los diferentes riesgos y vulnerabilidades a las que están expuestas los sistemas de información, así como también gestionar los riegos y vulnerabilidades para garantizar la continuidad del negocio.

De tal forma existiendo otros estudios (aportes) realizados sobre la gestión de seguridad de información como ser "**Sistema de gestión de seguridad de información para una institución financiera**", elaborado por **Moisés Antonio Villena Aguilar,** mediante el cual da a conocer la aplicación de modelos de madures, herramientas y metodologías que sean aplicado para poder realizar un correcta gestión de seguridad de los sistemas de información de las entidades financieras del país hermano Perú. (Villena Aguilar, Sistema de Gestion de Seguridad de Informacion para una Institucion Financiera, 2006).

1.2. DESCRIPCIÓN DEL PROBLEMA:

El "Sistema Académico Siringuero", perteneciente a la Universidad Amazónica de Pando. Cumple un gran desempeño en la ejecución de procesos y tareas concernientes en la administración académica (Matriculación de universitarios antiguos/nuevos, matriculación de cursos de verano, matriculación de exámenes de mesa, entre otros), generando así una gran

cantidad de información sensible de mucha importancia para la UAP, motivo por el cual este activo (información académico) debe ser protegido.

La información que se administra en el "Sistema Académico Siringuero" carece de métodos, técnicas y mecanismos seguridad con relación a la Gestión de Riesgos.
De acuerdo a la descripción de las causas consideradas como problemas que tiene la organización, se plantea el siguiente problema principal:

¿Cómo mejorar la seguridad en la gestión de la información del Sistema Académico Siringuero con normas ISO 27000?

Por lo mencionado anteriormente este problema genera efectos negativos como ser:

Inadecuado seguimiento de amenazas a la información, así mismo el incremento del nivel de pérdida de información, en la cual se puede llegar a dar el tráfico de la información ilícita, surgiendo ataques constantes dirigidos a la información (activo) con la que trabaja el sistema.

1.3. OBJETIVOS:

1.3.1.1. Objetivo general:

Diseñar políticas de seguridad en la gestión de la Información basado en normas ISO 27000 para el Sistema Académico Siringuero de la Universidad Amazónica de Pando.

1.3.2. Objetivos específicos:

- ✓ Analizar la gestión de seguridad de la información de Sistema Académico Siringuero.
- ✓ Realizar la gestión de riesgo en relación a las amenazas y vulnerabilidades identificadas.
- ✓ Determinar el impacto del Riesgo obtenido con relación a las amenazas y vulnerabilidades.
- ✓ Establecer controles para mitigar el riesgo con relación a los datos obtenidos.

1.4. HIPOTESIS:

El Sistema Académico Siringuero de la Universidad Amazónica de Pando (U.A.P), posee un nivel de seguridad en la gestión de la información no acorde a la aplicación de normas ISO.

1.5. ALCANCES:

Con el desarrollo de la presente Tesis de grado se realizara un estudio de gestión de seguridad de la información al Sistema Siringuero de la Universidad Amazónica de Pando, realizando un estricto análisis de riesgos de la institución, con relación al "Sistema Siringuero", de tal forma que se ha llegado a tomar como eje central de la investigación, la Dirección Información Académica (DIA), la cual está relacionada de forma directa con el procesamiento de información que realiza el sistema, en sus diferentes funcionalidades, con relación al flujo de datos.

CAPITULO II

2. MARCO TEÓRICO

2.1. MARCO CONTEXTUAL:

La Universidad Amazónica de Pando, se encuentra ubicada en la ciudad de Cobija, capital del Departamento Pando, en el extremo norte del territorio nacional, en plena región amazónica, su lema es: "La preservación de la Amazonía es parte esencial de la subsistencia, de la vida, del progreso y desarrollo de la bella tierra pandina". Tiene como **Misión** "Formar profesionales idóneos, capaces de crear, adaptar y transformar la Educación en función del desarrollo sostenible y mejoramiento de la calidad de vida de la población".

Constituyéndose en Centro de Referencia Regional en la formación pedagógica, la investigación científica e interacción social, fortaleciendo la identidad cultural y la soberanía nacional. La Universidad, nació con el nombre de **Universidad Técnica de Pando**, sin embargo, por contar desde su inicio con carreras a nivel Licenciatura y por acuerdo del Comité de Funcionamiento de la Universidad, se denominó: "**Universidad Amazónica de Pando**", comenzando su funcionamiento el 3 de Diciembre de 1993, con las carreras de Biología y Enfermería a nivel de Licenciatura.

La modernización de la gestión académica en la U.A.P., se inicia a partir de la creación de la Dirección de Información Académica D.I.A. y el departamento de procesamiento de datos D.P.D.

A partir de abril del 2000 la UAP tuvo un logro muy importante, al ser la primera institución en Pando al proporcionar internet On-Line a la comunidad universitaria, continuando con los grandes avances de la UAP, en septiembre del 2001 la carrera de Ingeniería Informática realizo una página WEB del Congreso Nacional de Ciencias de la Computación (CCBol), el cual se realizó en el departamento de Pando, llevado a cabo en la Universidad Amazónica de Pando, por la carrera de Ingeniería Informática, otro gran avance en cuanto a la aplicación de las nuevas TIC's en la U.A.P, fue la implementación el Sistema de Información de Gestión Académica **SIGA-COIMATA**, en enero del 2004 desarrollado bajo la plataforma de software libre, adquirida mediante convenio suscrito con el Ministerio de Educación de Bolivia-Viceministerio de Educación Superior Ciencia y Tecnología (VESCYT), para la cual se tuvo que realizar el diseño de la página WEB de la UAP, sistema mediante el cual tuvo una serie de

modificaciones para satisfacer la demanda que toda universidad el crecimiento requiere, de tal forma se llegó a realizar la mejora del antiguo sistema **S.I.G.A.-COIMATA** dando como resultado al "**Sistema de Información de Gestión Académica" S.I.G.A**, fortaleciendo los procesos académicos con la implementación de nuevos módulos, actualmente la última modificación del sistema que permite administrar y gestionar la información de la comunidad universitaria se denomina "**Sistema Académico Siringuero**".

2.2. MARCO NORMATIVO:

2.2.1. Instituto Boliviano de Normalización y Calidad (IBNORCA):

Es el Instituto Boliviano de Normalización y Calidad (**IBNORCA**) que contempla como sus funciones básicas la Normalización Técnica y la Certificación, dos pilares fundamentales de la calidad. Fue creada el 29 de abril de 1993 según el decreto supremo Nº 23489.

El Decreto supremo N° 23489 promueve su creación, otorgándole sus funciones fundamentales:

- ✓ Normalización técnica
- ✓ Certificación de la calidad

Funciona desde el 5 mayo de 1993: Asociación privada sin fines de lucro.

El Decreto supremo N° 24498 creación del Sistema NMAC, ratifica su competencia.

GRAFICO 1: IBNORCA
FUENTE: Instituto Boliviano de normalización y Calidad (IBNORCA)

El Instituto Boliviano de Normalización y Calidad se encuentra desplegado en la gran parte de nuestro territorio Boliviano.

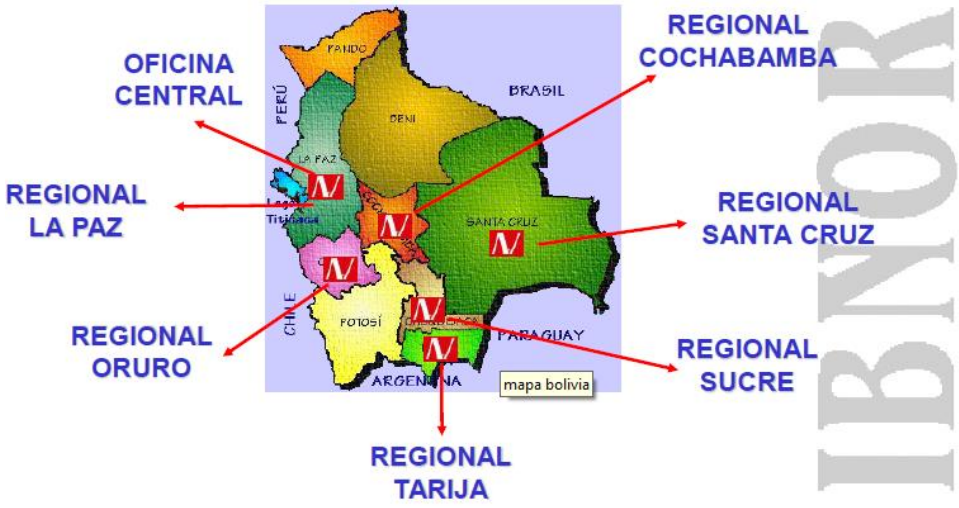


GRAFICO 2: IBNORCA en Bolivia
FUENTE: Instituto Boliviano de normalización y Calidad (IBNORCA)

2.2.2. Normalización que aplica Instituto Boliviano de Normalización y Calidad (IBNORCA):

Actividad que establece, con relación a problemas reales o potenciales, soluciones para aplicaciones repetitivas y comunes, con el objeto de lograr un grado óptimo de orden en un contexto dado.

En particular consiste en la elaboración, la publicación y la aplicación de normas.

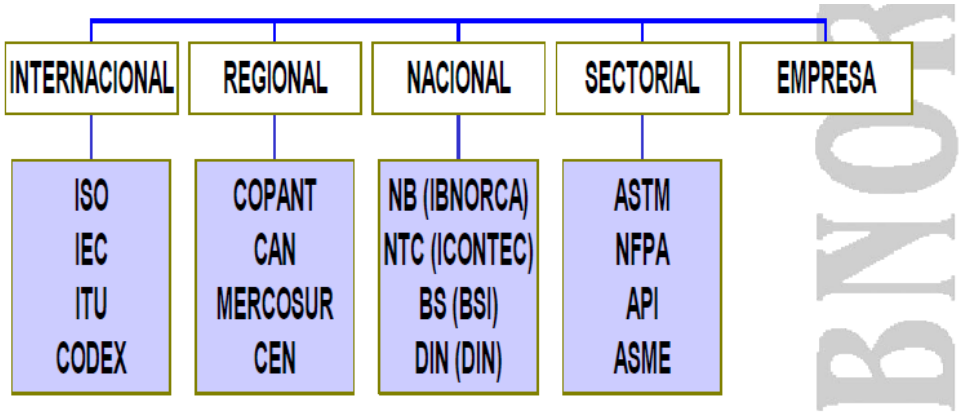


GRAFICO 3: Niveles de Normas
FUENTE: Instituto Boliviano de normalización y Calidad (IBNORCA)

2.3. MARCO TEMÁTICO:

2.3.1. Sistemas de Gestión:

Según (Merino Bada & Cañizares Sales) define como un marco de funcionamiento de una organización en el que se integran tanto la misión, visión, valores, objetivos principales y secundarios de la organización, como las políticas, procedimientos, registros e indicadores, que dan forma al sistema.

2.3.2. Seguridad de Información:

La Seguridad de Información tiene como fin la protección de la información y de los Sistemas de Información de una amplia variedad de amenazas como por ejemplo: acceso, uso, divulgación, interrupción o destrucción no autorizada. Su protección tiene como objeto asegurar la continuidad del negocio, minimizar los riesgos (combinación de la probabilidad de ocurrencia de un evento y sus consecuencias) y maximizar el retorno de la inversión y las oportunidades del negocio.

El fin de la Seguridad de la Información es la de proteger la Confidencialidad, Integridad y Disponibilidad de la Información.
Para (Merino Bada & Cañizares Sales) la seguridad de información consta de las Siguientes dimensiones de la Seguridad:

2.3.2.1. Confidencialidad:

Es la garantía de que la información no es conocida por personas, organizaciones o procesos que no disponen de la autorización necesaria.

2.3.2.2. Integridad:

Es la garantía de que la información no sea transformada ni modificada de forma no autorizada durante su procesamiento, transporte o almacenamiento.

2.3.2.3. Disponibilidad:

Es la garantía de que la información es accesible en el momento en el que los usuarios autorizados tengan la necesidad de acceder a ella.

2.3.2.4. Trazabilidad:

Es la garantía de que en todo momento se podrá determinar quién hizo que y en qué momento lo hizo.

2.3.2.5. Autenticidad:

Es la garantía de la identidad del usuario que origina una información. Permite conocer con certeza quien envía o genera una información específica.

2.3.3. Sistema de Gestión de la seguridad de información:

Parte del Sistema de gestión global, basada en un enfoque dirigida hacia los riesgos de una organización, negocio (entidad), cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

Par (Merino Bada & Cañizares Sales) es la estructuración del fortalecimiento de los procesos (activos), aplicando técnicas y procedimientos que le permitan garantizar una mejora continua en cuanto a la integridad de los activos de una determinada entidad.
Para la gestión de la Seguridad de la Información en una organización estos se basan en el concepto de mejora continua.

2.3.4. Análisis y Gestión de Riesgos:

En el campo de las Tecnologías de la Información, destacan las normas y metodologías de Análisis y Gestión del Riesgo mostradas a continuación, fundamentalmente patrocinadas por los organismos que se mencionan respectivamente:

- ✓ ***ISO 27005:2008*** (IEC - Internacional).
- ✓ ***UNE 71504:2008*** (AENOR - España).
- ✓ ***MAGERIT*** (Ministerio de Administraciones Públicas - España).
- ✓ ***OCTAVE*** (SEI Carnegie Mellon University - USA).
- ✓ ***CRAMM*** (Siemens Insight Consulting - UK).
- ✓ ***EBIOS*** (DCSSI - Francia).
- ✓ ***IT Baseline Protection Manual*** (BSI - Alemania).

- ✓ ***NIST SP800-30*** (NIST - USA).
- ✓ Otras: ***MÉHARI***, ***COBRA***, ***ISAAC***, ***RA2***, etc.

2.3.5. MAGERIT:

Según (Merino Bada & Cañizares Sales)Magerit está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los usuarios; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

Interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, Magerit les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con Magerit se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

En general, las metodologías mencionadas anteriormente parten de conceptos similares.

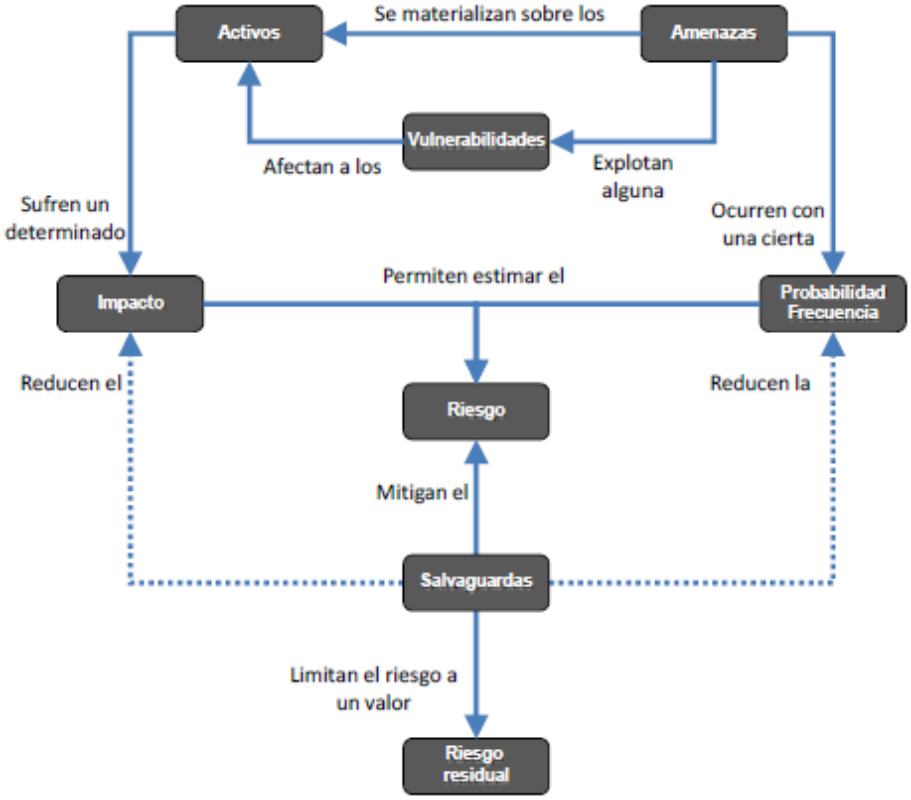


GRAFICO 4: Análisis de Riesgos.

FUENTE: Elaboración propia

2.3.6. Activos:

Según (Lopez Cuenca, 2012) Es aquel que engloba no sólo el Hardware, Redes y Software (que serían los más evidentes), sino también todos aquellos que los soportan, utilizan o afectan en alguna medida, como por ejemplo: el personal (administradores, usuarios, etc.), infraestructuras (edificios o suministros) u otros más intangibles como la propia información, la imagen o la reputación.

En cualquier caso, los activos son relevantes en función del valor que tengan para la Organización. Habitualmente, los activos mantienen relaciones unos con otros, creándose una jerarquía de dependencias. Estas dependencias influyen, determinando el valor de un activo, en función de los activos a los que asiste.

Existen dos métodos para estimar el valor de un activo:

Cuantitativo:

En el que se asigna un valor económico en función de su precio, coste de reposición u otros factores que influyan en ello.

Cualitativo:

En el que el valor oscila dentro de una escala limitada y progresiva, utilizando valores como “Bajo”, “Medio” o “Alto”, o cifras en un conjunto entre dos límites definidos.

2.3.7. Amenaza:

(INTECO, 2008), Estableció que una amenaza es una circunstancia o evento con la capacidad de causar daño a un sistema, entendiendo como daño una forma de destrucción, revelación o modificación de datos.

2.3.8. Vulnerabilidad:

(INTECO, 2008), Define vulnerabilidad como una debilidad que puede ser ‘activada’ de forma accidental o intencionadamente. Es un factor de riesgo interno de un elemento expuesto a una amenaza de ser susceptible a sufrir un daño y de encontrar dificultades en recuperarse posteriormente.

2.3.9. Impacto:

Para (Lopez Cuenca, 2012)Es el resultado de que una amenaza se materialice sobre un activo, sacando provecho de una vulnerabilidad asociada a éste, y provocándole una determinada degradación o pérdida de su valor.

2.3.10. Frecuencia/probabilidad:

Según (Lopez Cuenca, 2012)La probabilidad es un indicador de posibilidad, que determina si una potencial vulnerabilidad puede acontecer a través del entorno de amenaza apropiado, mientras que en el caso de la frecuencia el indicador refleja el número de veces que se materializaría la amenaza por unidad de tiempo.

Estos indicadores pueden resultar más fácilmente estimables en ataques no deliberados (naturales, industriales) o basados en series históricas (análisis estadístico). Por el contrario resulta difícil de estimar en el caso de ataques deliberados, en sistemas o entornos nuevos y ante hechos abstractos.

En general, la estimación de la probabilidad/frecuencia introduce una cierta incertidumbre en detrimento de la credibilidad del análisis de riesgos.

2.3.11. Riesgo:

Según, (INTECO, 2008) Un riesgo de un proyecto es un evento o condición incierto que, si se produce, tendrá un efecto positivo o negativo sobre al menos un objetivo del proyecto, como tiempo, coste, alcance o calidad, es decir, cuando el objetivo de tiempo de un proyecto es cumplir con el cronograma acordado; cuando el objetivo de coste del proyecto es cumplir con el coste acordado, etc.

2.3.12. Salvaguardas:

Para (Lopez Cuenca, 2012)trata de las medidas de seguridad, procedimientos o mecanismos tecnológicos orientados a reducir el riesgo. Puede tratarse de medidas de previsión o de preparación, de disuasión, protección, detección, aislamiento, confrontación, recuperación, restauración, compensación, etc.

La implantación y la madurez de las salvaguardas disminuye el riesgo, bien reduciendo el impacto causado por una amenaza, o bien la probabilidad o frecuencia de su materialización.

Existen modelos como el CMMI (Capability Maturity Model ® Integration) que establecen niveles diferenciados, para representar la existencia y estado de madurez de una salvaguarda.

2.3.13. Política de Seguridad de Información:

Según (Gomes Fernandez & Alvarez, 2012) indica que la política de seguridad de la información es un subconjunto de la política del **SGSI** y que ambas pueden plasmarse en un único documento. Sobre la política de seguridad de la información se establecen pocas más cosas en la **ISO** 27001: que debe revisarse a intervalos planificados y cuando se producen cambios significativos en la organización y durante la revisión por la dirección, que debe servir como base para la mejora continua, que debe ser aprobada por dirección y que debe ser comunicada a todos los empleados y partes interesadas.

2.3.14. Norma ISO/IEC:

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrónica Internacional). Es la organización más grande del mundo en el desarrollo de normas desde 1947 hasta hoy, la ISO ha publicado más de 18500 normas internacionales que van desde las normas para los sectores como la agricultura y la construcción, pasando por ingeniería mecánica o los productos sanitarios, a los desarrollados más recientes como los que tienen que ver con la tecnología de la información.

El gran impacto que genero las normas ISO 9001 e ISO 14001 sobre prácticas de calidad y mejora en las organizaciones ha estimulado el desarrollo de otras normas ISO que se adaptan a determinados sectores.

- ✓ Automovilismo
- ✓ Energético
- ✓ Alimentación
- ✓ **Seguridad de la información**
- ✓ Seguridad de la cadena de suministro

- ✓ Educación
- ✓ Riesgo

2.3.15. Etapas de desarrollo de las normas ISO:

Las normas internacionales son desarrolladas por comités técnicos de ISO (TIC) y subcomités (SC) por un proceso de seis pasos:

- ➢ Etapa 1: fase preliminar
- ➢ Etapa 2: fase de propuesta
- ➢ Etapa 3: fase preparatoria
- ➢ Etapa 4: fase de comité
- ➢ Etapa 5: fase de consulta
- ➢ Etapa 6: fase de aprobación
- ➢ Etapa 6: fase de publicación

Hoy en día las organizaciones pueden llegar a tener implantados múltiples sistemas de gestión, como pueden ser:

- ✓ **ISO-9001**- Sistemas de Gestión de calidad.
- ✓ **ISO-14001**- Sistemas de Gestión Medioambiental.
- ✓ **ISO-22000**- Sistemas de Gestión de Seguridad Alimentaria.
- ✓ **ISO-27001**- Sistemas de Gestión de Seguridad de la Información.
- ✓ **ISO-28000**- Sistemas de Gestión de Seguridad de la Cadena de Suministro.
- ✓ **OHSAS18001**- Sistema de Gestión de Seguridad y Salud Laboral

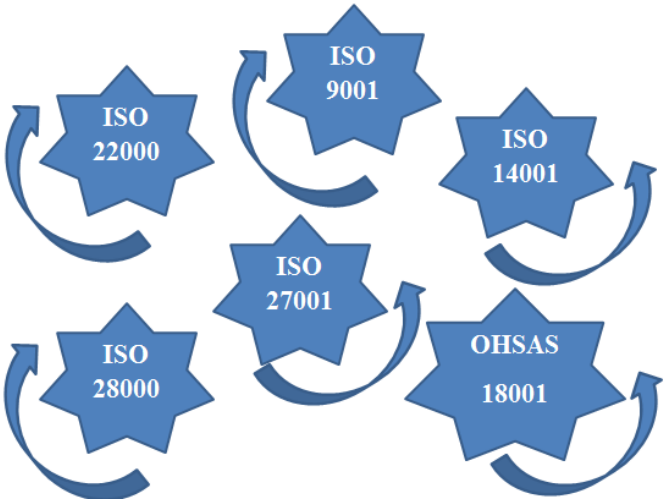


GRAFICO 5. Sistemas de Gestión
Fuente: Elaboración propia

2.3.16. Modelo PDCA:

Los sistemas de Gestión de la Seguridad de Información desarrollados según la norma ISO 27001, igual que muchos otros sistemas de gestión se basan en el concepto de mejora continua.

El "circulo de Deming" (Edwars Deming), también conocido como modelo o ciclo PDCA es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart.

Las Siglas PDCA son el acrónimo de Planificar, Hacer, Verificar, Actuar:

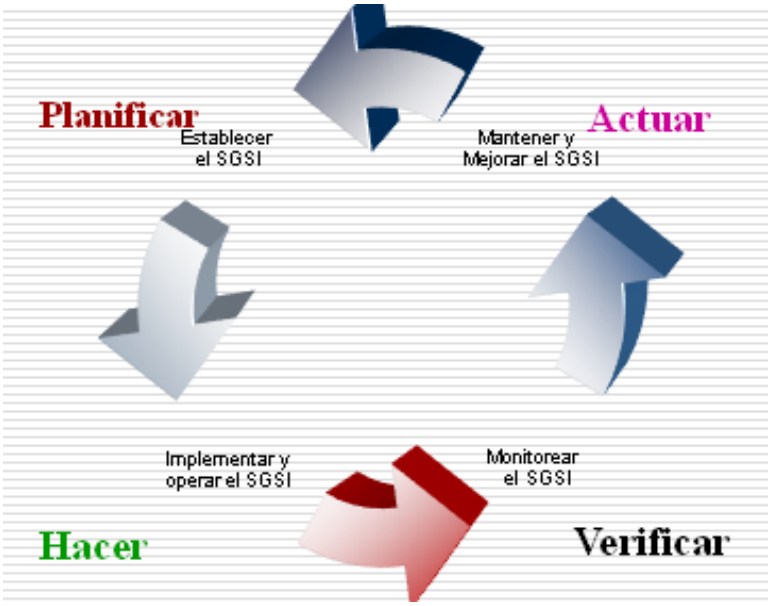


GRAFICO 6: Mejora Continua PDCA

FUENTE: Elaboración propia

2.3.17. Modelos de madurez:

Es un conjunto estructurado de elementos que describen el nivel de madurez de una organización en un aspecto determinado, que establece un orden claro, discreto y absoluto de valoración definiendo niveles o etapas de madurez lo que permite evaluar de forma explícita la evolución de la organización en dicho aspecto.

2.3.18. Modelos de madurez de la seguridad de la información:

Existen diferentes modelos de madures aplicables a la seguridad de la información entre los cuales se encuentran los siguientes:

- ✓ **NIST-CSEAT**
- ✓ **CITI-ISEM**
- ✓ **COBIT Msturity Model**
- ✓ **ISM3**
- ✓ **SSE-CMM**
- ✓ **CERT-CSO**

2.3.18.1. NIST-CSEAT:

El modelo **NIST-CSEAT (National Institute of Standards and Technology Computer Security Expert Assist Team)** Está orientado a la documentación y establece cinco niveles de madurez progresiva:

- ✓ **Política**
- ✓ **Procedimiento**
- ✓ **Implantación**
- ✓ **Prueba**
- ✓ **Integración**

2.3.18.2. CITI-ISEM:

El modelo de evaluación de la seguridad de la información de Citigroup (**CITI-ISEM**) Está orientado a la adaptación y concienciación de la organización y establece cinco niveles de madurez.

- ✓ **Autocomplacencia**
- ✓ **Reconocimiento**
- ✓ **Integración**
- ✓ **Prácticas comunes**
- ✓ **Mejora continua**

2.3.18.3. COBIT:

El modelo de madurez de COBIT está orientado a procesos y define a seis niveles de madurez:

- ✓ **Inexistente**
- ✓ **Inicial**
- ✓ **Repetible**
- ✓ **Definido**
- ✓ **Gestionado**
- ✓ **Optimizado**

2.3.18.4. ISM3:

El modelo ISM3 es un modelo de madurez orientado a procesos que facilita la mejora y alineación con las necesidades del negocio de los sistemas de gestión de la seguridad de organizaciones de cualquier tipo y tamaño. Y establece cinco niveles de madurez:

- ✓ **Nivel ISM3 0**
- ✓ **Nivel ISM3 1**
- ✓ **Nivel ISM3 2**
- ✓ **Nivel ISM3 3**
- ✓ **Nivel ISM3 4**

2.3.18.5. SSE-CMM:

El modelo SSE-CMM es un modelo de capacidad y madurez en la ingeniería de seguridad de sistemas, describe las características principales de los procesos de lo que debe disponer una organización para poder garantizar una adecuada seguridad de los sistemas. Y establece cinco niveles de madurez.

- ✓ **Realizado informalmente**
- ✓ **Planificado y perseguido**
- ✓ **Bien definido**
- ✓ **Controlado cuantitativamente**
- ✓ **Continuamente mejorado**

2.3.18.6. CERT-CSO:

El modelo CERT-CSO está orientado a la medición de la calidad relativa a niveles de documentación, centrado en la medición de la calidad relativa a niveles de documentación y establece cinco niveles de madurez progresiva.

- ✓ **Existente**
- ✓ **Repetible**
- ✓ **Persona designada**
- ✓ **Documentado**
- ✓ **Revisado y actualizado**

Que se miden usando cuatro niveles:

- **Inicial**
- **En desarrollo**
- **Establecido**
- **Gestionado**

CAPITULO III

3. MARCO METODOLÓGICO

3.1.Sistema de hipótesis:

VARIABLES	DEFINICION	DIMENCIONES	INDICADORES
Sistema de Información Académico Siringuero **DEPENDIENTE**	Se refiere a la automatización, organización, de los procesos que se dan en la institución.	**Confidencialidad** **Integridad** **Disponibilidad**	✓ Servicios ✓ Aplicaciones/Software ✓ Datos/Información ✓ Identificador de Usuarios ✓ Soporte Informático ✓ Instalaciones ✓ Equipos Informáticos ✓ Soportes Electrónicos ✓ Equipamiento Auxiliar ✓ Rede de comunicación
Gestión de Seguridad en la Información **INDEPENDIENTE**	Se refiere a la previsión y procedimientos necesarios para establecer y mantener la información (activo) segura para el cumplimiento de los objetivos de la Institución	**Análisis de riesgos** **Gestión de riesgos**	✓ Metodologías ✓ Salvaguardas

3.2.Tipo de investigación:

La obtención de la información necesaria para la presente investigación es realizada por medio de una INVESTIGACIÓN EMPIRICA: es basado en la evidencia. Teniendo esto en cuenta, mediante el cual se llega a trabajar con hipótesis que pueden comprobarse mediante la observación y los experimentos.

Obteniendo así resultados en base a la investigación basada en la experimentación o la observación (evidencias). Llegando a cabo a poner en prueba la hipótesis planteada.

Es por ello que para la realización de la Gestión de Seguridad de Información del Sistema Siringuero de la Universidad Amazónica de Pando (**UAP**), se ha tomado a bien hacerlo por este método de investigación ya que es el que se considera que satisface las necesidades de nuestra investigación.

La identificación del problema es realizada a través del uso de entrevistas y encuestas estructuradas dirigidas a la Dirección de Información Académica (**DIA**) para determinar las condiciones del desarrollo de la Gestión de Seguridad de la Información Todo esto con el fin de conocer y salvaguardar la información con la que trabaja el Sistema Siringuero de la Universidad Amazónica de Pando.

3.3.Método de Muestreo:

3.3.1. No Probabilístico:

Este método no es un tipo de muestreo riguroso y científico, dado que no todos los elementos de la población pueden formar parte de la muestra, se trata de seleccionar a los sujetos siguiendo determinados criterios procurando que la muestra sea representativa. Es decir, los elementos de la muestra son seleccionados por procedimientos al azar o con probabilidades conocidas de selección.

Se aplicara para el Director de Información Académica ya que siendo el responsable oficial de la Dirección de Información Académica de la Universidad Amazónica de Pando (U.A.P), es la persona indicada para proporcionar una considerable cantidad de información importante y necesaria para el desarrollo de la gestión de riesgos y también se aplicara para los reponles en las áreas de redes comunicación de datos, responsable del sistema, que pertenecen a la Dirección de Información Académica.

3.4.Tipo de Muestreo:

Para la investigación se a utilizado el siguiente tipo de muestreo:

3.4.1. Muestreo de Juicio:

El investigador toma la muestra seleccionando los elementos que a él le parecen representativos o típicos de la población, por lo que depende del criterio del investigador.

En este caso: se tomarán como muestra a los Responsables en las áreas de la Unidad de Sistemas de Información Académica de la Dirección de Información Académica (**DIA**).

3.5.Universo y Muestra:

3.5.1. Universo:

Es el conjunto de personas, cosas o fenómenos sujetos a investigación, que tienen algunas características definitivas. Ante la posibilidad de investigar el conjunto en su totalidad.

En este caso la investigación será realizada abarcando dos tipos de poblaciones que son: Los Responsables del Sistema y Los Operadores del Sistema.

TABLA 1: Universo

Responsables del Sistema y Operadores del Sistema	Cantidad de Personas
Director Dirección de Información Académica-DIA	1
Responsable de Sistemas Información Académica	1
Responsable de Redes Comunicación de Datos	1
Programadores	2
Funcionarios	3

FUENTE: Elaboración propia

3.5.2. Muestra:

Es una parte del universo, la cual debe tener las mismas características del universo en su totalidad ya que es representativa de este. Y se utiliza cuando no es conveniente considerar a todos los elementos que lo componen.

En éste caso no se realizará un estudio para la Muestra ya que a todas las personas tomadas en cuenta dentro del Universo se les realizará la encuesta.

3.6. Técnicas de Reelección de la Información:

Para la obtención de la información necesaria para conocer las necesidades que existen con relación al Sistema Siringuero de la Universidad Amazónica de Pando, se hará uso de los siguientes métodos de investigación:

3.6.1. Entrevista:

Es la comunicación establecida entre el investigador y el sujeto de estudio a fin de obtener respuestas verbales a las interrogantes planteadas sobre el problema propuesto.

3.6.2. Encuesta:

Este método consiste en obtener información de los sujetos de estudio, proporcionada por ellos mismos, sobre opiniones, actitud eso sugerencias.

Se han utilizado éstos métodos debido a que son los más conocidos, son de fácil aplicación y permiten obtener información concreta y directa de las personas involucradas.

3.7. Instrumentos de recolección de datos:

3.7.1. Cuestionario:

Es el método que utiliza un instrumento o formulario impreso, destinado a obtener respuestas sobre el problema en estudio y que el consultado llena por sí mismo.

El Cuestionario se les aplicará los responsables de la Dirección de Información Académica y contendrá preguntas abiertas y cerradas, para obtener información básica relacionada al tema de investigación.

3.7.2. Cédula de Entrevista:

La instrumentación consiste en el diseño de un documento elaborado para medir opiniones sobre eventos o hechos específicos. Se basa en una serie de preguntas. En una entrevista las respuestas a las cuestiones pueden escribirse en la cédula de entrevista o puede llevarse en una interacción cara a cara.

La cédula de entrevista se le realizará al Director de Información Académica y a los respectivos responsables de la Unidad de Sistemas de Información Académica, las preguntas serán abiertas, con el objetivo de obtener información relevante que ayude conocer la situación actual que sirva de parámetro para la Gestión de Seguridad de Información.

3.8. Forma en que se analizaran e interpretan los resultados:

Para elaborar el análisis e interpretación de los resultados obtenidos de las preguntas realizadas al Director de Información Académica y a los Responsables de la Unidad de Sistema de Información Académica de la Universidad Amazónica de Pando a través de la encuesta y las preguntas realizadas por medio de la entrevista, se desarrollaron el siguiente procedimiento:

3.8.1. Preguntas:

Las preguntas elaboradas para el Cuestionario, el cual va dirigido a la Unidad de Sistemas Información Académica, serán de forma cerrada y con respuestas simples y las preguntas que se realizarán por medio de la Entrevista serán de forma abierta para conocer la opinión del Director de Información Académica.

3.8.2. Objetivo:

La meta o finalidad de lo que se pretende alcanzar mediante la investigación, de ésta manera se podrá obtener una mayor claridad de lo que se está investigando.

3.8.3. Cuadro de Resultados:

Por medio de este cuadro se mostrará la información recopilada de las Encuestas para crear así una asimilación con los resultados obtenidos en la investigación.

3.8.4. Representación Gráfica:

Los resultados obtenidos por medio del Cuestionario realizado en la Dirección de Información Académica, se mostrarán de forma gráfica utilizando el Gráfico de Pastel, en el cual cada respuesta será representada por un color determinado, para su mejor comprensión.

3.8.5. Interpretación:

Esta será la forma mediante la cual se procurará expresar y plantear de forma clara la información obtenida por medio de la investigación.

3.9. Capitulado Tentativo:

En el apartado que se muestra a continuación se describe de forma tentativa el formato mediante el cual se ha desarrollado la tesis:

CAPITULO 1 FORMULACION DEL PROBLEMA

1.1. Antecedentes
1.2. Descripción del problema
1.3. Objetivos
1.3.1. Objetivo general
1.3.2. Objetivo específico
1.4. Hipótesis
1.5. Alcances

CAPITULO 2 MARCO REFERENCIAL

2.1. Marco Contextual
2.2. Marco Normativo
2.3. Marco Temático

CAPITULO 3 MARCO METODOLOGICO

3.1. Sistema de Hipótesis
3.2. Tipo de Investigación
3.3. Método de Muestreo
3.4. Tipo de Muestreo
3.5. Universo y Muestra
3.6. Técnicas de Recolección de Información
3.7 Instrumentos de Recolección de Información
3.8. Forma en que se Analizarán e Interpretarán los Resultados
3.9. Capitulado Tentativo
3.10. Fases de un Sistema de Gestión en la Seguridad de la Información.

CAPITULO 4 ANALISIS E INTERPRETACION DE RESULTADOS

4.1. Análisis de la información
4.2. Dependencia de Activos
4.3. Valoración de Activos
4.4. Caracterización de las Amenazas

4.5. Estimación de Impacto y Riesgo
4.6. Estimación del estado de Riesgo
4.7. Gestión de Riesgos
4.8. Plan de Seguridad
4.9. Evolución de los Indicadores de Impacto
4.10. Diseño de las Políticas de Seguridad

CAPITULO 5 CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones
5.2. Recomendaciones

Los Sistema de Gestión de Seguridad de la Información están compuestos por fases que a la misma vez están compuestos por actividades y los últimos por tareas.

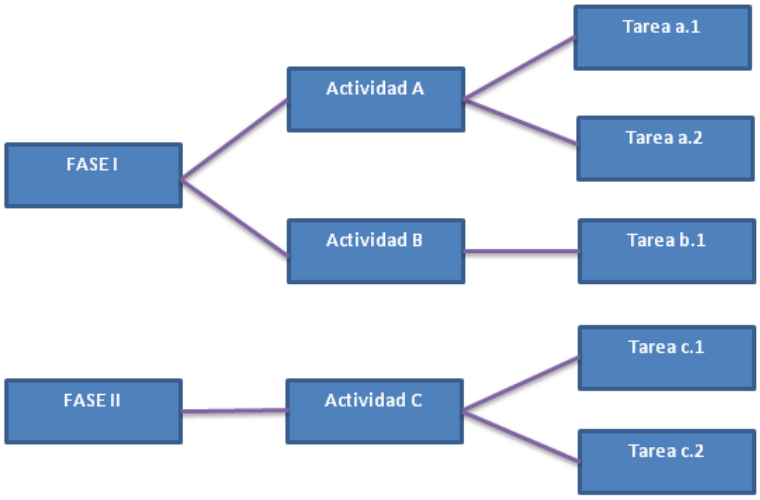


GRAFICO 7: Fases de un SGSI
FUENTE: Elaboración propia

3.10. Fases de un Sistema de Gestión en Seguridad de la Información (SGSI):

Las fases y actividades en las que se realiza el diseño del SGSI según el estándar ISO 27001 son:

Fase I:

Planificación del proyecto
Análisis de situación respecto de la norma (Gap Análisis)
Definición de la organización de la seguridad de la información

Fase II:

Análisis de riesgos
Gestión de riesgos
Elaboración de los planes y programas de acción

Fase III:

Elaboración de la documentación del sistema de gestión (PDCA)
Definición de las acciones para la comunicación, formación y concienciación
Evaluación del control operativo
Elaboración de los indicadores de gestión
Puesta de funcionamiento del sistema de gestión

Fase IV:

Rodaje y mejora del sistema de gestión
Indicadores
Auditoria interna

Fase V:

Acciones correctivas y de mejora del de gestión

Este cuadro muestra las actividades del desarrollo del SGSI:

GRAFICO 8: Actividades de Implantación de un SGSI
FUENTE: Elaboración propia

ACTIVIDAD	FASE	Diseño SGSI (1°Ciclo PDCA)	Mejora continua Ciclos PDCA
Planificación del proyecto	**FASE I**		
Análisis de situación respecto de la norma (Gap Análisis)	**FASE I**		
Definición de la organización de la seguridad de la Información	**FASE I**	**PLAN**	Revisión de la definición de la Organización de la seguridad de la Información
Análisis y gestión de riesgos	**FASE II**	**PLAN**	Nuevo análisis de riesgos
Elaboración de los planes y programas de acción	**FASE II**	**PLAN**	Revisión anteriores y nuevos planes y programas de seguridad
Elaboración de la documentación del sistema de gestión	**FASE III**		Revisión
Definición de las acciones para la comunicación, formación y concienciación.	**FASE III**	**DO**	Revisión
Evaluación del control operativo	**FASE III**	**DO**	Revisión
Elaboración de los indicadores de gestión	**FASE III**	**DO**	Revisión elaboración de nuevos
Puesta en funcionamiento del sistema de gestión	**FASE III**	**DO**	
Rodaje y mejora del sistema de gestión	**FASE IV**	**DO**	
Indicadores	**FASE IV**	**DO**	
Auditoria Interna	**FASE IV**	**CHECK**	
Acciones correctivas y de mejora del sistema de gestión	**FASE V**	**ACT-PLAN**	

TABLA 2: Actividades de un SGSI
FUENTE: Elaboración propia

3.11. Políticas de Seguridad de Información:

Para la aplicación de politicas de Seguridad de Informacion esta se encuentran compuestas por 4 fases y 11 etapas:

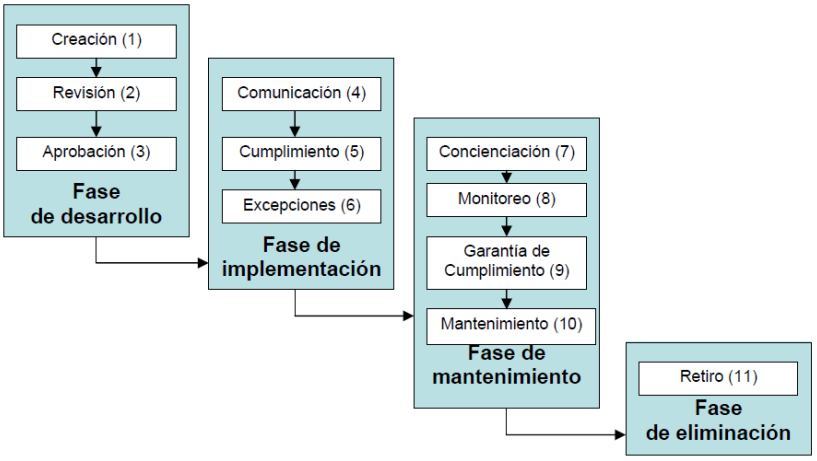


GRAFICO 9: ETAPAS EN EL DESARROLLO DE POLITICAS
FUENTE: UNC "Guía para elaboración de políticas de seguridad"

1. **Fase de desarrollo**: durante esta fase la política es creada, revisada y aprobada.
2. **Fase de implementación:** en esta fase la política es comunicada y acatada (o no cumplida por alguna excepción).
3. **Fase mantenimiento:** los usuarios deben ser cocientes de la importancia de la política, su cumplimiento debe ser monitoreado, se debe garantizar su cumplimiento y se le debe dar mantenimiento (actualizarla).
4. **Fase de eliminación:** la política se retira cuando no se requiera más.

3.11.1. Etapas de la aplicación de Políticas de Seguridad de la Información:

3.11.1.1. Creación:

Planificación, investigación, documentación y coordinación de la política.

La creación de una política implica identificar por qué se necesita la política, determinar el alcance y la aplicabilidad de la política, los roles y las responsabilidades inherentes a la aplicación de la política y garantizar la factibilidad de su implementación. La creación de una política también incluye la investigación para determinar los requerimientos organizacionales para desarrollar las políticas (es decir, que autoridades deben aprobarla, con quién se debe coordinar el desarrollo y estándares del formato de redacción), y la investigación de las mejores prácticas en la industria para su aplicabilidad a las necesidades organizacionales actuales. De esta etapa se tendrá como resultado la documentación de la política de acuerdo con los procedimientos y estándares de la universidad, al igual que la coordinación con entidades internas y externas que la política afectará, para obtener información y su aceptación. En general, la creación de una política es la función más fácil de entender en el ciclo de vida de desarrollo de una política.

3.11.1.2. Revisión:

Evaluación independiente de la política.

La revisión de la política es la segunda etapa en la fase de desarrollo del ciclo de vida. Una vez la documentación de la política ha sido creada y la coordinación inicial ha sido iniciada, esta debe ser remitida a un grupo (o un individuo) independiente para su evaluación antes de su aprobación final. Hay varios beneficios de la revisión independiente: una política más viable a través del escrutinio de individuos que tienen una perspectiva diferente o más vasta que la persona que redactó la política; apoyo más amplio para la política a través de un incremento en el número de involucrados; aumento de credibilidad en la política gracias a la información recibida de diferentes especialistas del grupo de revisión. Propio de esta etapa es la presentación de la política a los revisores, ya sea de manera formal o informal, exponiendo cualquier punto que puede ser importante para la revisión, explicando su objetivo, el contexto y los beneficios potenciales de la política y justificando por qué es necesaria. Como parte de esta función, se espera que el creador de la política recopile los comentarios y las recomendaciones para realizar cambios en la política y efectuar todos los ajustes y las revisiones necesarias para obtener una versión final de la política lista para la aprobación por las directivas.

3.11.1.3. Aprobación:

Obtener la aprobación de la política por parte de las directivas

El paso final en la fase de desarrollo de la política es la aprobación. El objetivo de esta etapa es obtener el apoyo de la administración de la universidad, a través de la firma de una persona ubicada en una posición de autoridad.

La aprobación permite iniciar la implementación de la política. Requiere que el proponente de la política haga una selección adecuada de la autoridad de aprobación, que coordine con dicho funcionario, presente las recomendaciones emitidas durante la etapa de revisión y haga el esfuerzo para que sea aceptada por la administración. Puede ocurrir que por incertidumbre de la autoridad de aprobación sea necesaria una aprobación temporal.

3.11.1.4. Comunicación:

Difundir la política

Una vez la política ha sido aprobada formalmente, se pasa a la fase de implementación. La comunicación de la política es la primera etapa que se realiza en esta fase. La política debe ser inicialmente difundida a los miembros de la comunidad universitaria o a quienes sean afectados directamente por la política (contratistas, proveedores, usuarios de cierto servicio,

etc.). Esta etapa implica determinar el alcance y el método inicial de distribución de la política (es posible que deban tenerse en cuenta factores como la ubicación geográfica, el idioma, la cultura y línea de mando que será utilizada para comunicar la política). Debe planificarse esta etapa con el fin de determinar los recursos necesarios y el enfoque que debe ser seguido para mejorar la visibilidad de la política.

3.11.1.5. Cumplimiento:

Implementar la política

La etapa de cumplimiento incluye actividades relacionadas con la ejecución de la política. Implica trabajar con otras personas de la universidad, vicerrectores, decanos, directores de departamento y los jefes de dependencias (de división o de sección) para interpretar cuál es la mejor manera de implementar la política en diversas situaciones y oficinas; asegurando que la política es entendida por aquellos que requieren implementarla, monitorearla, hacerle seguimiento, reportar regularmente su cumplimiento y medir el impacto inmediato de la política en las actividades operativas. Dentro de estas actividades está la elaboración de informes a la administración del estado de la implementación de la política.

3.11.1.6. Excepciones:

Gestionar las situaciones donde la implementación no es posible

Debido a problemas de coordinación, falta de personal y otros requerimientos operacionales, no todas las políticas pueden ser cumplidas de la manera que se pensó al comienzo. Por esto, cuando los casos lo ameriten, es probable que se requieran excepciones a la política para permitir a ciertas oficinas o personas el no cumplimiento de la política.

Debe establecerse un proceso para garantizar que las solicitudes de excepciones son registradas, seguidas, evaluadas, enviadas para aprobación o desaprobación, documentadas y vigiladas a través del periodo de tiempo establecido para la excepción. El proceso también debe permitir excepciones permanentes a la política al igual que la no aplicación temporal por circunstancias de corta duración.

3.11.1.7. Concienciación:

Garantiza la concienciación continuada de la política

La etapa de concienciación de la fase de mantenimiento comprende los esfuerzos continuos realizados para garantizar que las personas están conscientes de la política y buscan facilitar su cumplimiento. Esto es hecho al definir las necesidades de concienciación de los diversos grupos de audiencia dentro de la organización (directivos, jefes de dependencias, usuarios, etc.); en relación con la adherencia a la política,

determinar los métodos de concienciación más efectivos para cada grupo de audiencia (es decir, reuniones informativas, cursos de entrenamiento, mensajes de correo, etcétera); y desarrollo y difusión de material de concienciación (presentaciones, afiches, circulares, etc.). La etapa de concienciación también incluye esfuerzos para integrar el cumplimiento de la política y retroalimentación sobre el control realizado para su cumplimiento. La tarea final es medir la concienciación de los miembros de la comunidad universitaria con la política y ajustar los esfuerzos.

3.11.1.8. Monitoreo:

Seguimiento y reporte del cumplimiento de la política

Durante la fase de mantenimiento, la etapa de monitoreo es realizada para seguir y reportar la efectividad de los esfuerzos en el cumplimiento de la política. Esta información se obtiene de la observación de los docentes, estudiantes, empleados y los cargos de supervisión, mediante auditorias formales, evaluaciones, inspecciones, revisiones y análisis de los reportes de contravenciones y de las actividades realizadas en respuesta a los incidentes.

Esta etapa incluye actividades continuas para monitorear el cumplimiento o no de la política a través de métodos formales e informales y el reporte de las deficiencias encontradas a las autoridades apropiadas.

3.11.1.9. Garantía de cumplimiento:

Afrontar las contravenciones de la política

La etapa de garantía de cumplimiento de las políticas incluye las respuestas de la administración a actos u omisiones que tengan como resultado contravenciones de la política con el fin de prevenir que sigan ocurriendo. Esto significa que una vez una contravención sea identificada, la acción correctiva debe ser determinada y aplicada a los procesos (revisión del proceso y mejoramiento), a la tecnología (actualización) y a las personas (acción disciplinaria) involucrados en la contravención con el fin de reducir la probabilidad de que vuelva a ocurrir. Se recomienda incluir información sobre las

acciones correctivas adelantadas para garantizar el cumplimiento en la etapa de concienciación.

3.11.1.10. Mantenimiento:

Asegurar que la política esté actualizada

La etapa de mantenimiento está relacionada con el proceso de garantizar la vigencia y la integridad de la política. Esto incluye hacer seguimiento a las tendencias de cambios (cambios en la tecnología, en los procesos, en las personas, en la organización, en el enfoque del negocio, etcétera) que puede afectar la política; recomendando y coordinando modificaciones resultado de estos cambios, documentándolos en la política y registrando las actividades de cambio. Esta etapa también garantiza la disponibilidad continuada de la política para todas las partes afectadas por ella, al igual que el mantenimiento de la integridad de la política a través de un control de versiones efectivo. Cuando se requieran cambios a la política, las etapas realizadas antes deben ser re-visitadas, en particular las etapas de **revisión, aprobación, comunicación y garantía de cumplimiento**.

3.11.1.11. Retiro:

Prescindir de la política cuando no se necesite más

Después que la política ha cumplido con su finalidad y no es necesaria (por ejemplo, la empresa cambió la tecnología a la cual aplicaba o se creó una nueva política que la reemplazó) entonces debe ser retirada. La etapa de retiro corresponde a la fase de eliminación del ciclo de vida de la política, y es la etapa final del ciclo. Esta función implica retirar una política superflua del inventario de políticas activas para evitar confusión, archivarla para futuras referencias y documentar la información sobre la decisión de retirar la política (es decir, la justificación, quién autorizó, la fecha, etcétera).

Estas cuatro fases del ciclo de vida reúnen 11 etapas diferentes que deben seguirse durante el ciclo de vida de una política específica. No importa cómo se agrupen, tampoco importa si estas etapas son abreviadas por necesidades de inmediatez, pero cada etapa debe ser realizada. Si en la fase de desarrollo la universidad intenta crear una política sin una revisión independiente, se tendrán políticas que no estarán bien concebidas ni serán bien recibidas por

la comunidad universitaria. En otras circunstancias, y por falta de visión, puede desearse omitir la etapa de excepciones de la fase de implementación, pensando equivocadamente que no existirán circunstancias para su no cumplimiento. También se podría descuidar la etapa de mantenimiento, olvidando la importancia de mantener la integridad y la vigencia de las políticas. Muchas veces se encuentran políticas inoficiosas en los documentos de importantes organizaciones, indicando que la etapa de retiro no está siendo realizada.

No sólo se requiere que las once etapas sean realizadas, algunas de ellas deben ser ejecutadas de manera cíclica, en particular ***mantenimiento, concienciación, monitoreo,*** **y** ***garantía de cumplimiento*****.**

De las etapas y fases detalladas y mostradas en el gráfico "**Etapas en el desarrollo de políticas**" anterior nuestro trabajo se enfocará únicamente a la etapa de creación, en la fase de desarrollo, debido a que para el avance de las siguientes etapas se requerirá de la conformación de un equipo de personas propiamente de la empresa que tomen en cuenta todas las consideraciones y convenios con la dirección necesarios, lo cual está fuera de nuestro alcance.

3.11.2. Prácticas recomendadas para escribir una política:

Sin importar que una política se enuncie formal o informalmente, esta debe incluir 12 tópicos:

1. La declaración de la política (cuál es la posición de la administración o qué es lo que se desea regular).
2. Nombre y cargo de quien autoriza o aprueba la política
3. Nombre de la dependencia, del grupo o de la persona que es el autor o el proponente de la política
4. Debe especificarse quién debe acatar la política (es decir, a quién está dirigida) y quién es el responsable de garantizar su cumplimiento
5. Indicadores para saber si se cumple o no la política
6. Referencias a otras políticas y regulaciones en las cuales se soporta o con las cuales tiene relación
7. Enunciar el proceso para solicitar excepciones

8. Describir los pasos para solicitar cambios o actualizaciones a la política

9. Explicar qué acciones se seguirán en caso de contravenir la política

10. Fecha a partir de la cual tiene vigencia la política

11. Fecha cuando se revisará la conveniencia y la obsolescencia de la política

12. Incluir la dirección de correo electrónico, la página web y el teléfono de la persona o personas que se pueden contactar en caso de preguntas o sugerencias.

Etapa	Políticas	Estándares y buenas prácticas	Guías	Procedimientos
Creación	Función seguridad informática	Función seguridad informática e ingenieros con conocimiento en el área	Función seguridad informática e ingenieros con conocimiento en el área	Dependencia que los propone
Revisión	Comité de evaluación de políticas	Comité de evaluación de políticas	Comité de evaluación de políticas	Función seguridad informática y director de dependencia
Aprobación	Rector general o vicerrector general	Rector general o vicerrector	Rector general o vicerrector	Directivo del área
Comunicación	Secretaría o UNIMEDIOS	Secretaría o UNIMEDIOS	Secretaría o UNIMEDIOS	Dependencia que los propone
Cumplimiento	Docentes, estudiantes, empleados y funcionarios con responsabilidades de supervisión en toda la universidad	Docentes, estudiantes, empleados y funcionarios con responsabilidades de supervisión en toda la universidad	Docentes, estudiantes, empleados y funcionarios con responsabilidades de supervisión en toda la universidad	Empleados y funcionarios con responsabilidades de supervisión de la dependencia
Excepciones	Comité de evaluación de políticas	Comité de evaluación de políticas	No aplica	Directivo del área
Concienciación	Función seguridad informática y función capacitación	Función seguridad informática y función capacitación	Función seguridad informática y función capacitación	Jefe de dependencia
Monitoreo	Funcionarios con responsabilidades de supervisión, función seguridad informática y función auditoria	Funcionarios con responsabilidades de supervisión, función seguridad informática y función auditoria	Funcionarios con responsabilidades de supervisión, función seguridad informática y función auditoria	Funcionarios con responsabilidades de supervisión y personas asignadas dentro de la dependencia, función seguridad informática y función auditoria
Garantizar cumplimiento	Funcionarios con responsabilidades de supervisión	Funcionarios con responsabilidades de supervisión	No aplica	Funcionarios con responsabilidades de supervisión asignados en la dependencia
Mantenimiento	Función seguridad informática	Función seguridad informática	Función seguridad informática	Dependencia que los propone
Retiro	Función seguridad informática	Función seguridad informática	Función seguridad informática	Dependencia que los propone

Tabla 3: Modelo de responsabilidad por etapa para cada tipo de política
FUENTE: UNC "Guía para elaboración de políticas de seguridad"

CAPITULO IV

4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1. Análisis de la información obtenida:

4.1.1. Servicio de Tramitación:

El servicio de tramitación se presta por medio de una aplicación informática desarrollada en el pasado sobre una base de datos. A esta aplicación se accede a través de una identificación local del usuario que controla sus privilegios de acceso. En la faceta de tramitación presencial, es la persona que está atendiendo al usuario final la que se identifica frente al sistema. En el caso de la tramitación remota, el propio administrado quien se identifica.

Toda la tramitación incluye una fase de solicitud (y entrada de datos) y una fase de respuesta (y entrega de datos). El usuario realiza su solicitud y espera una notificación para recoger la respuesta.

Iniciar una tramitación supone abrir un expediente que se almacena localmente en la oficina.

También supone recabar una serie de datos del archivo central de información, datos que se copian localmente. Al cierre del expediente, los datos y un informe de las actuaciones realizadas se remiten al archivo central para su custodia, eliminándose la información de los equipos locales.

El personal de la unidad se identifica por medio de su cuenta de usuario, mientras que los usuarios remotos se identifican por su RU. En ambos casos el sistema requiere una contraseña para autenticarlos.

4.1.2. Servicio de archivo central:

En forma de intranet, se presta un servicio centralizado de archivo y recuperación de documentos.

Los usuarios acceden por medio de una interfaz web local, que se conecta por medio de una red con el servidor local, identificándose por medio de su RU. Este servicio sólo está disponible para el personal de la unidad y para el empleado que presta el servicio de tramitación.

4.1.3. Equipamiento informático:

La unidad dispone de varios equipos personales de tipo PC situados dentro de los locales. Estos equipos disponen de un navegador web y un paquete ofimático estándar (procesador de textos y hoja de cálculo).

Existe una capacidad de almacenamiento local de información en el disco del PC, del que no se realizan copias de seguridad; es más, existe un procedimiento de instalación / actualización que borra el disco local y reinstala el sistema integro.

Los equipos no disponen de unidades de disco removible de ningún tipo: disquetes, CD, DVD, USB, etc.

Se dispone de un servidor de tamaño medio, de propósito general, dedicado a las tareas de:

• Servidor de ficheros.

• Servidor de bases de datos: expedientes en curso e identificación de usuarios.

• Servidor web para la tramitación por la intranet local.

4.1.4. Comunicaciones:

Se dispone de una red de área local que cubre las dependencias de trabajo y la sala de equipos.

Está explícitamente prohibida la instalación de módems de acceso remoto y redes inalámbricas, existiendo un procedimiento rutinario de inspección.

Existe una conexión de red LAN, sobre este enlace se prestan múltiples servicios:

- Servicio (propio) de tramitación
- Servicio (propio) de acceso a información

La conexión a la red se realiza única y exclusivamente a través de unos cortafuegos que limitan las comunicaciones a nivel de red, permitiendo únicamente:

- El intercambio de ficheros con el servidor de datos
- El intercambio web con el servidor web

La red con el edificio central utiliza una aplicación informática software. La red se establece al inicio de la jornada, cortándose automáticamente a la hora de cierre. En el establecimiento los equipos terminales se reconocen mutuamente y establecen una clave de sesión para la jornada. No hay intervención de ningún operador local.

4.1.5. Seguridad física:

El personal trabaja en los locales de la unidad, principalmente en zonas interiores, salvo una serie de terminales en los puntos de atención al público. El acceso a las zonas interiores está limitado a las horas de oficina, quedando cerrado con llave fuera de dicho horario. En horas de oficina hay un control de entrada que identifica a los empleados y registra su hora de entrada y de salida.

La sala de equipos es simplemente una habitación interior que permanece cerrada con llave, de la que es custodio el administrador de sistemas. La sala dispone de un sistema de detección y revisa anualmente.

Los locales de la unidad ocupan íntegramente la planta baja de un edificio de oficinas de 2 plantas.

Los controles de acceso son propios de la unidad, no del edificio, que es de uso compartido con otras actividades. No hay ningún control sobre qué hay en el piso de arriba o en el piso de abajo.

4.2. Dependencia de activos:

Teniendo en cuenta las dependencias para operar (disponibilidad) y de almacenamiento de datos (integridad y confidencialidad), se ha determinado la siguiente matriz de dependencias entre activos:

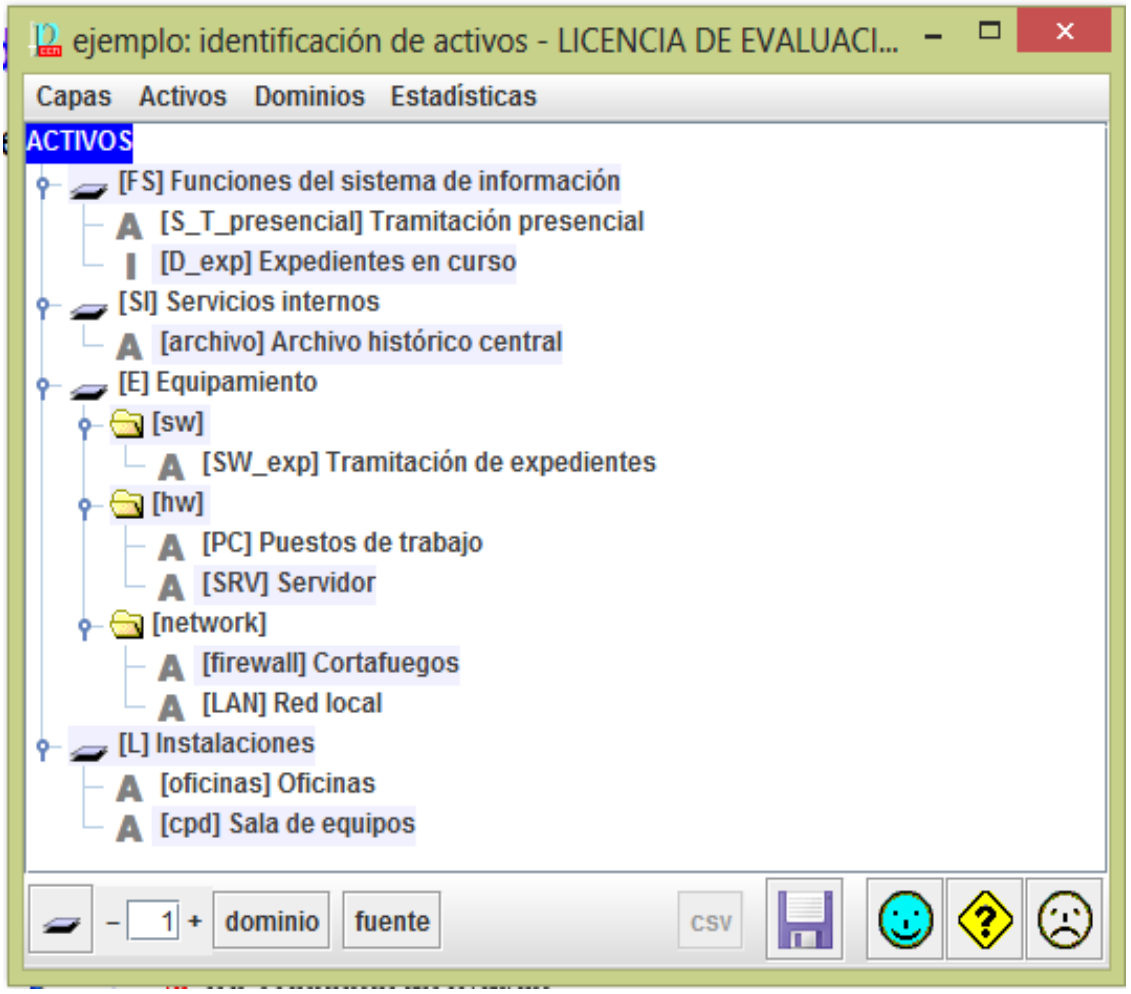


GRAFICO 10: Identificación de Activos

FUENTE: Elaboración propia

En este proceso se utilizará la herramienta PILAR en su versión de análisis cualitativo.

La relación de activos agrupa a estos en cuatro capas (en negrita). La estructuración en capas es mero artilugio de ordenación de la información. En cada capa se indican qué activos hay de cada tipo. Se ha empleado la relación del "Catálogo de Elementos", capítulo "2. Tipos de activos".

ACTIVO	S_T_PRESENCIAL	D_EXP	ARCHIVO	SW_EXP	PC	SRV	FIREWALL	LAN
S_T_PRESENCIAL		V	V	V	V	V		V
D_EXP			V	V	V	V		V
ARCHIVO						V	V	
SW_EXP								
PC								
SRV								
FIREWALL								
LAN								

TABLA 4: Dependencia de Activos
FUENTE: Elaboración propia

Representación de la tabla de dependencias gráfica de la dependencia entre activos:

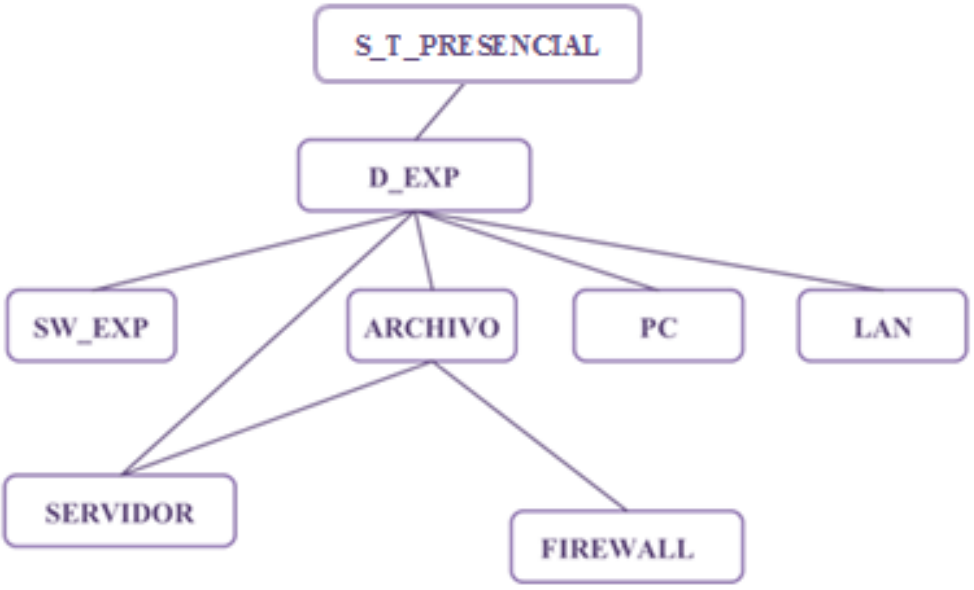


GRAFICO 11: Dependencia de Activos

FUENTE: ELABORACIÓN PROPIA

4.3. Valoración de Activos:

La dirección está preocupada por el potencial abuso que se pueda dar en los procesos de tramitación, algunos de los cuales pueden incluir el abono de cantidades económicas importantes, bien a beneficio de la Institución y responsables, existiendo una especial incomodidad relacionada con la impunidad de atacantes que pudieran perpetrar ataques desde cualquier remoto punto de la red del local.

También hay una especial sensibilidad relativa a la disponibilidad de los servicios. En particular hay preocupación porque no se pudiera atender una gran demanda.

Los servicios web a usuarios externos, se consideran simbólicos y se quieren cuidar con esmero para dar una imagen de modernidad, eficacia y vocación de servicio. Todo lo que suponga dar una mala imagen, bien porque no está disponible el servicio, bien porque se presta de forma errónea, bien porque las incidencias no son atendidas con presteza, todas estas situaciones se quieren evitar en la medida de lo posible.

Las bases de datos locales hospedan información relativa a personas que quedarán adscritos al nivel medio dentro de la calificación de datos de carácter personal.

En vista de todo ello, se ha consensuado la siguiente valoración de los activos del sistema. Sólo se han valorado explícitamente los activos superiores del árbol de dependencias, que quedan de la siguiente manera:

	DIMENSIONES DE SEGURIDAD						
ACTIVO	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
TRAMITACION PRESENCIAL	[5][1]			[7][2]		[6][3]	
EXPEDIENTES EN CURSO		[5][4]	[6][5]		[5][6]		[5][7]

TABLA 5: Valoración de activos

FUENTE: Elaboración propia

Escalas Estándar para la valoración de activos en base a las dimensiones establecidas:

Las siguientes escalas se han obtenido en base a las tablas que pretenden guiar con más detalle a los usuarios para la valoración de forma homogénea activos cuyo valor es importante por diferentes motivos **ver anexo**.

(1) [5.da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones.

(2) [7.da] Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.

[5.lro] Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación.

(3) [6.pi2] Información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.

(4) [5.da] Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones.

(5) [6.pi2] Información personal: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.

(6) [5.lro] Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación.

(7) [5.lro] Obligaciones legales: probablemente sea causa de incumplimiento de una ley o regulación.

Para cada activo se indica su valoración en cada dimensión de seguridad.

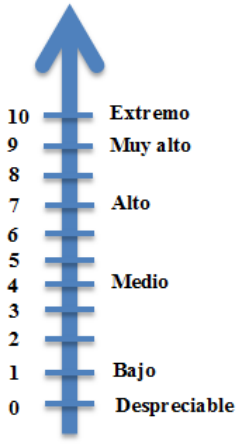


GRAFICO 12: Criterio de valoración

FUENTE: MAGERIT

VALOR		CRITERIO
10	**Extremo**	Daño extremadamente grave
9	**Muy alto**	Daño muy grave
6-8	**Alto**	Daño grave
3-5	**Medio**	Daño importante
1-2	**Bajo**	Daño menor
0	**Despreciable**	Irrelevante a efectos prácticos

TABLA 6: CRITERIO DE VALORACION

FUENTE: MAGERIT

Como criterios de valoración se ha empleado el capítulo "4. Criterios de valoración" del "Catálogo de Elementos".

Como dimensiones de seguridad se ha empleado la relación del capítulo "3. Dimensiones de valoración" del "Catálogo de Elementos".

Cuando esta valoración se propaga a través del árbol de dependencias, resulta la siguiente tabla de valor acumulado en cada uno de los activos del sistema (se muestra sobre fondo blanco lo que es valor propio, y sobre fondo de color lo que es acumulado):

En este punto se obtiene el "Modelo de Valor" de la organización.

	DIMENSIONES DE SEGURIDAD						
ACTIVO	[D]	[I]	[C]	[A_S]	[A_D]	[T_S]	[T_D]
TRAMITACION PRESENCIAL	[5]			[7]		[6]	
EXPEDIENTES EN CURSO	[5]	[5]	[6]	[7]	[5]	[6]	[5]
ARCHIVO HISTORICO CENTRAL	[5]			[7]		[6]	
TRAMITACION DE EXPEDIENTES	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[PC]PUESTOS DE TRABAJO	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[SVR]SERVIDOR	[5]	[5]	[6]	[7]	[5]	[6]	[5]
[FIREWALL]CORTAFUEGOS	[5]	[5]	[6]	[7]	[5]	[6]	[5]

[LAN] RED LOCAL	[5]	[5]	[6]	[7]	[5]	[6]	[5]

TABLA 7: Valor Acumulado
FUENTE: elaboración propia

SIMBOLO DIMENSION	DIMENSION
[D]	Disponibilidad
[I]	Integridad
[C]	Confidencialidad
[A]	Autenticidad
[T]	Trazabilidad

Ver "Guía de Técnicas" sección "2.2.1. Modelo cualitativo".
Ver "Apéndice 4.1. Modelo de valor" del "Catálogo de Elementos" **ver anexo**.

4.4. Caracterización de las amenazas:

En esta actividad se procede a caracterizar lo que podría ocurrirle a los activos si no hubiera salvaguardas desplegadas, se recurre a una calificación estándar de las amenazas típicas sobre los activos teniendo en cuenta su naturaleza y su valor.

Con todas estas consideraciones, y a título ilustrativo, la siguiente tabla muestra las amenazas que se han considerado típicas para el caso de los expedientes administrativos.

		DIMENSIONES DE SEGURIDAD				
ACTIVO/AMENAZA	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Expedientes en curso		50%	50%	100%	100%	100%
[E.1] Errores de los usuarios	10	10%	10%			
[E.2] Errores del administrador	1	20%	20%	10%	10%	10%
[E.3] Errores de monitorización (log)	1					50%
[E.4] Errores de configuración	0,5	50%	10%	10%	50%	50%
[E.14] Escapes de información	1			1%		
[E.15] Alteración de la información	10		1%			
[E.16] Introducción de falsa información	100		1%			
[E.17] Degradación de la información	10		1%			
[E.18] Destrucción de la información	10	1%				
[E.19] Divulgación de información	1			10%		
[A.4] Manipulación de la configuración	0,1	50%	10%	50%	100%	100%
[A.11] Acceso no autorizado	100		10%	50%	50%	

[A.14] Intercepción de información (escucha)	10			50%		
[A.15] Modificación de información	10		50%			
[A.16] Introducción de falsa información	20		50%			
[A.17] Corrupción de la información	0		50%			
[A.18] Destrucción de la información	0	50%				
[A.19] Divulgación de información	10			100%		

TABLA 8: Amenazas Expedientes en Curso

FUENTE: Elaboración propia

Nótese que hay una diferencia entre la percepción del usuario y las amenazas potenciales en el sistema. Esta diferencia se debe a la existencia de salvaguardas, que se tendrá en cuenta más adelante.

En este punto se obtiene el "Mapa de Riesgos" de la organización.

La primera columna muestra las amenazas típicas sobre el activo. La segunda columna recoge la frecuencia de ocurrencia expresada como tasa anual (incidencias por año). Las demás columnas recogen la degradación del activo expresada como porcentaje de su valor **ver anexo**.

		DIMENSIONES DE SEGURIDAD				
ACTIVO/AMENAZA	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Tramitación presencial		50%	50%	50%	100%	100%
[E.1] Errores de los usuarios	1	10%	10%	10%		
[E.2] Errores del administrador	1	20%	20%	20%		
[E.15] Alteración de la información	1		1%			
[E.18] Destrucción de la información	1	10%				
[E.19] Divulgación de información	1			10%		
[E.24] Caída del sistema por agotamiento de recursos	0	50%				
[A.5] Suplantación de la identidad	1		50%	50%	100%	
[A.6] Abuso de privilegios de Acceso	1	1%	10%	10%	100%	
[A.7] Uso no previsto	1	1%	10%	10%		
[A.11] Acceso no autorizado	1		10%	50%	100%	
[A.13] Repudio (Negación de actuaciones)	0					100%

[A.15] Modificación de información	10			50%		
[A.18] Destrucción de la información	1	50%				
[A.19] Divulgación de información	1			50%		
[A.24] Denegación de servicio	10	50%				

TABLA 9: Amenazas Tramitación Presencial

FUENTE: ELABORACION PROPIA

	DIMENSIONES DE SEGURIDAD					
ACTIVO/AMENAZA	**FRECUENCIA**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Archivo Histórico Central			20%	50%	100%	100%
[E.1] Errores de los usuarios	1		10%	10%		
[E.2] Errores del administrador	1		20%	20%		
[E.9] Errores de [re-]encaminamiento	1			10%		
[E.10] Errores de secuencia	1		10%			
[E.15] Alteración de información	1		1%			
[E.19] Fugas de Información	10			10%		
[A.5] Suplantación de la identidad	1		10%	50%	100%	
[A.6] Abuso de privilegios de Acceso	1		10%	50%	100%	
[A.7] Uso no previsto	1		10%	10%		
[A.9] [Re-]encaminamiento de mensajes	0			10%		
[A.10] Alteración de Secuencia	1		10%			
[A.11] Acceso no autorizado	1		10%	50%	100%	
[A.12] Análisis de trafico	1			2%		
[A.13] Repudio (negación de actuaciones)	0					100%
[A.14] Interceptación de información (escucha)	0			10%		
[A.15] Modificación de la información	0		10%			
[A.19] Revelación de información	1			50%		

TABLA 10: Amenazas Archivo Histórico Central

FUENTE: ELABORACION PROPIA

	DIMENSIONES DE SEGURIDAD					
ACTIVO/AMENAZA	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Tramitación de Expedientes			100%	100%	100%	
[E.1] Errores de los usuarios	1		10%	10%		
[E.2] Errores del administrador	1		20%	20%		
[E.8] Difusión de software dañino	1		10%	10%		
[E.15] Alteración de información	1		1%			
[E.19] Fugas de Información	1			10%		
[E.20] Vulnerabilidades de los programas (software)	10		20%	20%		
[E.21] Errores de mantenimiento/ actualización de programas	1		1%			
[A.5] Suplantación de la identidad	1		50%	50%	100%	
[A.6] Abuso de privilegios de Acceso	1		10%	10%		
[A.7] Uso no previsto	1		10%	10%		
[A.8] Difusión de software dañino	1		100%	10%		
[A.11] Acceso no autorizado	1		10%	50%		
[A.15] Modificación de la Información	1		50%			
[A.19] Revelación de información	1			50%		
[A.22] Manipulación de programas	1		100%	100%		

TABLA 11: Amenazas Tramitación de Expedientes

FUENTE: ELABORACION PROPIA

	DIMENSIONES DE SEGURIDAD					
ACTIVO/AMENAZA	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Puestos de Trabajo			100%	100%	100%	
[I. 11]Emanaciones electromagnéticas	1			1		
[E.1] Errores de los usuarios	1		10%	10%		
[E.2] Errores del administrador	1		20%	20%		
[E.8] Difusión de software dañino	1		10%	10%		
[E.15] Alteración de información	1		1%			
[E.19] Fugas de Información	1			10%		

[E.20] Vulnerabilidades de los programas (software)	1		20%	20%		
[E.21] Errores de mantenimiento/ actualización de programas	10		1%			
[E.25] Perdida de equipos	0			10%		
[A.5] Suplantación de la identidad	1		50%	50%	100%	
[A.6] Abuso de privilegios de Acceso	1		10%	10%		
[A.7] Uso no previsto	1		1%	10%		
[A.8] Difusión de software dañino	1		100%	100%		
[A.11] Acceso no autorizado	1		10%	50%		
[A.15] Modificación de la Información	1		50%			
[A.19] Revelación de información	1			50%		
[A.22] Manipulación de programas	1		100%	100%		
[A.23] Manipulación de programas	0.5			50%		
[A.25] Robo de equipos	0			10%		

TABLA 12: Amenazas Puestos de Trabajo

FUENTE: ELABORACION PROPIA

	DIMENSIONES DE SEGURIDAD					
ACTIVO/AMENAZA	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Servidor			100%	100%	100%	
[I. 11]Emanaciones electromagnéticas	1			1		
[E.1] Errores de los usuarios	1		10%	10%		
[E.2] Errores del administrador	1		20%	20%		
[E.8] Difusión de software dañino	1		10%	10%		
[E.15] Alteración de información	1		1%			
[E.19] Fugas de Información	1			10%		
[E.20] Vulnerabilidades de los programas (software)	1		20%	20%		
[E.21] Errores de mantenimiento/ actualización de programas	10		1%			
[E.25] Perdida de equipos	0			100%		

[A.5] Suplantación de la identidad	1		50%	50%	100%	
[A.6] Abuso de privilegios de Acceso	1		100%	100%		
[A.7] Uso no previsto	1		10%	100%		
[A.8] Difusión de software dañino	1		100%	100%		
[A.11] Acceso no autorizado	1		100%	100%		
[A.15] Modificación de la Información	1		50%			
[A.19] Revelación de información	1			50%		
[A.22] Manipulación de programas	1		100%	100%		
[A.23] Manipulación de programas	0			50%		
[A.25] Robo de equipos	0			100%		

TABLA 13: Amenazas Servidor

FUENTE: ELABORACION PROPIA

	DIMENSIONES DE SEGURIDAD					
ACTIVO/AMENAZA	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Firewall			100%	100%	100%	
[I. 11]Emanaciones electromagnéticas	1			1%		
[E.1] Errores de los usuarios	1		10%	10%		
[E.2] Errores del administrador	1		20%	20%		
[E.8] Difusión de software dañino	1		10%	10%		
[E.15] Alteración de información	1		1%			
[E.19] Fugas de Información	1			10%		
[E.20] Vulnerabilidades de los programas (software)	1		20%	20%		
[E.21] Errores de mantenimiento/ actualización de programas	10		1%			
[E.25] Perdida de equipos	0			50%		
[A.5] Suplantación de la identidad	1		50%	50%	100%	
[A.6] Abuso de privilegios de Acceso	1		10%	50%		
[A.7] Uso no previsto	1		1%	10%		
[A.8] Difusión de software dañino	1		100%	100%		
[A.11] Acceso no autorizado	1		10%	50%		
[A.15] Modificación de la Información	1		50%			

[A.19] Revelación de información	1			50%		
[A.22] Manipulación de programas	1		100%	100%		
[A.23] Manipulación de programas	0			50%		
[A.25] Robo de equipos	0			50%		

TABLA 14: Amenazas Firewall
FUENTE: ELABORACION PROPIA

	DIMENSIONES DE SEGURIDAD					
ACTIVO/AMENAZA	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Red Local			20%	50%	100%	
[E.1] Errores de los usuarios	1		20%	20%		
[E.2] Errores del administrador	1			10%		
[E.8] Difusión de software dañino	1		10%			
[E.15] Alteración de información	1		1%			
[E.19] Fugas de Información	1			10%		
[E.20] Vulnerabilidades de los programas (software)	1		10%	50%	100%	
[E.21] Errores de mantenimiento/ actualización de programas	10		10%	50%	100%	
[E.25] Perdida de equipos	0		10%	10%		
[A.5] Suplantación de la identidad	1			10%		
[A.6] Abuso de privilegios de Acceso	1		10%			
[A.7] Uso no previsto	1		10%	50%	100%	
[A.8] Difusión de software dañino	1			2%		
[A.11] Acceso no autorizado	1			1%		
[A.15] Modificación de la Información	1		10%			
[A.19] Revelación de información	1			50%		

TABLA 15: Amenazas Red Local
FUENTE: ELABORACION PROPIA

	DIMENSIONES DE SEGURIDAD					
ACTIVO/AMENAZA	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Oficinas			10%	50%		
[I. 11] Emanaciones electromagnéticas	0.1			1%		

[A.5] Suplantación de identidad	1		10%			
[A.6] Abuso de privilegios de Acceso	1		10%	50%		
[A.7] Uso no previsto	1		10%	50%		
[A.11] Acceso no autorizado	5		10%	50%		
[A.27] Ocupación enemiga	1			50%		

TABLA 16: Amenazas Oficinas
FUENTE ELABORACION PROPIA

	DIMENSIONES DE SEGURIDAD					
ACTIVO/AMENAZA	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
Sala de Equipos			10%	50%		
[I. 11] Emanaciones electromagnéticas	0.1			1%		
[A.5] Suplantación de identidad	1		10%	50%		
[A.6] Abuso de privilegios de Acceso	1		10%	50%		
[A.7] Uso no previsto	1		10%	50%		
[A.11] Acceso no autorizado	5		10%	50%		
[A.27] Ocupación enemiga	1			50%		

TABLA 17: Amenazas Sala de Equipos
FUENTE: ELABORACION PROPIA

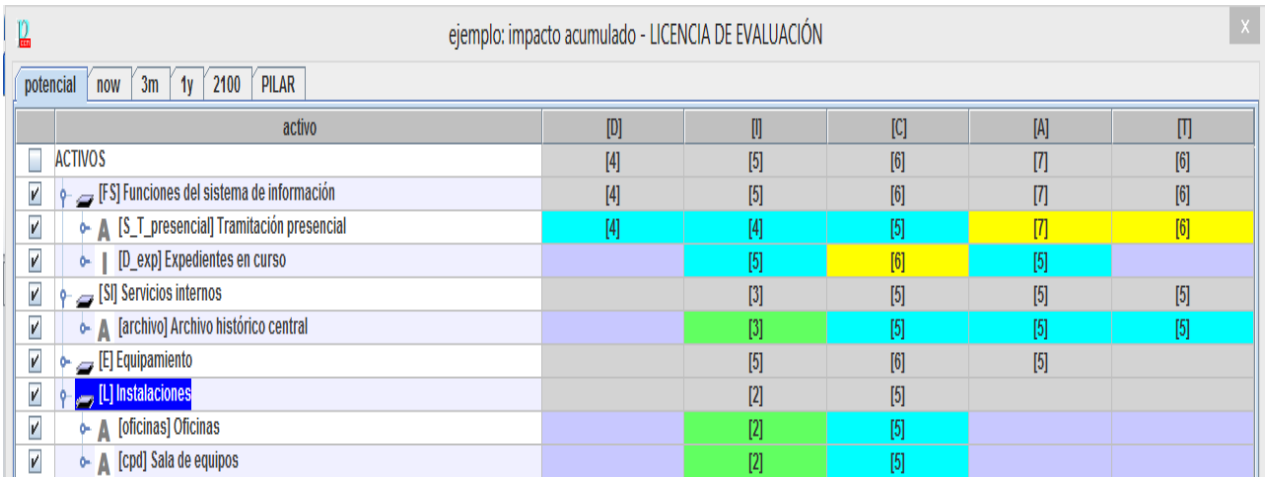
Hay una columna por dimensión de seguridad (véase "Catálogo de Elementos", capítulo 3. "Dimensiones de valoración").

Ver "Apéndice 4.2. Mapa de riesgos" del "Catálogo de Elementos" **ver anexo (3)**.

4.5. Estimación de impacto y riesgo:

Sin tener todavía en cuenta las salvaguardas, se derivan las siguientes estimaciones de impacto y riesgo acumulado sobre los diferentes activos. Las tablas siguientes recogen para cada activo (filas) la estimación de impacto y riesgo en cada dimensión de seguridad (columnas).

4.5.1. Impacto Acumulado:

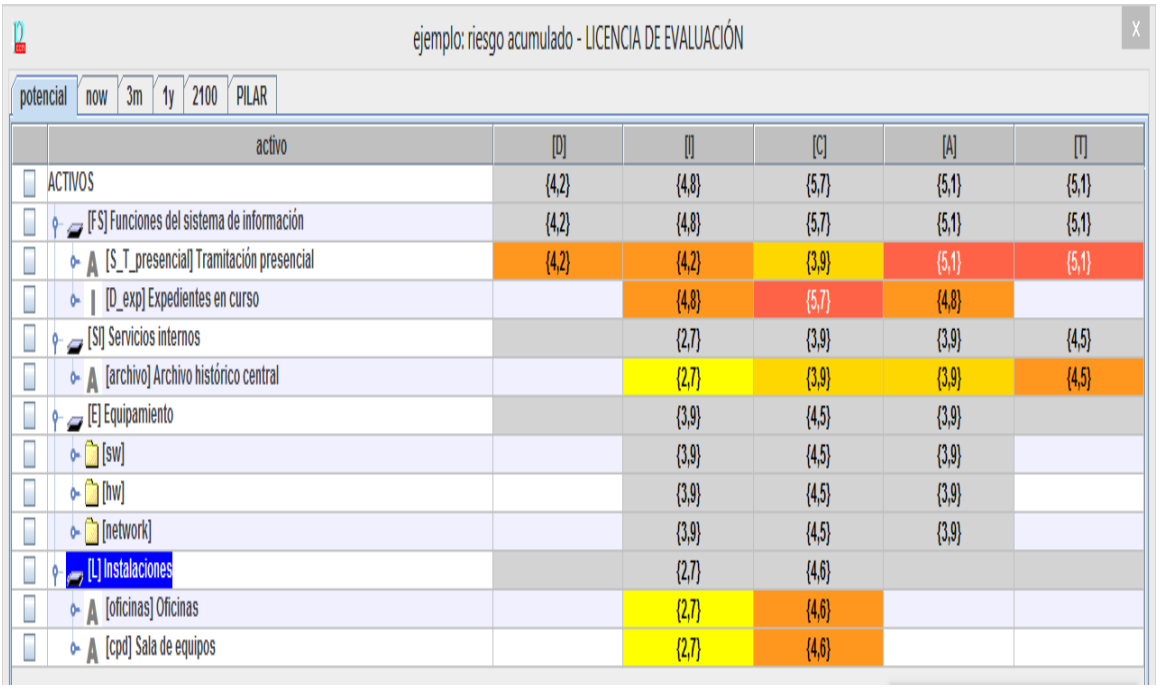


activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[4]	[5]	[6]	[7]	[6]
[FS] Funciones del sistema de información	[4]	[5]	[6]	[7]	[6]
[S_T_presencial] Tramitación presencial	[4]	[4]	[5]	[7]	[6]
[D_exp] Expedientes en curso		[5]	[6]	[5]	
[SI] Servicios internos		[3]	[5]	[5]	[5]
[archivo] Archivo histórico central		[3]	[5]	[5]	[5]
[E] Equipamiento		[5]	[6]	[5]	
[L] Instalaciones		[2]	[5]		
[oficinas] Oficinas		[2]	[5]		
[cpd] Sala de equipos		[2]	[5]		

GRAFICO 13 Impacto Acumulado
FUENTE: Elaboración propia

TABLA 18: Interpretación de valores:
FUENTE: ELABORACION PROPIA

4.5.2. Riesgo Acumulado:



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{4,2}	{4,8}	{5,7}	{5,1}	{5,1}
[FS] Funciones del sistema de información	{4,2}	{4,8}	{5,7}	{5,1}	{5,1}
[S_T_presencial] Tramitación presencial	{4,2}	{4,2}	{3,9}	{5,1}	{5,1}
[D_exp] Expedientes en curso		{4,8}	{5,7}	{4,8}	
[SI] Servicios internos		{2,7}	{3,9}	{3,9}	{4,5}
[archivo] Archivo histórico central		{2,7}	{3,9}	{3,9}	{4,5}
[E] Equipamiento		{3,9}	{4,5}	{3,9}	
[sw]		{3,9}	{4,5}	{3,9}	
[hw]		{3,9}	{4,5}	{3,9}	
[network]		{3,9}	{4,5}	{3,9}	
[L] Instalaciones		{2,7}	{4,6}		
[oficinas] Oficinas		{2,7}	{4,6}		
[cpd] Sala de equipos		{2,7}	{4,6}		

GRAFICO 14: Riesgo Acumulado

FUENTE: Elaboración propia

TABLA 19: Interpretación de Valores

FUENTE: ELABORACION PROPIA

Para el cálculo del impacto acumulado se sigue lo indicado en la sección “2.1.3. Paso 4: Determinación del impacto”, donde se tiene en cuenta el valor acumulado sobre el activo (en la citada dimensión) y la degradación causada por la amenaza (en la citada dimensión). Véase también la sección “2.2.1. Modelo cualitativo” de la “Guía de Técnicas”.

Para el cálculo del riesgo acumulado se sigue lo indicado en la sección “2.1.4. Determinación del riesgo”, donde se incorpora la frecuencia estimada de ocurrencia de la amenaza. Se utiliza un modelo tabular similar al descrito en la sección “2.1. Análisis mediante tablas” de la “Guía de Técnicas”. Se utiliza una escala de {0} a {5} para calibrar el riesgo.

4.5.3. Impacto repercutido:

En estas tablas se analiza cada activo (superior) valorado en sí mismo (con valor propio) y se hace un seguimiento de aquellos otros activos (inferiores) de los que depende. Cuando las amenazas se materializan sobre los activos inferiores, el perjuicio repercute sobre los superiores.

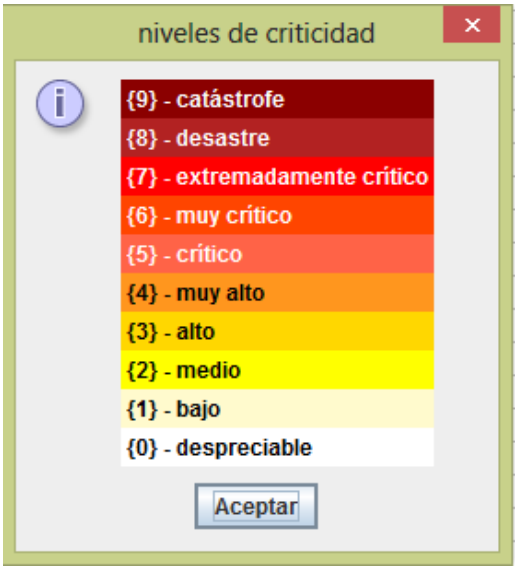
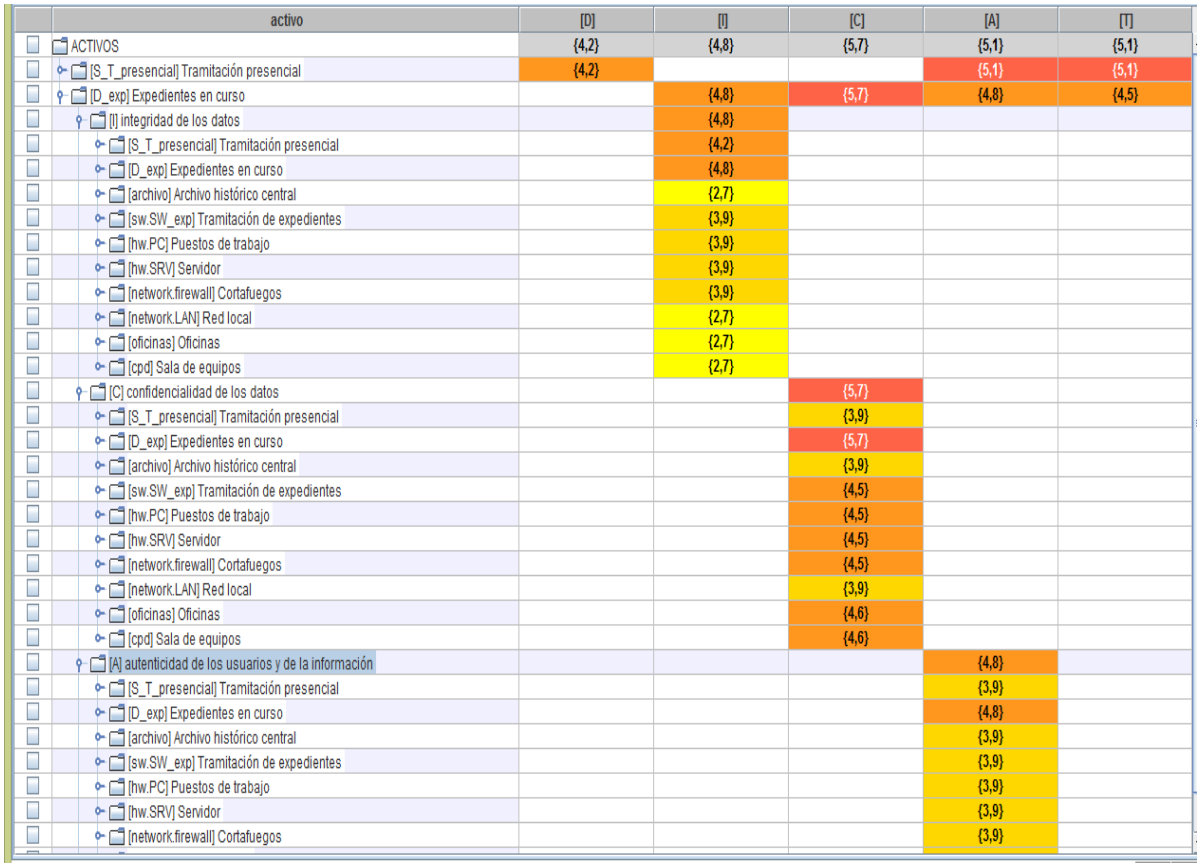


TABLA 20: Interpretacion Nivel de Criticidad

FUENTE : ELABORACION PROPIA

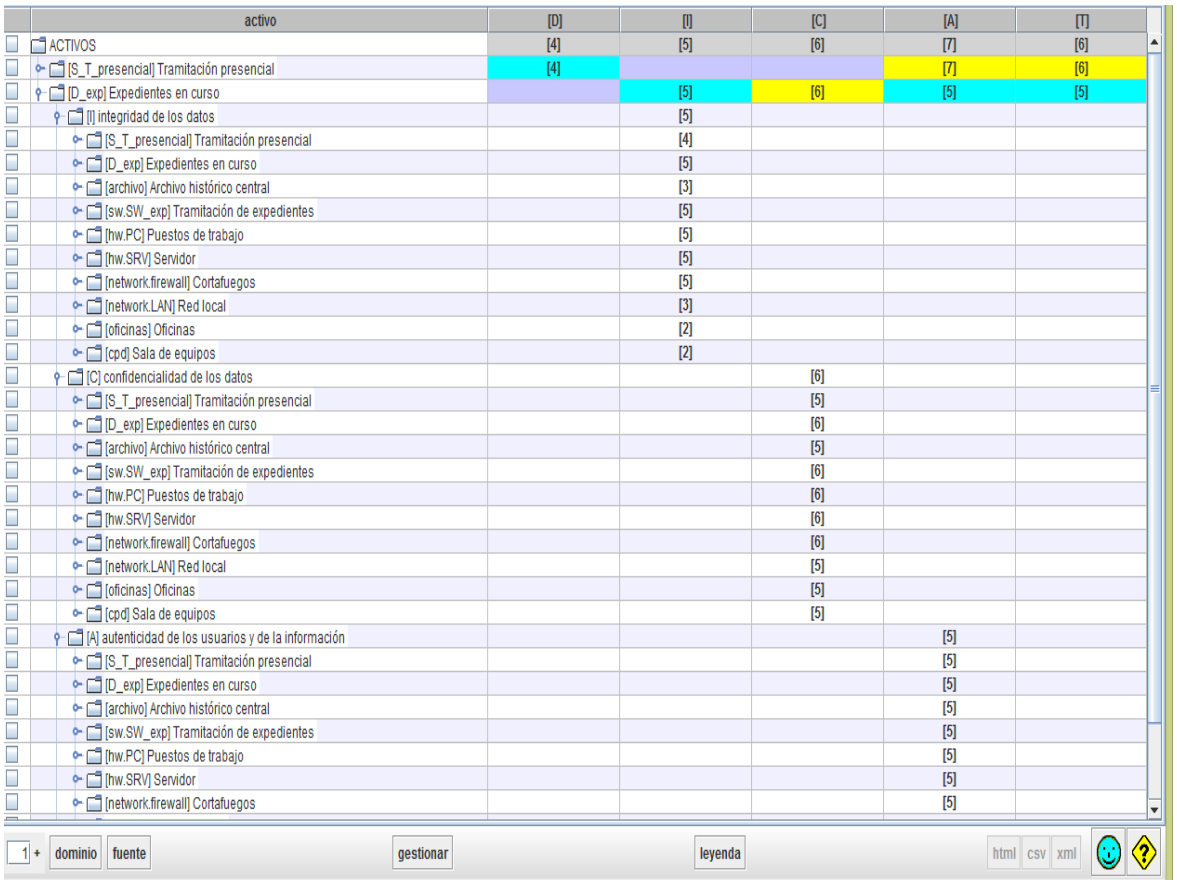


activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{4,2}	{4,8}	{5,7}	{5,1}	{5,1}
[S_T_presencial] Tramitación presencial	{4,2}			{5,1}	{5,1}
[D_exp] Expedientes en curso		{4,8}	{5,7}	{4,8}	{4,5}
[I] integridad de los datos		{4,8}			
[S_T_presencial] Tramitación presencial		{4,2}			
[D_exp] Expedientes en curso		{4,8}			
[archivo] Archivo histórico central		{2,7}			
[sw.SW_exp] Tramitación de expedientes		{3,9}			
[hw.PC] Puestos de trabajo		{3,9}			
[hw.SRV] Servidor		{3,9}			
[network.firewall] Cortafuegos		{3,9}			
[network.LAN] Red local		{2,7}			
[oficinas] Oficinas		{2,7}			
[cpd] Sala de equipos		{2,7}			
[C] confidencialidad de los datos			{5,7}		
[S_T_presencial] Tramitación presencial			{3,9}		
[D_exp] Expedientes en curso			{5,7}		
[archivo] Archivo histórico central			{3,9}		
[sw.SW_exp] Tramitación de expedientes			{4,5}		
[hw.PC] Puestos de trabajo			{4,5}		
[hw.SRV] Servidor			{4,5}		
[network.firewall] Cortafuegos			{4,5}		
[network.LAN] Red local			{3,9}		
[oficinas] Oficinas			{4,6}		
[cpd] Sala de equipos			{4,6}		
[A] autenticidad de los usuarios y de la información				{4,8}	
[S_T_presencial] Tramitación presencial				{3,9}	
[D_exp] Expedientes en curso				{4,8}	
[archivo] Archivo histórico central				{3,9}	
[sw.SW_exp] Tramitación de expedientes				{3,9}	
[hw.PC] Puestos de trabajo				{3,9}	
[hw.SRV] Servidor				{3,9}	
[network.firewall] Cortafuegos				{3,9}	

GRAFICO 15: Impacto Repercutido

FUENTE: Elaboración propia

Para el cálculo del impacto repercutido se sigue lo indicado en la sección “2.1.3. Paso 4: Determinación del impacto”, donde se utiliza el valor propio del activo superior y la degradación causada por la amenaza sobre el activo inferior indicado.



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[4]	[5]	[6]	[7]	[6]
[S_T_presencial] Tramitación presencial	[4]			[7]	[6]
[D_exp] Expedientes en curso		[5]	[6]	[5]	[5]
[I] integridad de los datos		[5]			
[S_T_presencial] Tramitación presencial		[4]			
[D_exp] Expedientes en curso		[5]			
[archivo] Archivo histórico central		[3]			
[sw.SW_exp] Tramitación de expedientes		[5]			
[hw.PC] Puestos de trabajo		[5]			
[hw.SRV] Servidor		[5]			
[network.firewall] Cortafuegos		[5]			
[network.LAN] Red local		[3]			
[oficinas] Oficinas		[2]			
[cpd] Sala de equipos		[2]			
[C] confidencialidad de los datos			[6]		
[S_T_presencial] Tramitación presencial			[5]		
[D_exp] Expedientes en curso			[6]		
[archivo] Archivo histórico central			[5]		
[sw.SW_exp] Tramitación de expedientes			[6]		
[hw.PC] Puestos de trabajo			[6]		
[hw.SRV] Servidor			[6]		
[network.firewall] Cortafuegos			[6]		
[network.LAN] Red local			[5]		
[oficinas] Oficinas			[5]		
[cpd] Sala de equipos			[5]		
[A] autenticidad de los usuarios y de la información				[5]	
[S_T_presencial] Tramitación presencial				[5]	
[D_exp] Expedientes en curso				[5]	
[archivo] Archivo histórico central				[5]	
[sw.SW_exp] Tramitación de expedientes				[5]	
[hw.PC] Puestos de trabajo				[5]	
[hw.SRV] Servidor				[5]	
[network.firewall] Cortafuegos				[5]	

GRAFICO 16: Riesgo Repercutido

FUENTE: Elaboración Propia

Para el cálculo del riesgo repercutido se sigue lo indicado en la sección "2.1.4. Determinación del riesgo", donde se incorpora la frecuencia estimada de ocurrencia de la amenaza sobre el activo inferior indicado.

4.5.4. Caracterización de las salvaguardas:

A la hora de evaluar el estado de seguridad de la unidad bajo estudio, hay que indagar una serie de aspectos generales y una serie de aspectos específicos de cada activo. En esta indagación hay que tener en cuenta tanto la naturaleza de los activos como su valor y las amenazas a que está expuesto.

En aspectos generales hay que averiguar:

• Cómo se organiza la seguridad: responsables, toma de decisiones, contactos externos, etc.

• Si hay una identificación de roles del personal, asociados a privilegios de acceso

• Sí hay segregación efectiva de tareas

• Si existe una política de seguridad documentada y revisada periódicamente

• Cómo se gestionan las incidencias

• Cómo se gestionan los registros de actividad

• Si existe Respecto de los servicios prestados por la Organización, hay que averiguar

• Si existe normativa y procedimientos de uso, conocidos y empleados

• Si hay una planificación de capacidades

• Si hay mecanismos de prevención del repudio

• Si hay mecanismos de prevención de ataques de denegación de servicio

• Cómo se gestionan los usuarios

• Qué registro queda de lo que se hace

Respecto de los datos manejados por la Organización, hay que averiguar:

• Si hay un inventario de ficheros, con identificación de responsable

• Si existe normativa y procedimientos de uso, conocidos y empleados

• Si se hacen copias de respaldo y con qué calidad

• Si se han previsto mecanismos para garantizar el secreto

• Si se han previsto mecanismos para garantizar la integridad

• Si se han previsto mecanismos de registro de acceso

Respecto de los aplicativos en uso, hay que averiguar:

• Cómo se gestiona su mantenimiento

• Cómo se controla su configuración, en particular de usuarios y derechos de acceso

• Si se ha inspeccionado el código, especialmente frente a puertas traseras de acceso

Respecto del servicio de archivo, hay que averiguar:

• Si existe normativa y procedimientos de uso, conocidos y empleados

• Cómo se controla quién accede a su uso

• Cómo se garantiza el secreto de los datos que transportan

• Cómo se garantiza su disponibilidad

Respecto del equipamiento informático, hay que averiguar:

• Si existe normativa y procedimientos de uso, conocidos y empleados

• Cómo se gestiona su mantenimiento

• Cómo se controla su configuración, en particular de usuarios y derechos de acceso

• Cómo se garantiza su disponibilidad

Respecto de las comunicaciones, hay que averiguar:

• Si existe normativa y procedimientos de uso, conocidos y empleados

• Cómo se controla quién accede a su uso

• Cómo se garantiza el secreto de los datos que transportan

• Cómo se garantiza su disponibilidad

Indagando se averigua que:

• Existe una política de seguridad heredada de la Organización matriz de la unidad que nos ocupa. Al ser una unidad de pequeñas dimensiones, existe un responsable único de seguridad que informa directamente a la Dirección y es el contacto frente a otras organizaciones.

Además existe un procedimiento local de escalado de incidencias que puede provocar un escalado más allá de la propia unidad.

• El servidor central hospeda una tabla para controlar qué privilegios de acceso tiene cada usuario, en particular diferenciando la capacidad administrativa para dar curso a los expedientes a lo largo de su proceso. Toda la actividad se registra en un fichero al que sólo se tiene acceso el operador y que se remite diariamente al archivo central.

• Los procedimientos de trabajo con los sistemas no están escritos. Se confía en que las propias aplicaciones web adapten las actividades que se pueden realizar en cada momento según el estado del expediente en curso y los privilegios del usuario. Sí se realiza un registro de todas y cada una de las actuaciones del personal sobre los servicios web. Para el proceso manual existen una serie de impresos disponibles con instrucciones incluidas sobre cuándo usarlos, qué datos proporcionar y cómo tramitarlos.

• Una persona de la unidad tiene las funciones de operador, encargándose de todas las tareas de instalación, configuración y resolución de incidencias. Esta persona dispone de procedimientos escritos para las actividades rutinarias; pero debe improvisar en situaciones atípicas, para las que puede recurrir al soporte técnico de la Organización matriz.

• No existe ningún plan de contingencia (más allá del proceso manual de las actividades).

• Existen contratos de mantenimiento con los suministradores de los equipos y de los programas básicos: sistema operativo, ofimática y servidores web.

• Los usuarios externos se dan de alta personalmente, indicando su RU. Para recabar su contraseña deben personarse físicamente la primera vez. Una vez registrados no se hace un seguimiento de las cuentas, que duran indefinidamente.

• Tanto los usuarios internos como externos se identifican por medio de un nombre de usuario y una contraseña. Todos reciben unas someras instrucciones sobre cómo elegir contraseñas; pero no se verifica que las cumplan, ni que las contraseñas se cambien regularmente.

• Tanto los usuarios internos como externos se identifican por medio de un nombre de usuario y una contraseña. Todos reciben unas someras instrucciones sobre cómo elegir contraseñas; pero no se verifica que las cumplan, ni que las contraseñas se cambien regularmente.

• Se ha realizado recientemente una auditoría de los datos de carácter personal, habiendo sido superada plenamente en todos los aspectos.

• Los datos procedentes del archivo central se consideran correctos. Los datos introducidos por los ciudadanos deben ser validados por el personal de la unidad. Los datos introducidos por los usuarios internos deben ser validados por un segundo usuario; normalmente los introduce una persona y lo valida quien firma el progreso del expediente.

• El aplicativo de tramitación de expedientes es suministrado por la Organización matriz, considerándose "de calidad suficiente".

• Se ha instalado un sistema anti-virus y se ha contratado un servicio de mantenimiento 24x7 a través de la Organización matriz con un tiempo de respuesta inferior a 1 día.

• El servicio de mensajería se centraliza en el servidor de forma que el acceso de los usuarios internos es a través de una interfaz web. Sistemáticamente se elimina todo tipo de anexo en el correo saliente y se analiza con el anti-virus los anexos del correo entrante.

• El servicio de archivo central es un servicio prestado externamente que se va a considerar

"de calidad suficiente". En un análisis más detallado habrá que entrar en la prestación de este servicio.

• La conexión al archivo central se realiza sobre por una red LAN, que se establece entre los extremos. Esta red está configurada y mantenida desde el archivo central, sin tener capacidad local de configuración alguna. Se considerará "de calidad suficiente".

En este punto se obtiene la "Evaluación de Salvaguardas" de la organización.

Insuficiencias detectadas:

Cotejados los descubrimientos, se aprecian las siguientes insuficiencias:

• La segregación de tareas es adecuada excepto en el caso del administrador de sistemas que dispone de amplia capacidad de acceso a todos los sistemas, instalaciones y configuraciones.

• Debería existir un plan de contingencia: gestión de emergencias, plan de continuidad y plan de recuperación.

• Deberían existir procedimientos escritos para todas las tareas ordinarias y para las incidencias previsibles, incluyendo todas las que se hayan dado en el pasado.

• Deberían establecerse mecanismos para detectar y reaccionar a un ataque de denegación de servicio.

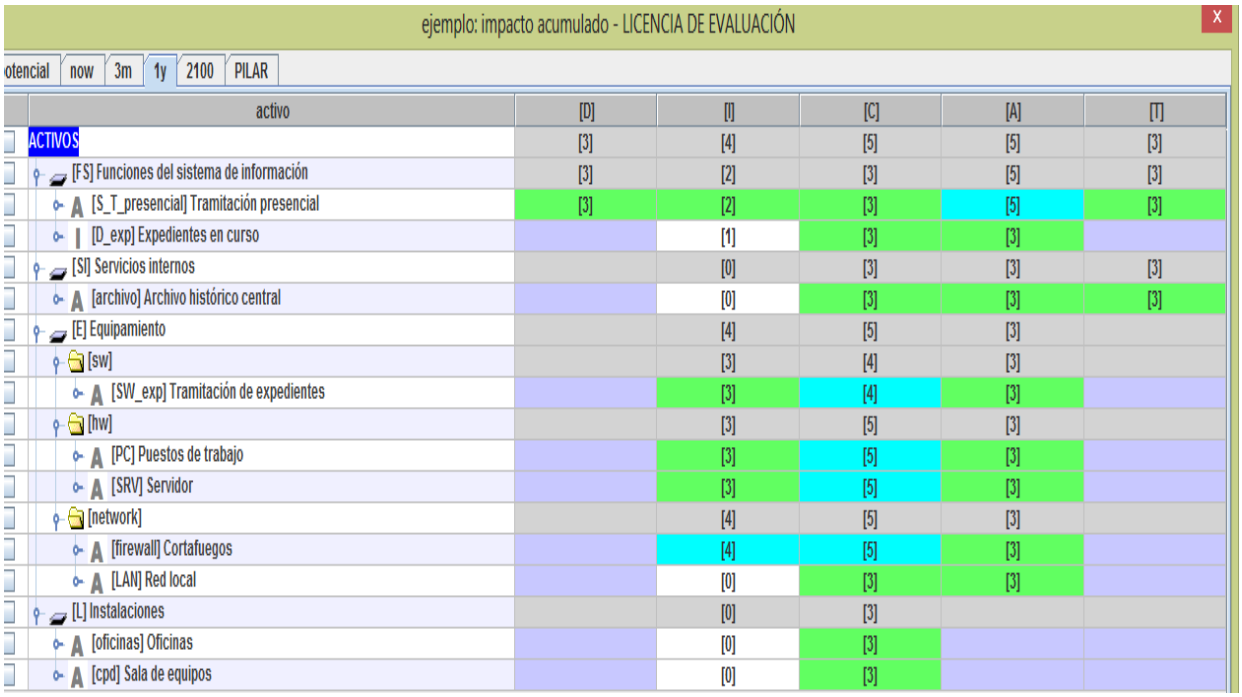
• Debería hacerse un seguimiento de las cuentas de los usuarios externos, al menos detectando largos periodos de inactividad, intentos de penetración y comportamientos anómalos en general.

• El uso de contraseñas como mecanismo de autenticación se considera "débil", recomendándose el uso de tarjetas criptográficas de identificación.

En este punto se obtiene el "Informe de Insuficiencias" de la organización.

4.6. Estimación del estado de riesgo:

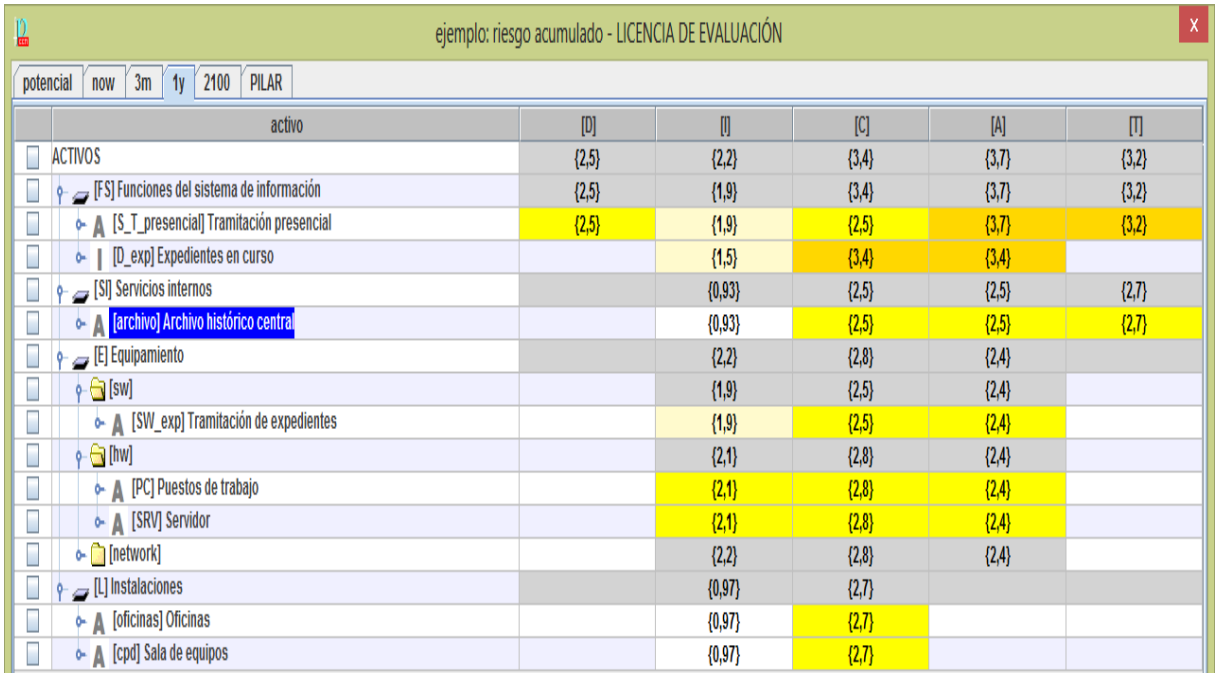
Conocidos el "Modelo de Valor", el "Mapa de Riesgos" y la "Evaluación de Salvaguardas" se procede a la estimación de los indicadores de impacto y riesgo, tanto acumulado (sobre los activos inferiores) como repercutido (sobre los activos superiores).



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[3]	[4]	[5]	[5]	[3]
[FS] Funciones del sistema de información	[3]	[2]	[3]	[5]	[3]
[S_T_presencial] Tramitación presencial	[3]	[2]	[3]	[5]	[3]
[D_exp] Expedientes en curso		[1]	[3]	[3]	
[SI] Servicios internos		[0]	[3]	[3]	[3]
[archivo] Archivo histórico central		[0]	[3]	[3]	[3]
[E] Equipamiento		[4]	[5]	[3]	
[sw]		[3]	[4]	[3]	
[SW_exp] Tramitación de expedientes		[3]	[4]	[3]	
[hw]		[3]	[5]	[3]	
[PC] Puestos de trabajo		[3]	[5]	[3]	
[SRV] Servidor		[3]	[5]	[3]	
[network]		[4]	[5]	[3]	
[firewall] Cortafuegos		[4]	[5]	[3]	
[LAN] Red local		[0]	[3]	[3]	
[L] Instalaciones		[0]	[3]		
[oficinas] Oficinas		[0]	[3]		
[cpd] Sala de equipos		[0]	[3]		

GRAFICO 17: Impacto Acumulado Residual:

FUENTE: Elaboración propia



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{2,5}	{2,2}	{3,4}	{3,7}	{3,2}
[FS] Funciones del sistema de información	{2,5}	{1,9}	{3,4}	{3,7}	{3,2}
[S_T_presencial] Tramitación presencial	{2,5}	{1,9}	{2,5}	{3,7}	{3,2}
[D_exp] Expedientes en curso		{1,5}	{3,4}	{3,4}	
[SI] Servicios internos		{0,93}	{2,5}	{2,5}	{2,7}
[archivo] Archivo histórico central		{0,93}	{2,5}	{2,5}	{2,7}
[E] Equipamiento		{2,2}	{2,8}	{2,4}	
[sw]		{1,9}	{2,5}	{2,4}	
[SW_exp] Tramitación de expedientes		{1,9}	{2,5}	{2,4}	
[hw]		{2,1}	{2,8}	{2,4}	
[PC] Puestos de trabajo		{2,1}	{2,8}	{2,4}	
[SRV] Servidor		{2,1}	{2,8}	{2,4}	
[network]		{2,2}	{2,8}	{2,4}	
[L] Instalaciones		{0,97}	{2,7}		
[oficinas] Oficinas		{0,97}	{2,7}		
[cpd] Sala de equipos		{0,97}	{2,7}		

GRAFICO 18: Riesgo Acumulado Residual:

FUENTE: Elaboración propia

Ver “Apéndice 4.5. Informe de insuficiencias” del “Catálogo de Elementos”.

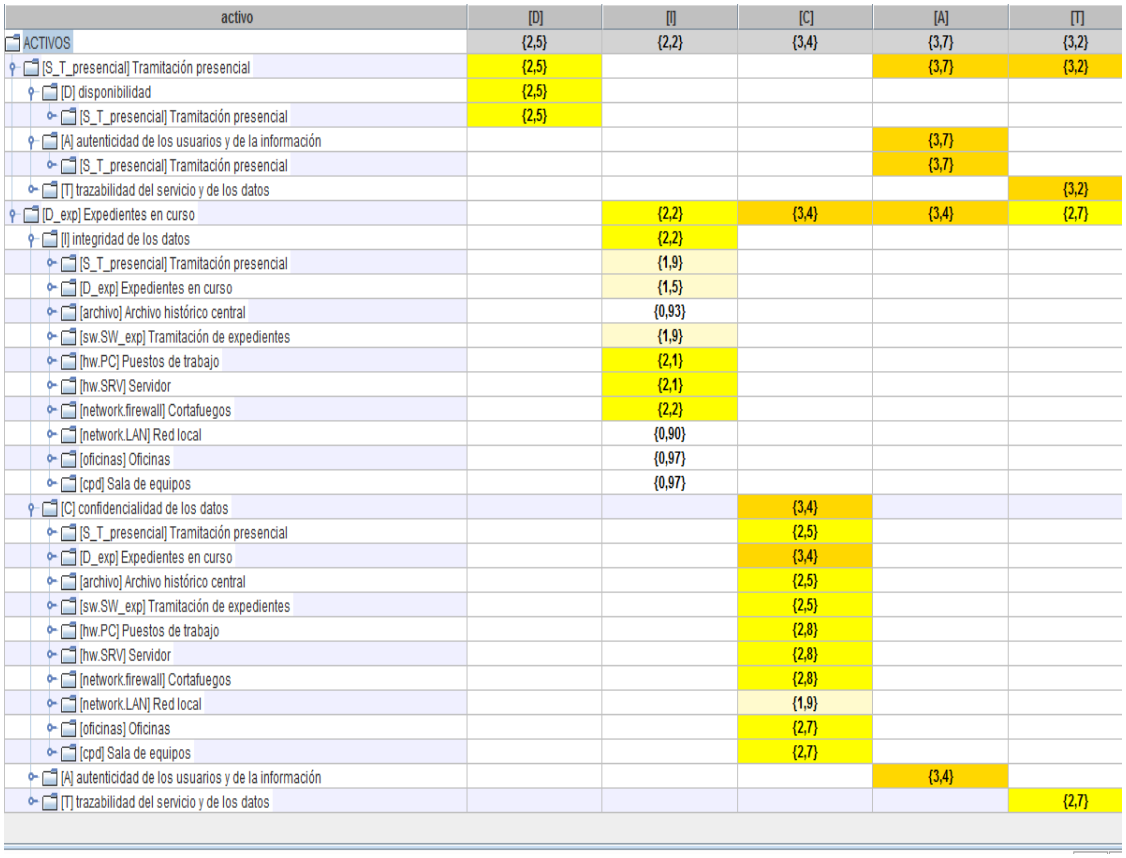
Para el cálculo del impacto residual se sigue lo indicado en la sección “2.1.6. Revisión del paso 4: impacto residual. Véase también la sección “2.2.1. Modelo cualitativo” de la “Guía de Técnicas”.

Para el cálculo del riesgo residual se sigue lo indicado en la sección “2.1.7. Revisión del paso 5: riesgo residual. Véase también la sección “2.1. Análisis mediante tablas” de la “Guía de Técnicas”.

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	[3]	[4]	[5]	[5]	[3]
[S_T_presencial] Tramitación presencial	[3]			[5]	[3]
[D] disponibilidad	[3]				
[S_T_presencial] Tramitación presencial	[3]				
[A] autenticidad de los usuarios y de la información				[5]	
[S_T_presencial] Tramitación presencial				[5]	
[T] trazabilidad del servicio y de los datos					[3]
[D_exp] Expedientes en curso		[4]	[5]	[3]	[3]
[I] integridad de los datos		[4]			
[S_T_presencial] Tramitación presencial		[2]			
[D_exp] Expedientes en curso		[1]			
[archivo] Archivo histórico central		[0]			
[sw.SW_exp] Tramitación de expedientes		[3]			
[hw.PC] Puestos de trabajo		[3]			
[hw.SRV] Servidor		[3]			
[network.firewall] Cortafuegos		[4]			
[network.LAN] Red local		[0]			
[oficinas] Oficinas		[0]			
[cpd] Sala de equipos		[0]			
[C] confidencialidad de los datos			[5]		
[S_T_presencial] Tramitación presencial			[3]		
[D_exp] Expedientes en curso			[3]		
[archivo] Archivo histórico central			[3]		
[sw.SW_exp] Tramitación de expedientes			[4]		
[hw.PC] Puestos de trabajo			[5]		
[hw.SRV] Servidor			[5]		
[network.firewall] Cortafuegos			[5]		
[network.LAN] Red local			[3]		
[oficinas] Oficinas			[3]		
[cpd] Sala de equipos			[3]		
[A] autenticidad de los usuarios y de la información				[3]	
[T] trazabilidad del servicio y de los datos					[3]

GRAFICO 19: Impacto Repercutido Residual

FUENTE:Elaboracion propia



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{2,5}	{2,2}	{3,4}	{3,7}	{3,2}
[S_T_presencial] Tramitación presencial	{2,5}			{3,7}	{3,2}
[D] disponibilidad	{2,5}				
[S_T_presencial] Tramitación presencial	{2,5}				
[A] autenticidad de los usuarios y de la información				{3,7}	
[S_T_presencial] Tramitación presencial				{3,7}	
[T] trazabilidad del servicio y de los datos					{3,2}
[D_exp] Expedientes en curso		{2,2}	{3,4}	{3,4}	{2,7}
[I] integridad de los datos		{2,2}			
[S_T_presencial] Tramitación presencial		{1,9}			
[D_exp] Expedientes en curso		{1,5}			
[archivo] Archivo histórico central		{0,93}			
[sw.SW_exp] Tramitación de expedientes		{1,9}			
[hw.PC] Puestos de trabajo		{2,1}			
[hw.SRV] Servidor		{2,1}			
[network.firewall] Cortafuegos		{2,2}			
[network.LAN] Red local		{0,90}			
[oficinas] Oficinas		{0,97}			
[cpd] Sala de equipos		{0,97}			
[C] confidencialidad de los datos			{3,4}		
[S_T_presencial] Tramitación presencial			{2,5}		
[D_exp] Expedientes en curso			{3,4}		
[archivo] Archivo histórico central			{2,5}		
[sw.SW_exp] Tramitación de expedientes			{2,5}		
[hw.PC] Puestos de trabajo			{2,8}		
[hw.SRV] Servidor			{2,8}		
[network.firewall] Cortafuegos			{2,8}		
[network.LAN] Red local			{1,9}		
[oficinas] Oficinas			{2,7}		
[cpd] Sala de equipos			{2,7}		
[A] autenticidad de los usuarios y de la información				{3,4}	
[T] trazabilidad del servicio y de los datos					{2,7}

GRAFICO 20: Riesgo Repercutido Residual

FUENTE:Elaboracion propia

En este punto se obtiene el "Estado de Riesgo" de la organización. Este "Estado de Riesgo" viene documentado por el informe de "Evaluación de Salvaguardas" que recoge de despliegue actual de seguridad, y el "Informe de Insuficiencias" que recoge las debilidades descubiertas.

4.7. Gestión de riesgos:

4.7.1. Toma de decisiones:

Vistos los indicadores de riesgo residual y las insuficiencias de la unidad, la Dirección decide clasificar en los siguientes niveles los programas de seguridad a desarrollar:

De carácter urgente:
P1: Desarrollar un plan de contingencia

P2: Monitorizar y gestionar las cuentas de usuarios
Consideraciones importantes:
P3.1: Documentar todos los procedimientos de trabajo, revisando los actuales y añadiendo los que falten P3.2: Segregar las funciones del administrador de sistemas
Temas a considerar en el futuro:
• Uso de tarjetas de identificación • Relaciones con el proveedor de comunicaciones para garantizar la calidad del servicio • Contratación de un servicio alternativo de comunicaciones • Medidas frente a ataques de denegación de servicio

TABLA 21: Niveles de Seguridad

FUENTE: Elaboración propia

Ver "Apéndice 4.4. Estado de riesgo" del "Catálogo de Elementos".

Ver "Apéndice 4.5. Informe de insuficiencias" del "Catálogo de Elementos".

Ver "Apéndice 4.6. Plan de seguridad" del "Catálogo de Elementos".

4.8. Plan de seguridad:

Todas las consideraciones anteriores hay que plasmarlas en un "Plan de Seguridad" que organiza las actividades de forma planificada y gestionada.

El desarrollo del plan de contingencia (programa P1) se traduce en un proyecto específico para el que:

1. Este año se realizará una estimación de costes del proyecto y una solicitud de propuestas que se completará con la adjudicación a un contratista externo

2. A la vista de la oferta ganadora se destinarán fondos el año que viene para la realización del plan; en esta realización se incluirán todas las tareas administrativas (dimensionado, selección de soluciones, procedimientos, etc.), exceptuándose las posibles ejecuciones de obra civil o contratación de servicios externalizados de continuidad, que serán objeto de futuras licitaciones

Para la monitorización de cuentas (programa P2) se lanza un proyecto para el desarrollo de un sistema de gestión de cuentas que incluya la detección de intrusiones y el lanzamiento de alarmas.

Se estima que este proyecto se puede lanzar inmediatamente y que su duración será de un año.

Para la documentación de todos los procedimientos (programa P3.1) se recurrirá a una ampliación del contrato de consultoría y asesoramiento que la Organización matriz tiene actualmente. En esta ampliación, consultores externos se encargarán de recabar la información pertinente, completando los manuales actuales. Esta tarea no se acometerá hasta el próximo ejercicio. En la elaboración de procedimientos se definirán las tareas específicas de un operador (local) y un administrador (remoto) de forma que se alcance el objetivo del programa P3.2. Se negocia con archivo central la disposición de un servicio centralizado de administración, dejando a nivel local las meras funciones de operación.

Por último se recaba de la Organización matriz información sobre el uso de tarjetas de identificación, como medios que pudieran utilizarse en el futuro para mejorar la autenticidad de los usuarios. Para el próximo ejercicio se contratará un estudio de las modificaciones requeridas para incorporar dichos mecanismos, tanto para los usuarios internos como para los usuarios externos. Parte de ese estudio será un plan detallado de realización, que en ningún caso se acometerá antes de dos años.

4.9. Evolución de los indicadores de impacto y riesgo:

Las siguientes figuras muestran la evolución de los indicadores de impacto y riesgo, acumulado y repercutido, en tres instantes de la gestión del sistema de información sometido a estudio:

- Sin salvaguardas
- En el momento presente
- Tras la ejecución de los programas P1, P2 y P3 del plan de seguridad

4.9.1. Impacto acumulado:

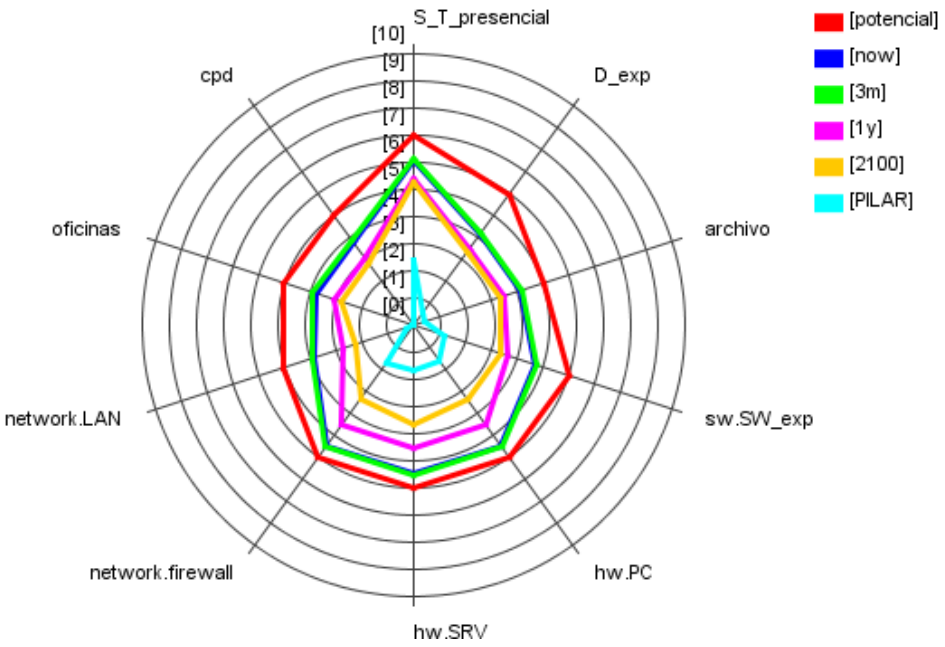


GRAFICO 21: Impacto Acumulado

FUENTE: Elaboración Propia

4.9.2. Riesgo acumulado:

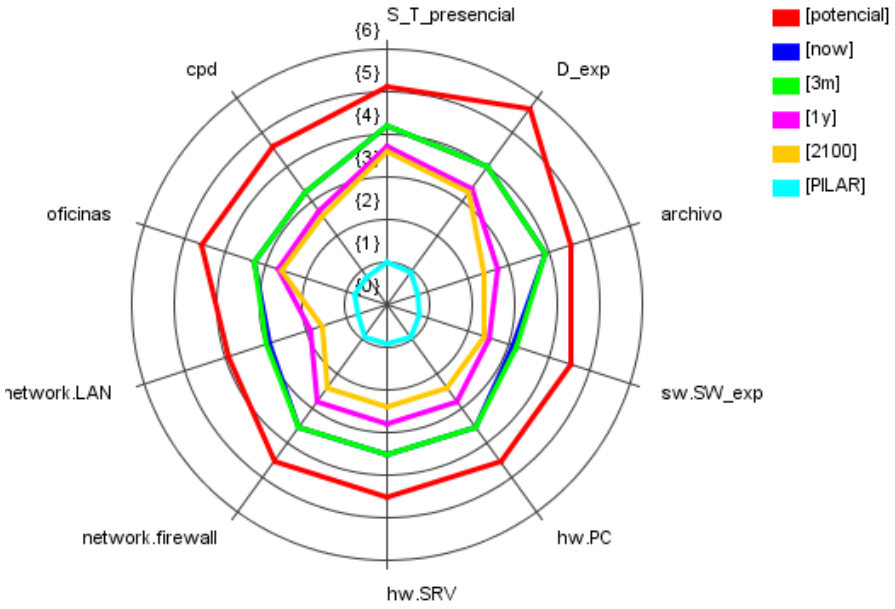


GRAFICO 22: Riesgo acumulado

FUENTE: Elaboración Propia

4.9.3. Impacto repercutido:

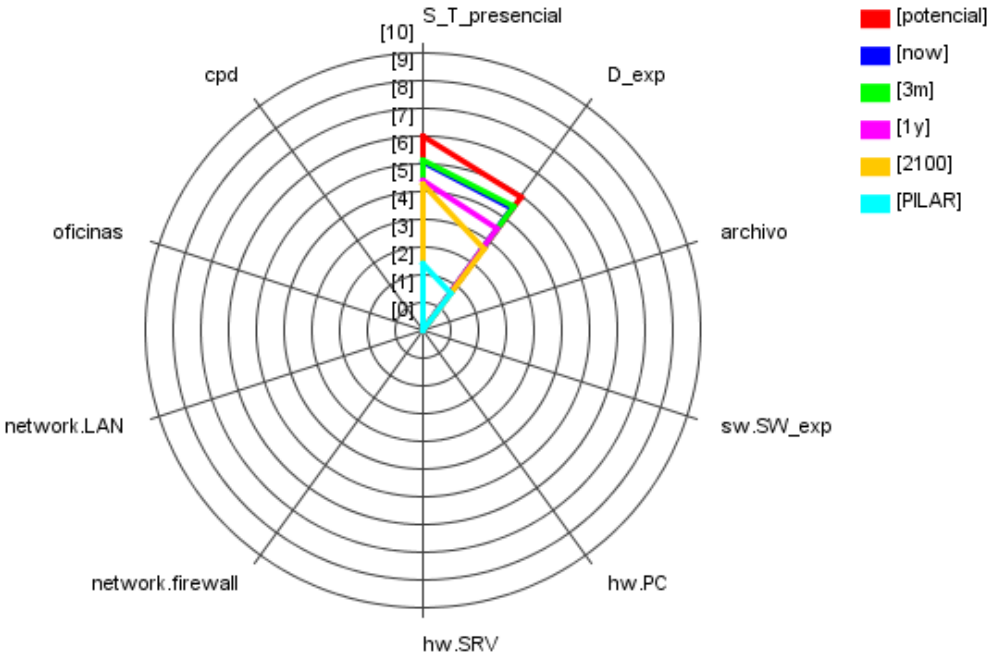


GRAFICO 23: Impacto Repercutido

FUENTE: Elaboración propia

4.9.4. Riesgo repercutido:

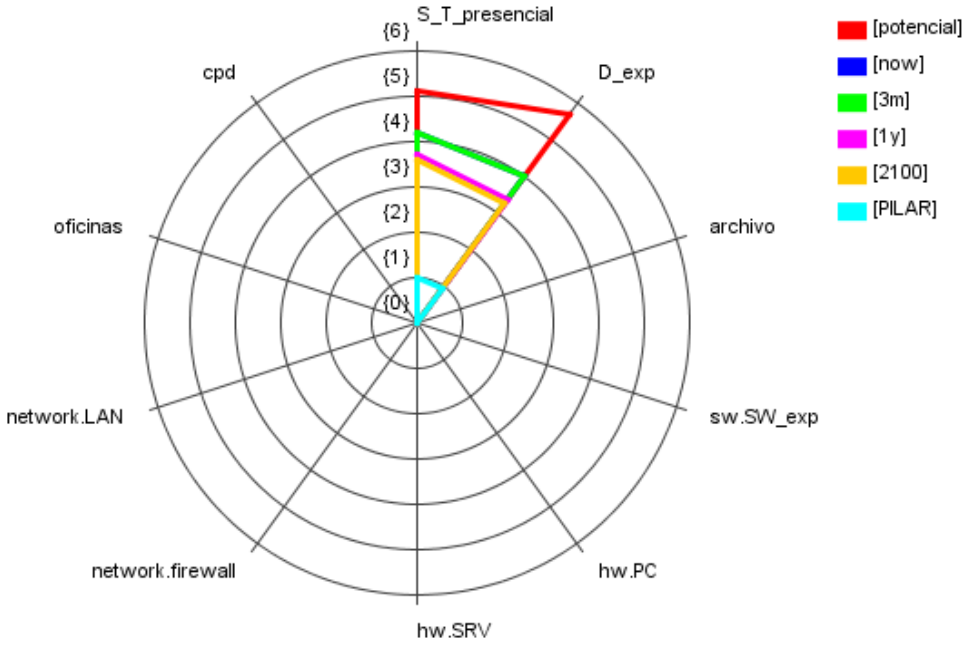


GRAFICO 24: Riesgo repercutido

FUENTE: Elaboración propia

4.10. Diseño de las políticas de seguridad:

Las políticas que se desarrollarán a continuación serán sugerencias propuestas, estas estarán basadas en el análisis de gestión de seguridad de la información realizado, en el cual identificamos las principales vulnerabilidades y amenazas que podrían comprometer la seguridad informática de la empresa.

La creación de las políticas se realizará manteniendo el modelo de dominios ya definido en el capítulo anterior.

4.10.1. Políticas para el dominio de redes:

Las políticas detalladas en este dominio serán responsabilidad del personal de la Unidad de Sistemas de Académicos de la Dirección Información Académica perteneciente a la Universidad Amazónica de Pando, el cual estará a cargo de difundir el reglamento para el uso de la red y de sus componentes, así como también de verificar su cumplimiento.

1. El departamento de Sistemas deberá emitir las normas y los requerimientos para la instalación de servidores de páginas locales, de bases de datos, así como las especificaciones para que el acceso a estos sea seguro. De esta forma se administrará de manera correcta todos los servicios que se brindan en la red.
2. Se debe evitar todo tipo de publicación de información como: nombre de sucursales, ubicaciones, nombre de dispositivos, marcas y demás, mediante etiquetas o en la configuración de los equipos de red tales como: routers, servidores, clientes, etc. De esta forma se evitará que terceras personas conozcan información sobre la red de la institución, lo cual dificultará su acceso.
3. Las contraseñas usadas para la configuración de equipos de redes y telecomunicaciones deberán estar basadas en un estándar que defina aspectos como: estructura, tiempo de validez, reusabilidad, etc. Así daremos mayor seguridad a todos los dispositivos informáticos de la empresa, evitando posibles accesos de terceras personas.
4. Borrar todos los usuarios y contraseñas que vienen por defecto en los equipos informáticos usados en la red. De esta forma se dará mayor seguridad a la red evitando el fácil acceso de terceros a la red de la empresa, a través de los equipos de red.

5. Todos los puertos y protocolos de los dispositivos utilizados en la red, que no estén en uso deberán ser bloqueados adecuadamente. Así se le dará mayor protección a la red, evitando ataques ya sean internos o externos, y al mismo tiempo se facilitará la administración de la red.

6. Se deberá llevar un documento que registre todas las configuraciones que se realicen sobre los dispositivos de red. De esta forma se facilitará y agilizará el proceso de reparación o mantenimiento de los dispositivos de red, más aun cuando los responsables de estos equipos no estén.

7. Al momento de diseñar la red se deberá considerar todas las seguridades y ventajas que los equipos de red estén en capacidad de proveer. De esta manera se obtendrá el máximo desempeño de los recursos de red utilizados, mejorando considerablemente la seguridad, la administración, y facilidad de mantenimiento.

8. Todos los dispositivos de red deberán estar correctamente salvaguardados, tomando en cuenta aspectos como ubicación, protección física y suministro eléctrico (de ser necesario). De esta forma se pretende proteger los dispositivos en lo que a riesgos de tipo físico se refiere, evitando así su deterioro o daños irreparables

9. La ubicación de todos los dispositivos de red deberán seguir en lo posible estándares de medidas y ubicación lo cual facilitará su disponibilidad para mantenimiento o reparación. De esta forma se evitará la pérdida de tiempo o complicaciones al momento de dar mantenimiento a los dispositivos de red.

10. El personal que realiza las configuraciones de los dispositivos de red deberá poseer una certificación o título que avale sus capacidades y conocimientos. De esta forma se garantizará el trabajo realizado, evitando posibles fallas que comprometan a la red de la empresa.

11. Todos los enlaces de red sean estos fijos o redundantes, a través de medios guiados o no, deberán ser probados rigurosamente con el fin de garantizar su servicio. De esta forma se garantiza la conexión entre los dispositivos de red y que la transmisión de datos sea confiable, evitando así la interrupción de servicios.

12. Se debe definir un proceso de reemplazo de equipos, ya sea manteniendo acuerdos con proveedores (precios, tiempo de reposición, disponibilidad) o de ser posible tener

uno de respaldo en bodega. Así el tiempo de suspensión de los servicios que el equipo provee será corto y se mantendrá la continuidad del negocio.

13. Se debe implementar enlaces redundantes de las conexiones más importantes para la red interna de la organización. De esta forma se mantendrán disponibles los servicios de la red, evitando la pérdida de datos y demoras en transmisión que puedan afectar la continuidad del negocio.

14. Todo el cableado y los puntos de acceso a la red deberán ser protegidos adecuadamente, y aquellos puntos que no estén en uso tendrán que ser bloqueados o restringidos apropiadamente. Así se evitará el acceso de terceros o personal no autorizado a la red de la empresa.

15. Se debe llevar una correcta organización de los cables que interconectan los equipos informáticos y dispositivos de red. Así se pretende mantener un orden con los dispositivos de red que faciliten su administración y mantenimiento.

16. Todo tipo de etiqueta o señalización que muestre información de los dispositivos deberá ser ubicada en lugares estratégicos que impida su visualización por terceros. Así se evitará que terceras personas identifiquen fácilmente servicios y dispositivos para atacarlos.

17. De ser posible, la empresa deberá contar con una instalación auxiliar acondicionada adecuadamente para albergar sus equipos informáticos.

Con esta política se pretende darle continuidad al negocio en el caso de que las instalaciones informáticas de la empresa colapsen o no se pueda acceder a las instalaciones.

18. La Unidad de Sistemas Académicos en coordinación con la Unidad de Sistemas de Información y Comunicación será el único responsable de proporcionar a los usuarios el acceso a los servicios de red y recursos informáticos. De esta forma se facilitará la administración de usuarios y de los servicios de red, al mismo tiempo se crea una medida de protección ante ataques malintencionados o no.

19. El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos, equipo de cómputo centralizado y distribuido, etc.) conectado a la red será administrado por la Unidad de Sistemas Académicos en coordinación con la unidad de sistemas de información y comunicación. De esta forma se facilitará la administración

y control de acceso usuarios y de los servicios de red, ya que ambas unidades tiene los conocimientos necesarios para llevar estas actividades a cabo.

20. A los responsables de los servidores de Web corresponde la verificación de respaldo y protección adecuada. De esta forma se pretende proteger la red del Sistema Académico Siringuero de posibles ataques externos y mantener la información bien salvaguardada.

21. Todo software que maneje autenticación debe cifrar la información que circule a través de la red. Esto evitara que terceras personas puedan leer fácilmente la información confidencial que circula en la red.

4.10.2. Políticas para el dominio de hardware:

Las políticas detalladas en este dominio serán responsabilidad del personal de la Unidad de Sistemas de Académicos de la Dirección Información Académica perteneciente a la Universidad Amazónica de Pando, el cual estará a cargo de difundir el reglamento para el uso de los dispositivos de hardware, así como también de verificar su cumplimiento.

22. A la Unidad de Sistemas Académicos le corresponde la realización del mantenimiento periódico preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico.

Para lo cual se debería crear un procedimiento formal (fechas, responsables, informe escrito) que especifique la forma en la que se realizará este mantenimiento. De esta forma se evitará la pérdida de tiempo o complicaciones al momento de dar mantenimiento a los dispositivos, prolongando su vida útil, evitando que personal que no tenga conocimiento técnico manipule los equipos.

23. Todos los equipos y dispositivos que estén o no en uso tanto de redes, como de hardware en general, deberán estar almacenados en un lugar seguro frente a robos, accesos no autorizados y eventualidades que puedan averiarlos. De esta manera se pretende proteger físicamente a todos los dispositivos de la organización.

24. Se deberá llevar un inventario de todos los equipos y dispositivos que formen parte del sistema informático, estén o no en uso, este inventario deberá ser actualizado periódicamente, debe incluir parámetros como: fecha de adquisición, proveedor, modelo, manual técnico y de usuario, responsable, garantía, y demás aspectos que el

departamento crea conveniente. De esta forma se podrá administrar con facilidad los activos del Sistema Académico Siringuero, conocer su estado actual y disponibilidad en bodega.

25. Todo el hardware que posee el Sistema Siringuero, esté en uso o no, debe estar acompañado de un documento que describa la configuración y estado actual del equipo, así como de posibles advertencias sobre el buen uso del mismo. De esta forma se pretende lograr la manipulación adecuada de los equipos, y rapidez en su mantenimiento.

26. Cerca de todos los equipos se deberá ubicar un extintor adecuado, y de no ser posible, al menos cerca de los equipos más importantes, se debe tomar en cuenta que los extintores sean para uso de equipos eléctricos.

De esta manera se protegerá la seguridad de los equipos en caso de un incendio.

27. Los lugares en los que se ubiquen dispositivos de hardware deben poseer todas las advertencias necesarias que informen sobre uso, manipulación y prohibiciones. De esta forma se pretende salvaguardar los recursos de la empresa ante posibles daños ocasionados por accesos no autorizados, o mal uso de equipos.

28. Todos los dispositivos y periféricos ubicados en la zona central deberán ser en lo posible completamente protegidos ante posibles daños físicos y manipulación de personal no autorizado. De esta manera se pretende proteger adecuadamente a todos los equipos utilizados en el área de producción para evitar la suspensión de sus procesos y al mismo tiempo alargar la vida útil de los equipos.

29. Le corresponde a la Unidad de Sistemas Académicos dar a conocer las listas de las personas, que puedan tener acceso a los equipos y a las áreas de acceso no autorizado. Así se evitará confusiones pues los empleados de la empresa conocerán las áreas a las que pueden ingresar y a las que no, incrementando la seguridad en los departamentos y áreas de la empresa.

30. Se deberá establecer un control en las áreas principales donde se ubican los dispositivos de gran importancia como: cuartos de servidores, el cual deberá registrar todas las todas las actividades realizadas por el personal que accede a estas. De esta manera se llevará un control y se conocerá factores como: ¿quién?, ¿para qué? y ¿a qué hora?, ingreso a estas áreas a manipular los dispositivos.

31. Las puertas y ventanas de los lugares que albergan equipos informáticos deberán ser protegidos y revisados constantemente (vidrios rotos, chapas en mal estado, protecciones, etc.). De esta forma se asegurará la protección de los equipos ubicados en estos lugares y se evitará el acceso no autorizado.

32. La reubicación del equipo de cómputo se realizará satisfaciendo las normas y procedimientos de la Unidad de Sistemas Académicos, se hará únicamente bajo la autorización de dicha Unidad o los responsables designados, se deberá documentar dicho proceso con aspectos como: razones de reubicación, nombre de responsable, equipos reubicados, etc. Este punto facilitara la administración del hardware que el departamento de sistemas maneja.

33. Todos y cada uno de los equipos serán asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos. De esta se mejorará la administración de los recursos y se facilitará su mantenimiento.

34. Queda estrictamente prohibido dar mantenimiento a equipo de cómputo que no es propiedad de la institución. De esta forma se evitará problemas con los empleados ya que estos únicamente realizarán las labores que les corresponde dentro de la empresa.

4.10.3. Políticas para el dominio de software:

Las políticas detalladas en este dominio serán responsabilidad del personal de la Unidad de Sistemas de Académicos de la Dirección Información Académica perteneciente a la Universidad Amazónica de Pando, el cual estará a cargo de difundir el reglamento para el uso y mantenimiento del software, así como también de verificar su cumplimiento.

35. Toda pc utilizado en el Sistema Siringuero debe tener configurada la opción de cierre de sesión después de un lapso (determinado por la Unidad de sistemas) de inactividad. De esta manera se evitará el acceso de usuarios no autorizados a estos computadores, previniendo la pérdida de información.

36. Debe haber una correcta administración de todos los usuarios que tienen acceso a un dispositivo o equipo y los privilegios sobre el sistema operativo y las aplicaciones que opera. Así se llevará una correcta administración de los usuarios y de los equipos, previniendo el mal uso de los mismos.

37. Corresponde a la Unidad de Sistemas emitir las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo. De esta manera se protegerá a todos los dispositivos del Sistema Siringuero, se evitara que los usuarios instalen software malicioso que perjudique a la empresa y se mejorará el control ya que se conocerá que software está permitido y cual no.

38. En los equipos de cómputo, dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y de acorde a la propiedad intelectual. Así se evitará el uso de aplicaciones o software inútil que provoque el mal uso de los recursos o perdida de información.

39. Con el propósito de proteger la integridad de los sistemas informáticos, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, y otros que se apliquen). De esta manera se pretende brindar mayor protección al Sistema Siringuero, evitando la proliferación de virus que puedan suspender los servicios de red u ocasionen pérdida o fugas de información.

40. Todo software nuevo antes de ponerlo en uso debe ser probado y evaluado correctamente antes de ponerlo en funcionamiento. De esta forma se evitará el uso de software defectuoso que pueda poner en peligro la integridad o perdida de la información.

41. Se debe realizar periódicamente revisiones del funcionamiento del software e instalación de actualizaciones en caso de que existan. Así se pretende aprovechar al máximo el rendimiento de los equipos y prolongar su tiempo de vida útil.

42. El Sistema Académico Siringuero deberá presentar mensajes de error claros que puedan ser interpretados fácilmente por sus usuarios.

De esta manera se pretende evitar la pérdida de tiempo al solucionar los errores que presente el sistema, y que éste sea utilizado de una forma adecuada.

43. Todo software utilizado en la empresa deberá en lo posible tener un manual técnico y de usuario que facilite su uso y mantenimiento. En caso de compra se deberá exigir a sus proveedores, en el caso que esto no sea posible se lo diseñará, y, si el software es creado por la unidad los desarrolladores deberán realizar el manual correspondiente. De esta manera se pretende que el software empleado en la organización sea utilizado

correctamente, y que cualquier manteniendo o reparación se lo realice en el menor tiempo posible.

44. La Unidad de Sistema Académico es el responsable de realizar revisiones periódicas para asegurar que sólo programas permitidos estén instalados en las computadoras de la institución. De esta forma se verificara el correcto uso de los computadores y de los recursos informáticos brindados a los usuarios, evitando que programas con código malicioso pongan en peligro los servicios de red.

45. Todos los sistemas programados (programas, bases de datos, sistemas operativos, interfaces) o desarrollados con o a través de los recursos de la institución y la Unidad de Sistemas Académicos se mantendrán como propiedad de la institución. De esta manera se evitará que los recursos sean mal utilizados.

4.10.4. Políticas para el dominio de datos:

Las políticas detalladas en este dominio serán responsabilidad del personal de la Unidad de Sistemas de Académicos de la Dirección Información Académica perteneciente a la Universidad Amazónica de Pando, el cual estará a cargo de promover y difundir el reglamento para el buen uso, respaldo y salvaguarda de los datos digitales o impresos, así como también de verificar su cumplimiento.

46. Todos los datos de gran importancia para la empresa deberán ser respaldados. De esta manera se protegerá la información y en caso de desastre se pueda continuar con el negocio.

47. Todos los respaldos realizados deben estar almacenados en un lugar seguro. De esta manera se pretende proteger físicamente todos los respaldos de la organización que apoyarán la continuidad del negocio.

48. Todo el personal de la empresa o externo a ella, que manipule información sensible, o respaldos deberá comprometerse a protegerla o firmar un acuerdo de no divulgación. De esta manera se evitará la perdida, robo, daño y mal uso de la información y también se concientizará al personal de la empresa sobre la importancia del manejo adecuado de esta.

49. Todos los datos, tanto originales como de respaldo deberán ser revisados periódicamente. Así se pretende mantener la información segura, integra y disponible para cuando se la necesite.

50. Se debe incorporar a la base de datos un proceso que registre todos los accesos y las actividades realizadas. Así se podrá conocer todo lo que pase dentro de la base de datos, y detectar fácilmente posibles agresores.

51. Se debe implementar un mecanismo formal que administre y controle la eliminación de información lógica y física. De esta forma evitaremos el mal uso de la información que la empresa descarte.

52. Toda la información que se maneja el Sistema Académico Siringuero deberá estar clasificada según los parámetros que la Unidad de sistemas crea conveniente. De esta manera se facilita su administración y manipulación.

53. Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución deben estar resguardados.

De esta manera se protegerán adecuadamente los datos manejados en los distintos procesos de la empresa.

54. Cualquier software que requiera ser instalado para trabajos dentro de la institución deberá ser evaluado por el personal de la Unidad de Sistemas Académicos. De esta manera se mantendrá un control adecuado sobre el software que debe o no ser utilizado, y se garantizará a los usuarios que las aplicaciones funcionen adecuadamente.

55. Todo el sistema propiedad de la institución deberá ser usado exclusivamente para asuntos relacionados con las actividades de esta. Así se evitará que el sistema de la empresa sea mal utilizado.

4.10.5. Políticas para el dominio de sistema eléctrico:

Las políticas detalladas en este dominio serán responsabilidad del personal de la Unidad de Sistemas de Académicos de la Dirección Información Académica perteneciente a la Universidad Amazónica de Pando, el cual estará a cargo de difundir el reglamento para el buen uso y mantenimiento de los componentes relacionados al sistema eléctrico, así como también de verificar su cumplimiento.

56. Toda toma eléctrica y equipo de alimentación auxiliar deben estar protegidos adecuadamente. Así se evitará que estos sean desconectados por descuido o intencionalmente, evitando que los equipos a los cuales suministra energía dejen de funcionar.

57. Todo cable o toma eléctrica que no esté en uso debe ser aislada correctamente. De esta forma evitamos posibles cortocircuitos, o demás peligros relacionados con la energía eléctrica que comprometan la continuidad del negocio.

4.10.6. Políticas para el dominio de talento humano:

Las políticas detalladas en este dominio serán responsabilidad del personal de la Unidad de Sistemas de Académicos de la Dirección Información Académica perteneciente a la Universidad Amazónica de Pando, debido a que son políticas de seguridad informática, aunque se puede interactuar con otras unidades que se crean convenientes, los cuales estarán a cargo de difundir el reglamento para el buen uso y mantenimiento de los componentes relacionados al sistema eléctrico, así como también de verificar su cumplimiento.

Debido al carácter confidencial de la información, el personal de la organización deberá de conducirse de acuerdo a los códigos de ética profesional y normas y procedimientos establecidos.

58. Todo el personal de la empresa sin importar el cargo que desempeñe dentro de ella, deberá ser informado de la importancia de la seguridad información y de la seguridad en general para la organización. De esta forma se hará conciencia de la importancia de su participación y colaboración en todo el proceso de desarrollo.

59. Es necesario que todos los empleados tengan conocimiento de los bienes más importantes de le empresa. De esta forma los empleados pueden ayudar a salvaguardar dichos activos.

60. Se debe concientizar a los empleados de la institución sobre la importancia y las responsabilidades de la información que manipulan.

Así cada empleado tendrá los cuidados adecuados de la información que utilizan.

61. Toda persona, empleado fijo que manipule información de la empresa deberá firmar un contrato de no divulgación. Con esto se pretende proteger la información, de tal forma que esta no sea utilizada en contra de la integridad de la empresa.

62. Todos los privilegios, claves y permisos otorgados a los empleados deben ser bloqueados o eliminados luego de que estos terminen sus actividades de forma definitiva. En caso de terminar el contrato en malos términos se impedirá que el personal despedido acceda y dañe la información de la empresa o que otras personas accedan a los datos de estos usuarios.

63. Los empleados de la empresa deben estar conscientes de la correcta manipulación de alimentos dentro y fuera de las áreas permitidas. Así se evitarán posibles daños a los equipos o a la información con la que los empleados trabajan.

64. Queda terminantemente prohibido cualquier tipo de actividad o celebración dentro de las áreas en las cuales existen equipos, dispositivos o información de la institución. Ya que estos equipos pueden resultar dañados y provocar suspensión de servicios u ocasionar la parra de la producción.

65. El documento que contiene las políticas de seguridad deber ser difundido a todo el personal involucrado en la definición de estas políticas. De esta manera se mantendrá informado al personal de la empresa de lo que puede o no puede hacer, lo cual facilitará la implementación del proceso de seguridad de la información.

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1.CONCLUSIONES:

Aplicando herramientas, metodologías de investigación y el correcto análisis de riesgo se ha logrado determinar que el Sistema Académico Siringuero de la U.A.P (Universidad Amazónica de Pando), de acuerdo a la escala establecida en las dimensiones de valoración de riesgos posee un nivel de riesgo alto.

Tomando en cuenta la gran importancia que tiene un análisis de gestión de riesgos, se ha llegado a determinar para el diseño de políticas de seguridad de la Información:

A la Universidad Amazónica de Pando "Sistema Siringuero" se recomienda aplicar medidas de seguridad guiados y documentados, por lo cual este estudio será de gran beneficio para minimizar riesgos en el futuro.

Gracias a la Metodología Magerit donde se ha seguido una serie de pasos estructurados para el análisis y gestión de riesgos, fase fundamental en este estudio ya que se obtuvo resultados realistas del estado de riesgo actual en la empresa donde se supo escoger que medidas serán necesarias para mitigar el riesgo dando como resultado el diseño de políticas de seguridad de la Información.

La herramienta PILAR fue de gran ayuda en la obtención de resultados, en este **Proyecto de Tesis** ya que ayudo en la valoración de los riesgos en diferentes etapas potencial, situación actual y objetivo. Gracias a esta aplicación se supo de manera directa que mecanismos de seguridad se tiene que implementar en esta institución "Universidad Amazónica de Pando" (**Sistema Siringuero**).

5.2.RECOMENDACIONES:

Se recomienda que haya una revisión periódica de las amenazas y riesgos ya que la tecnología está cambiando continuamente y deben ser controlados para evitar futuros problemas.

Se sugiere al Responsable de la entidad contar con personal con experiencia en la implementación de salvaguardas que se encarguen del análisis de riesgos.

Para reducir los riesgos que existen en los activos de la empresa se recomienda tener administración completa de los sistemas de red de datos y otros sistemas telemáticos de esa forma mejora el mantenimiento de equipos.

Así mismo de capacitar y concientizar al personal la importancia del cumplimiento de las políticas de seguridad como parte de la gestión de riesgos, para la institución.

Bibliografía:

Vargas Avilés, J. R. (2009). *Conceptos de Auditoria informatica.*

Academia de administracion y Sociales. (2011). *Auditoria Informatica.*

Argollo, E. (2007). *Como ser Feliz.* Cobija: Bruño.

ASCENDIA. (s.f.). *Sistemas de Gestion de la Seguridad de la Informacion ISO/IEC 27001:2005.*

Belloch, C. (s.f.). *las tecnologias de informacion y comunicacion en el aprendizaje.*

Gomes Fernandez, L., & Alvarez, A. A. (2012). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de informacion para pymes.* AENOR.

INTECO. (2008). *Guia avanzada de gestion de riesgos.* LNCS.

Leon, U. (2004). *Auditoria Informatica.*

Lopez Cuenca, D. (2012). *Analisis de Riesgos Dinamicos en Sistemas de Informacion.* Madrid-España.

Merino Bada, C., & Cañizares Sales, R. (s.f.). *Implantacion de un Sistema de Seguridad de la Informacion segun ISO 27001.* Madrid: Fundacion Confemetal.

OSILAC. (2004). *Medición de la Sociedad de la Información en América Latina y el Caribe.* Santiago de Chile.

Perez, E. (s.f.). *Sistema de Gestion de Seguridad de la Informacion* .

Ribadas Pena, F. J. (2010). *Test de Intrusion.*

Santiago Chinchilla, E. J. (2009). *Test de penetración como apoyo a la evaluación.*

Ureña Leon, E. E. (s.f.). *Sistema de Gestion de la Seguridad de la Informacion* .

Villena Aguilar, M. A. (2006). *Sistemas de Gestion de la Seguridad de la Informacion.*

ANEXOS

ANEXO A

SOLICITUD

SOL. USC: 005/10

A: Ing. Abel Huaygua
Director de la Dirección de información Académica

REF:. Permiso de desarrollo de encuesta

FECHA: 18 de Noviembre de 2014

De mi mayor consideración mediante la presente me dirijo hacia su persona por el motivo de pedirle su ayuda urgente como Director de la Dirección de Información Académica (**DIA**).

Para poder realizar mi trabajo de campo en su Dirección, el cual consiste en obtener datos, para posteriormente realizar un análisis de riesgos, aplicando instrumentos de investigación, para mi Modalidad de Graduación (Tesis) el cual abarca como tema : ´Sistema de Gestión de Seguridad de la Información para el Sistema Siringuero´.

Esto ayudara en la identificación del nivel de seguridad con la que cuenta el Sistema Siringuero, dando de esta manera el punto inicial para que en posterioridad este sistema pueda ser certificado bajo la norma de la ISO/IEC 270001
Sin otro motivo nos despedimos cordialmente, deseándole éxitos en la labor que cumple y esperando una respuesta.

"POR UN FUTURO PRODUCTIVO"

Jnvi. Marcos Roman Rojas Choque
Carrera Ing. de Sistemas
Ru:5322

Ing. Juan Carlos Gallardo Jiménez
Docente Tutor de la Taller de Modalidad de Graduación II

Cc./archivoOMRH

Ing. Pedro C. Vázquez Pérez
Coordinador de la Carrera de Ingeniería de Sistemas

UNIVERSIDAD AMAZONICA DE PANDO
AREA DE CIENCIAS Y TECNOLOGIA
COBIJA - BOLIVIA

Universidad Amazónica de Pando
DIRECCIÓN DE INFORMACIÓN ACADÉMICA
RECIBIDO
Cobija, 18 NOV 2014
Horas: 16:57
Firma:

[lpo] Obligaciones legales		
9	9.lro	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	probablemente sea causa de incumplimiento de una ley o regulación
3	3.lro	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	1.lro	pudiera causar el incumplimiento leve o técnico de una ley o regulación
[si] Seguridad		
10	10.si	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.si	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.si	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización
[po] Orden público		
9	9.po	alteración seria del orden público
6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales

[cei] Intereses comerciales o económicos		
9	9.cei.a	de enorme interés para la competencia
	9.cei.b	de muy elevado valor comercial
	9.cei.c	causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	causa de muy significativas ganancias o ventajas para individuos u organizaciones
	9.cei.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial
	7.cei.c	causa de graves pérdidas económicas
	7.cei.d	proporciona ganancias o ventajas desmedidas a individuos u organizaciones
	7.cei.e	constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
3	3.cei.a	de cierto interés para la competencia
	3.cei.b	de cierto valor comercial
	3.cei.c	causa de pérdidas financieras o merma de ingresos
	3.cei.d	facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	de bajo interés para la competencia
	2.cei.b	de bajo valor comercial
1	1.cei.a	de pequeño interés para la competencia
	1.cei.b	de pequeño valor comercial
0	0.3	supondría pérdidas económicas mínimas

[adm] Administración y gestión		
9	9.adm	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	7.adm	probablemente impediría la operación efectiva de la Organización
5	5.adm	probablemente impediría la operación efectiva de más de una parte de la Organización
3	3.adm	probablemente impediría la operación efectiva de una parte de la Organización
1	1.adm	pudiera impedir la operación efectiva de una parte de la Organización

[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones

[crm] Persecución de delitos		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos

[lbl.nat] Información clasificada (nacional)		
10	10.lbl	Secreto
9	9.lbl	Reservado
8	8.lbl	Confidencial
7	7.lbl	Confidencial
6	6.lbl	Difusión limitada
5	5.lbl	Difusión limitada
4	4.lbl	Difusión limitada
3	3.lbl	Difusión limitada
2	2.lbl	Sin clasificar
1	1.lbl	Sin clasificar

ANEXO B

MODELO DE VALOR

A4.1. Modelo de valor

Caracterización del valor que representan los activos para la Organización así como de las dependencias entre los diferentes activos.

1. Identificación del proyecto
   Código, descripción, propietario, organización.
   Versión, fecha.
   Biblioteca de referencia.
2. Activos
   2.1. Árbol de activos (relaciones de dependencia)
   2.2. Valoración de los activos (valor propio)
      Indicando la razón de la valoración atribuida a cada activo en cada dimensión.
3. Descripción detallada
   Para cada activo:
   - clasificación (ver capítulo 2)
   - activos superiores e inferiores
   - valoración: valor propio y acumulado en cada dimensión

MAPA DE RIESGOS:

A4.2. Mapa de riesgos

Relación de las amenazas a que están expuestos los activos.

1. Identificación del proyecto
   Código, descripción, propietario, organización.
   Versión, fecha.
   Biblioteca de referencia.
2. Activos
   2.1. Árbol de activos (relaciones de dependencia)
   2.2. Valoración de los activos (valor propio)
      Indicando la razón de la valoración atribuida a cada activo en cada dimensión.
3. Amenazas por activo
   Para cada activo:
   - amenazas relevantes (ver capítulo 5)
   - degradación estimada en cada dimensión
   - frecuencia anual estimada
4. Activos por amenaza
   Para cada amenaza:
   - activos afectados
   - degradación estimada en cada dimensión
   - frecuencia anual estimada

CUESTIONARIOS:

ANEXO C

U.A.P.	FORMULARIO DE CUESTIONARIO (TRABAJO DE CAMPO)	FORM-ACYT-010 VERSIÓN No. 1

DATOS GENERALES DE LA PERSONA

NOMBRE COMPLETO:	INSTITUCION : **Universidad Amazónica de Pando**
CARGO:	UNIDAD: .....

DATOS GENERALES DE LA INSTITUCIÓN

Tomar en cuenta que si su respuesta es ¨ sí ¨ especifique su repuesta como tal.

DATOS/INFORMACION:

1. ¿Hace la utilización de ficheros que le permita almacenar la información con la que trabaja el sistema?

Sí ☐ No ☐

Especifique: _____

2. ¿Maneja Copias de Seguridad sobre la información con la que trabaja el sistema?

Sí ☐ No ☐

Especifique: _____

3. ¿Realiza datos de Configuración respecto al sistema?

Sí ☐ No ☐

Especifique: _____

4. ¿Trabaja con datos de Gestión Interna?

Sí ☐ No ☐

Especifique: _____

5. ¿La información con la que trabaja el sistema se realiza mediante el uso de credenciales (contraseñas)?

Sí ☐ No ☐

Especifique: _____

6. ¿El sistema trabaja con datos de control de acceso?

Sí ☐ No ☐

Especifique: _____

7. ¿Se realiza un registro de actividad cuando el sistema realiza un proceso?

Sí ☐ No ☐

Especifique: _____

SERVICIOS:

8. ¿El ingreso al sistema se puede realizar sin requerir identificación de usuario?

Sí ☐ No ☐

Especifique: _____

9. ¿El sistema presta servicios a toda persona en general sin alguna relación contractual?

Sí ☐ No ☐

Especifique: _____

10. ¿El sistema presta servicios a personas externas bajo una relación contractual?

Sí ☐ No ☐

Especifique: _____

11. ¿El sistema presta servicio a personas internas (usuarios de la propia unidad)?

Sí ☐ No ☐

Especifique: _____

12. ¿El sistema realiza servicios por la red?

Sí ☐ No ☐

Especifique: _____

13. ¿El sistema hace la utilización de correo electrónico?

Sí ☐ No ☐

Especifique: _____

14. ¿El sistema permite trabajar con el protocolo telnet (acceso remoto a cuenta local)?

Sí ☐ No ☐

Especifique: _____

15. ¿El sistema permite realizar el almacenamiento de ficheros?

Sí ☐ No ☐

Especifique: _____

---

16. ¿A través del sistema se puede realizar la transferencia de Ficheros?

Sí ☐ No ☐

Especifique: _____

---

17. ¿El sistema realiza el intercambio electrónico de datos?

Sí ☐ No ☐

Especifique: _____

---

18. ¿El sistema permite realizar el servicio de directorio?

Sí ☐ No ☐

Especifique: _____

---

19. ¿El sistema permite realizar la gestión de identidades?

Sí ☐ No ☐

Especifique: _____

---

20. ¿El sistema permite realizar la gestión de privilegios?

Sí ☐ No ☐

Especifique: _____

21. ¿El sistema para la ejecución de sus servicios ase la utilización de una Infraestructura de Clave Pública (PKI)?

Sí ☐ No ☐

Especifique: _____

SOTFWARE:

22. ¿El sistema fue desarrollado de forma propia?

Sí ☐ No ☐

Especifique: _____

23. ¿El sistema fue desarrollado a medida (subcontratado)?

Sí ☐ No ☐

Especifique: _____

24. ¿El sistema fue desarrollado de forma estándar?

Sí ☐ No ☐

Especifique: _____

25. ¿El acceso al sistema se da a través de un navegador web?

Sí ☐ No ☐

Especifique: _____

26. ¿El sistema trabaja con un servidor de aplicaciones?

Sí ☐ No ☐

Especifique: _____

27. ¿El sistema posee un cliente de correo electrónico?

Sí ☐ No ☐

Especifique: _____

28. ¿El sistema posee un servidor de correo electrónico?

Sí ☐ No ☐

Especifique: _____

29. ¿El sistema cuenta con un servidor de ficheros?

Sí ☐ No ☐

Especifique: _____

30. ¿Para la gestión de datos se ha contemplado el manejo de un Sistema de Gestión de Base de Datos (DBMS)?

Sí ☐ No ☐

Especifique: _____

31. ¿Para la ejecución de sus procesos el sistema contempla el uso de un monitor transaccional?

Sí ☐ No ☐

Especifique: _____

32. ¿El sistema trabaja con aplicaciones de ofimática?

Sí ☐ No ☐

Especifique: _____

33. ¿Para el funcionamiento del sistema se cuenta con antivirus?

Sí ☐ No ☐

Especifique: _____

34. ¿Para el funcionamiento del sistema se cuenta con un Sistema Operativo SO?

Sí ☐ No ☐

Especifique: _____

35. ¿El sistema posee un gestor de máquinas virtuales?

Sí ☐ No ☐

Especifique: _____

36. ¿El sistema posee un servidor de terminales?

Sí ☐ No ☐

Especifique: _____

37. ¿El sistema realiza copias de seguridad?

Sí ☐ No ☐

Especifique: _____

EQUIPAMIENTO INFORMATICO:

38. ¿Para la disponibilidad del sistema se hace la utilización de Equipos grandes (host)?

Sí ☐ No ☐

Especifique: _____

39. ¿Para la disponibilidad del sistema se hace la utilización de Equipos medios (mid)?

Sí ☐ No ☐

Especifique: _____

40. ¿Para la disponibilidad del sistema se hace la utilización de Informática personal (pc)?

Sí ☐ No ☐

Especifique: _____

41. ¿Para la disponibilidad del sistema se hace la utilización de Informática móvil (Mobile)?

Sí ☐ No ☐

Especifique: _____

42. ¿Para la organización de los procesos que tiene el sistema ase la utilización de agendas electrónicas?

Sí ☐ No ☐

Especifique: _____

43. ¿Para la disponibilidad del sistema se hace la utilización de equipamiento de respaldo?

Sí ☐ No ☐

Especifique: _____

44. ¿Para la disponibilidad del sistema se hace la utilización de periféricos?

Sí ☐ No ☐

Especifique: _____

45. ¿Para la disponibilidad del sistema se hace la utilización de medios de impresión?

Sí ☐ No ☐

Especifique: _____

46. ¿Para la disponibilidad del sistema se hace la utilización de scanners?

Sí ☐ No ☐

Especifique: _____

47. ¿Para la seguridad de la información del sistema se hace la utilización de dispositivos criptográficos?

Sí ☐ No ☐

Especifique: _____

48. ¿Para la estabilidad del sistema se hace la utilización de soporte de red?

Sí ☐ No ☐

Especifique: _____

49. ¿Para la estabilidad del sistema se hace la utilización de concentradores (hub)?

Sí ☐ No ☐

Especifique: _____

50. ¿Para la estabilidad del sistema se hace la utilización de conmutadores (switch)?

Sí ☐ No ☐

Especifique: _____

51. ¿Para la estabilidad del sistema se hace la utilización de en caminadores (router)?

Sí ☐ No ☐

Especifique: _____

52. ¿Para la estabilidad del sistema se hace la utilización de puentes de comunicación (bridge)?

Sí ☐ No ☐

Especifique: _____

52. ¿Para la estabilidad del sistema se hace la utilización de corta fuego (firewall)?

Sí ☐ No ☐

Especifique: _____

53.¿Para la estabilidad del sistema se hace la utilización de punto de acceso inalámbrico (wap)?

Sí ☐ No ☐

Especifique: _____

54. ¿Para la estabilidad del sistema se hace la utilización de teléfono ip?

Sí ☐ No ☐

Especifique: _____

REDES DE COMUNICACIÓN:

55. ¿Para el flujo de procesamiento de datos en el sistema se cuenta con una red telefónica?

Sí ☐ No ☐

Especifique: _____

---

56. ¿Para el flujo de procesamiento de datos en el sistema se cuenta con una red digital?

Sí ☐ No ☐

Especifique: _____

---

57. ¿Para el flujo de procesamiento de datos en el sistema se cuenta con una red de datos?

Sí ☐ No ☐

Especifique: _____

---

58. ¿Para el flujo de procesamiento de datos en el sistema se cuenta con una conexión de punto a punto?

Sí ☐ No ☐

Especifique: _____

---

59. ¿Para el flujo de procesamiento de datos en el sistema se cuenta con comunicaciones radios?

Sí ☐ No ☐

Especifique: _____

---

60. ¿Para el flujo de procesamiento de datos en el sistema se cuenta con una red inalámbrica?

Sí ☐ No ☐

Especifique: _____

---

61. ¿Para el flujo de procesamiento de datos en el sistema se cuenta con una conexión satelital?

Sí ☐ No ☐

Especifique: _____

---

62. ¿Para el flujo de procesamiento de datos en el sistema se cuenta con una red local (LAN)?

Sí ☐ No ☐

Especifique: _____

---

63. ¿Para el flujo de procesamiento de datos en el sistema se cuenta con una red metropolitana (MAN)?

Sí ☐ No ☐

Especifique: _____

---

64. ¿Para el flujo de procesamiento de datos en el sistema se cuenta con una conexión vía internet?

Sí ☐ No ☐

Especifique: _____

SOPORTE DE INFORMACION:

65. ¿Para la continuidad de los datos de sistema se cuenta con discos duros?

Sí ☐ No ☐

Especifique: _____

---

68. ¿Para la continuidad de los datos de sistema se cuenta con discos virtuales?

Sí ☐ No ☐

Especifique: _____

---

69. ¿Para la continuidad de los datos de sistema se cuenta con almacenamiento en red?

Sí ☐ No ☐

Especifique: _____

---

70. ¿Para la continuidad de los datos de sistema se cuenta con disquetes?

Sí ☐ No ☐

Especifique: _____

---

71. ¿Para la continuidad de los datos de sistema se cuenta con CD-ROM?

Sí ☐ No ☐

Especifique: _____

---

72. ¿Para la continuidad de los datos de sistema se cuenta con Memorias USB?

Sí ☐ No ☐

Especifique: _____

---

73. ¿Para la continuidad de los datos de sistema se cuenta con DVD?

Sí ☐ No ☐

Especifique: _____

---

74. ¿Para la continuidad de los datos de sistema se cuenta con tarjetas de memoria?

Sí ☐ No ☐

Especifique: _____

---

75. ¿Para la continuidad de los datos de sistema se cuenta con tarjetas inteligentes?

Sí ☐ No ☐

Especifique: _____

76. ¿Para la continuidad de los datos de sistema se cuenta con un material impreso?

Sí ☐ No ☐

Especifique: _____

77. ¿Para la continuidad de los datos de sistema se cuenta con cinta de papel?

Sí ☐ No ☐

Especifique: _____

78. ¿Para la continuidad de los datos de sistema se cuenta con microfilm?

Sí ☐ No ☐

Especifique: _____

79. ¿Para la continuidad de los datos de sistema se cuenta con tarjetas perforadas?

Sí ☐ No ☐

Especifique: _____

EQUIPAMIENTO AUXILIAR:

80. ¿En caso de supuestos que atenten contra la disponibilidad del sistema se cuenta con fuentes de alimentación?

Sí ☐ No ☐

Especifique: _____

81. ¿En caso de supuestos que atenten contra la disponibilidad del sistema se cuenta con sistemas de alimentación ininterrumpida?

Sí ☐ No ☐

Especifique: _____

---

82. ¿En caso de supuestos que atenten contra la disponibilidad del sistema se cuenta con generadores eléctricos?

Sí ☐ No ☐

Especifique: _____

---

83. ¿En caso de supuestos que atenten contra la disponibilidad del sistema se cuenta con equipos de climatización?

Sí ☐ No ☐

Especifique: _____

---

84. ¿En caso de supuestos que atenten contra la disponibilidad del sistema se cuenta con cableado?

Sí ☐ No ☐

Especifique: _____

---

85. ¿En caso de supuestos que atenten contra la disponibilidad del sistema se cuenta con cable eléctrico?

Sí ☐ No ☐

Especifique: _____

86. ¿En caso de supuestos que atenten contra la disponibilidad del sistema se cuenta con fibra óptica?

Sí ☐ No ☐

Especifique: _____

87. ¿En caso de supuestos que atenten contra la disponibilidad del sistema se cuenta con discos duros?

Sí ☐ No ☐

Especifique: _____

88. ¿En caso de supuestos que atenten contra la disponibilidad del sistema se cuenta con equipos de destrucción de soportes de información?

Sí ☐ No ☐

Especifique: _____

89. ¿En caso de supuestos que atenten contra la disponibilidad del sistema se cuenta con mobiliarios?

Sí ☐ No ☐

Especifique: _____

90. ¿En caso de supuestos que atenten contra la disponibilidad del sistema se cuenta con cajas fuertes?

Sí ☐ No ☐

Especifique: _____

INSTALACIONES:

91. ¿El sistema se encuentra ubicado en: ?

a) Recinto

b) Cuarto

c) Edificio

d) Otros:…….……

92. ¿El sistema respecto a su integridad cuenta con una instalación de respaldo?

Sí ☐ No ☐

Especifique: _____

PERSONAL:

93. ¿Para una mayor continuidad del sistema este se encuentra bajo la supervisión de usuarios externos?

Sí ☐ No ☐

Especifique: _____

---

94. ¿Para una mayor continuidad del sistema este se encuentra bajo la supervisión de internos?

Sí ☐ No ☐

Especifique: _____

95. ¿Para una mayor continuidad del sistema este se encuentra bajo la supervisión de operadores?

Sí ☐ No ☐

Especifique: _____

95. ¿Para una mayor continuidad del sistema este se encuentra bajo la supervisión de administradores de Sistemas?

Sí ☐ No ☐

Especifique: _____

96. ¿Para una mayor continuidad del sistema este se encuentra bajo la supervisión de administradores de comunicación?

Sí ☐ No ☐

Especifique: _____

97. ¿Para una mayor continuidad del sistema este se encuentra bajo la supervisión de administradores de seguridad?

Sí ☐ No ☐

Especifique: _____

98. ¿Para una mayor continuidad del sistema este se encuentra bajo la supervisión de desarrolladores/programadores?

Sí ☐ No ☐

Especifique: _____

---

99. ¿Para una mayor continuidad del sistema, se contiene una relación con proveedores?

Sí ☐ No ☐

Especifique: _____

Encuestador	**ENCUESTADO**	**DIRECTOR DE LA UNIDAD**

ENCUESTAS:

U.A.P.	**FORMULARIO DE ENCUESTA** **(TRABAJO DE CAMPO)**	**FORM-ACYT-010** **VERSIÓN No. 2**

DATOS GENERALES DE LA PERSONA

NOMBRE COMPLETO: **……**	**INSTITUCION:** **Universidad Amazónica de Pando**
CARGO: **……..……**	**UNIDAD:** **……**

1) De qué forma hace uso del Sistema Siringuero, como:

R.

☐ Universitario

☐ Funcionario

2) ¿Tiene una sesión (loguin) mediante un usuario y contraseña, el cual le permita identificarse en el sistema para prestar servicios con relación a su función?

R.

☐ Si No ☐

3) ¿Qué servicios realiza a través del Sistema Siringuero, especifique alguno de ellos?

R……
……
……
……
……
……
……
……
……
……

4) ¿Para la utilización del Sistema siringuero hace uso de Internet?

R.

☐ Si ☐ No

5) ¿Los servicios que presta mediante el Sistema Siringuero se realizan en horarios establecidos?

R.

☐ Si ☐ No

6) ¿Para el uso del sistema Siringuero con respecto a la función que ejerce ha recibido capacitación sobre el manejo correspondiente?
R.

☐ Si ☐ No

7) ¿Para el manejo del Sistema le han dado a conocer políticas de seguridad que debe tomar en cuenta para un correcto uso?

R

☐ Si ☐ No

8) ¿Si respondió la pregunta nro. 7 especifique a lo mínimo 5 políticas que aplique con relación a su rol?

R.

_____
_____
_____
_____
_____

Encuestador	**Encuestado**

VERIFICACIÓN DE ACTIVOS:

U.A.P.	**FORMULARIO DE LISTA DE ACTIVOS** **(TRABAJO DE CAMPO)**	**FORM-ACYT** **VERSIÓN No. 1**

DATOS GENERALES DE LA PERSONA

NOMBRE COMPLETO: ……	**INSTITUCION:** **Universidad Amazónica de Pando**
CARGO: ……	**UNIDAD:** ……

LISTA DE ACTIVOS	SI	NO
1. PC		
2. LAPTOP		
3. IMPRESORAS		
4. SCANNER		
5. DISCO DURO EXTERNO		
6. CD'S		
7. DVD		
8. SERVIDOR DE APLICACIONES		
9. SERVIDOR DE BASE DE DATOS		
10. SERVIDOR WEB		
11. AIRE ACONDICIONADO		
12. UPS-SISTEMA DE ALIMENTACION ININTERRUMPIDAD		
13. POWER-ESTABILIZADOR DE ENERGIA		
14. FIREWALLE		
15. MATERIAL IMPRESO		
16. ANTIVIRUS		
17. FIREWALLE		
18. SISTEMAS OPERATIVOS		
19. NAVEGADORES WEB		
20. MICROSOFT OFFIICE		
21. SWITCH		
22. ROUTER		
23. HUP		
24. RED LOCAL		
25. MANUAL DE INSTALACION DE APLICACIONES		
26. MANUAL DE USUARIO		
27. MUNUAL DEL SISTEMA		
28. MANUAL DE ESTRUCTURA DE LA RED DE DATOS		